



Convergencias de la tecnología y la justicia

Adriana del Pilar Henao Ochoa
Diana María Ramírez Carvajal
Compiladoras



**Institución
Universitaria
de Envigado**

VIGILADA MINEDUCACIÓN



Red

— Para el Estudio del Proceso y la Justicia —

Convergencias de la justicia y la tecnología

Institución Universitaria de Envigado

Red para el Estudio del Proceso y la Justicia

Convergencias de la justicia y la tecnología

Institución Universitaria de Envigado

Red para el Estudio del Proceso y la Justicia

Adriana del Pilar Henao Ochoa

Diana María Ramírez Carvajal

Coordinación académica



Henao, Adriana del Pilar; Ramírez Carvajal, Diana María (Comp.)
Convergencias de la justicia y la tecnología/ Coordinación académica, Adriana del Pilar
Henao Ochoa, Diana María Ramírez Carvajal – Envigado: Institución Universitaria de Envigado,
2023. 179 páginas.

ISBN-e: 978-628-7601-94-9

1– Administración de justicia – Innovaciones tecnológicas – 2. Derecho – procesal – Innovaciones
tecnológicas – 3. Administración de justicia – Inteligencia artificial – 4. Derecho procesal – Inteli-
gencia artificial – 5. Procedimiento penal – Innovaciones tecnológicas

347.013 (SCDD-ed.22)

CONVERGENCIAS DE LA JUSTICIA Y LA TECNOLOGÍA

© Red para el Estudio del Proceso y la Justicia

© Institución Universitaria de Envigado (IUE)

Colección académica

Edición: octubre de 2025

ISBN-e:978-628-7601-94-9

Institución Universitaria de Envigado

Rector

Rafael Alejandro Betancourt Durango

Vicerrector de Docencia

David Alberto Londoño Vásquez

Jefe de Biblioteca

Juan Paulo Vélez

Equipo Editorial

Coordinadora Fondo Editorial

Ladis Frías Cano

Asesora editorial

Juana María Alzate

Gestor editorial

Jaime Andrés Trujillo

Diagramación

Leonardo Sánchez Perea

Institución Universitaria de Envigado

Carrera 27 B # 39 A Sur 57 - Envigado Colombia

www.iue.edu.coTel: (+4) 604 339 10 ext. 1524

Red para el Estudio del Proceso y la Justicia

Coordinadora

Diana María Ramírez Carvajal

Decano IUE – representante

José Fernando Hoyos

Docente líder IUE – representante

Adriana del Pilar Henao Ochoa

Corrección de texto

Juan Carlos Márquez Valderrama

Coeditado con Red para el Estudio
del Proceso y la Justicia

red@procesalyjusticia.org

www.procesalyjusticia.org/

Medellín, Antioquia-Colombia

El contenido de esta obra corresponde al derecho de expresión del autor y no compromete el pensamiento institucional de la Institución Universitaria de Envigado, ni desata su responsabilidad frente a terceros. El autor asume la responsabilidad por los derechos de autor y conexos.



Esta obra está bajo una licencia de Creative Commons Reconocimiento -No Comercial-Sin Obra Derivada 4.0 Internacional. Más información: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

Contenido

Prólogo	9
Capítulo 1. Blockchain y su impacto en el ámbito de la Justicia	11
<i>Federico M. Álvarez Larrondo</i>	
Capítulo 2. Ciberespionaje en un mundo interconectado: un análisis de la estrategia China y la respuesta de Occidente	31
<i>Camilo Alberto Vargas Cano, Juan Fernando Gil Osorio y Jonnathan Jiménez Reina</i>	
Capítulo 3. Por qué es necesario un (nuevo) marco jurídico para promover (las formas y los registros para) las finanzas que necesitan las empresas del siglo XXI	59
<i>Sebastián Heredia Querro</i>	
Capítulo 4. Protección de los datos personales en la era cibernética: un enfoque constitucional y procesal	89
<i>Juan Esteban Aguirre Espinosa, Dany Steven Gómez Agudelo y Sebastián Díaz Bolívar</i>	
Capítulo 5. Aspectos legales y éticos de la Inteligencia Artificial: un enfoque en LLM y arquitecturas RAG	105
<i>Daniel Betancur Vásquez, Daniel Carmona Cardona y Edwin Alexander Moncada</i>	
Capítulo 6. Algor-ética: un concepto en construcción necesario para materializar la tutela judicial efectiva en una administración de justicia asistida por la inteligencia artificial	133
<i>Débora Guerra Moreno y Darwin Clavijo Cáceres</i>	
Capítulo 7. El “abogado programador” como alternativa para abordar la IA en el derecho procesal Perspectivas a partir de la Sentencia T-323/24	155
<i>Omar Alfonso Cárdenas Caycedo</i>	
Acerca de los autores	175

Prólogo

El mundo del derecho se encuentra en una encrucijada sin precedentes. En un contexto global marcado por la revolución digital, los sistemas jurídicos y las disciplinas afines enfrentan desafíos que exigen repensar los paradigmas tradicionales. La obra que el lector tiene en sus manos *Convergencias de la tecnología y la justicia*, no es solo un compendio de reflexiones sobre los temas emergentes en la intersección entre tecnología y justicia, es también una invitación a mirar hacia adelante, a anticipar y construir el futuro del derecho con las herramientas que el siglo XXI nos ofrece.

Los capítulos de este libro han sido elaborados con un enfoque interdisciplinar y colaborativo, lo que refleja el espíritu de trabajo de la comunidad académica y profesional que conforma la Red Proceso y Justicia. Este es nuestro décimo libro de investigación como esfuerzo conjunto, lo cual no solo es un testimonio del potencial transformador de las alianzas entre disciplinas como la ingeniería, la informática y el derecho, sino también un recordatorio de que la innovación jurídica no puede darse en aislamiento, por el contrario, demanda la confluencia de perspectivas diversas que enriquezcan y amplíen nuestra comprensión de los retos y oportunidades que plantean las nuevas tecnologías.

Su nombre, *Convergencias de la Tecnología y la Justicia*, parte de una premisa fundamental: en el corazón de la transformación digital se encuentra la justicia como pilar de las sociedades democráticas. Los avances tecnológicos, desde el *blockchain* hasta la inteligencia artificial (IA), no solo redefinen los procesos judiciales y administrativos, también replantean nociones tradicionales como el acceso a la justicia, la protección de derechos fundamentales y la ética en la toma de decisiones. Este nuevo horizonte es lo que denominamos Convergencias de la Tecnología y la Justicia, una disciplina emergente que reconoce la necesidad de conectar las herramientas tecnológicas con las normativas jurídicas para abordar de manera efectiva las problemáticas contemporáneas.

El primer capítulo explora el *blockchain*, diseñado inicialmente para registros financieros, y sienta las bases sobre cómo esta tecnología está revolucionando la transparencia, la seguridad y la eficiencia en procesos legales. Este análisis invita al lector a reflexionar sobre su implementación en sistemas judiciales que buscan ganar legitimidad y confianza públicas.

El capítulo dos analiza el “Ciber-espionaje en un mundo interconectado” y examina el delicado equilibrio entre el avance tecnológico y los conflictos geopolíticos. Este análisis, centrado en la estrategia de China y la respuesta de Occidente, ofrece



una perspectiva sobre cómo la soberanía digital y la seguridad informática deben integrarse en las políticas globales y locales.

En el capítulo tercero se plantea un desafío crucial: repensar las estructuras normativas que regulan las finanzas empresariales. En un entorno donde las tecnologías emergentes han desbordado los marcos tradicionales, este capítulo ofrece herramientas para diseñar políticas inclusivas que fomenten el crecimiento económico y la innovación.

A su vez, en los capítulos cuarto y quinto se abordan problemáticas que se encuentran en el núcleo de los derechos fundamentales. Por un lado, resulta vital pensar en la “Protección de los datos personales en la era cibernética” frente a la creciente amenaza de la vulneración de la privacidad. Por otro lado, en “Aspectos legales y éticos de la Inteligencia Artificial” se plantea un debate crucial sobre los modelos de lenguaje y las arquitecturas RAG (*retrieval-augmented generation*), y se destaca la necesidad de una regulación proactiva que equilibre innovación y responsabilidad.

Finalmente, con el surgimiento de estructuras híbridas, surge un término que será clave en el debate jurídico del futuro la: “Algor-Ética”, y la necesidad de proponer “El ‘abogado programador’ como alternativa”. Ambas son propuestas visionarias que combinan el conocimiento del derecho con habilidades humanas y técnicas para abordar los nuevos desafíos.

A medida que avanzamos hacia un futuro dominado por tecnologías disruptivas, es fundamental que el derecho, en tanto estructura que regula las relaciones humanas, no quede rezagado. La justicia del siglo XXI debe ser inclusiva, equitativa y transversalizada con las herramientas tecnológicas. Esta obra es una invitación a todos los lectores, ya sean estudiantes, académicos o profesionales, a formar parte activa de este proceso de transformación.

El desafío es inmenso, pero, como bien señala la Agenda 2030, “la construcción de sociedades pacíficas, justas e inclusivas es una tarea compartida”. Que este libro sea un paso hacia ese objetivo común.

Diana Ramírez Carvajal
Coordinadora



Capítulo 1

Blockchain y su impacto en el ámbito de la Justicia

Federico M. Álvarez Larrondo

Introducción a *Blockchain*

Las últimas décadas nos han legado avances tecnológicos impensados hace un tiempo atrás, al menos para el grueso de la humanidad. Día tras día nos sorprenden nuevas herramientas que nos enfrentan como sociedad a cambios muchas veces drásticos. Entre esos escenarios se destaca la cadena de bloques o *Blockchain*, como se la conoce ya a nivel global, en un nuevo anglicismo que se instala a los codazos entre nuestro rico lenguaje castizo.

Si bien muchos creen que esta tecnología nació con Bitcoin (2008), en verdad su origen data de un tiempo antes. La primera vez que se usó dicho término fue en el año 1982 en una disertación académica en la Universidad de Berkeley, brindada por David Chaum bajo el título “Sistemas informáticos establecidos, mantenidos y confiables por grupos mutuamente sospechosos”. En esa primera exposición pública, la idea no se centraba en ser el soporte de monedas digitales, aunque Chaum reconocería ese potencial y lanzaría una compañía denominada DigiCash en el año 1989 que sería responsable de la aparición de las primeras monedas virtuales en 1995. Sin embargo, su sistema operaba sobre el sistema tradicional de monedas estatales (es decir, emitidas por los Estados), y como Chaum no logró convencer a las entidades bancarias de sus beneficios y no disponía de la infraestructura con la que Internet cuenta hoy, su proyecto fracasó poco después.

Sin embargo, de manera casi contemporánea, dos científicos de investigación, Stuart Haber y W. Scott Stornetta, introdujeron en el año 1991 una solución computacionalmente práctica para los documentos digitales con el fin de que no pudieran ser modificados o manipulados. Ese sistema usó una cadena de bloques con seguridad criptográfica que almacenaba los documentos con sello de tiempo, y en 1992 incorporaron al diseño los árboles Merkle, lo que lo hizo más eficiente al permitir que varios documentos se reunieran en un solo bloque. Sin embargo, esta tecnología no se utilizó y la patente caducó en 2004.



Cuatro años después cuando asistiríamos al momento cumbre, donde la idea por otros macerada, encontraba la aplicación práctica que habría de cambiar el futuro inmediato. Fue en 2008 que presenciamos la publicación del artículo técnico titulado “Bitcoin: A Peer-to-Peer Electronic Cash System” que un autor, o un grupo de personas anónimas, actuando bajo el seudónimo de Satoshi Nakamoto, ofreció a la comunidad en su sitio web. En este documento, Nakamoto propuso la creación de una moneda digital, Bitcoin, que permitiría a las personas realizar transacciones directamente entre ellas sin la intervención de terceros como bancos o gobiernos. La innovación central de esta propuesta era la tecnología subyacente: la cadena de bloques o *Blockchain*.

Si bien inicialmente Blockchain fue diseñado como la infraestructura para Bitcoin y permitió un cambio de magnitudes inusitadas en el campo monetario, pronto se reconoció su potencial en otros sectores, ya que proporciona una solución eficiente para problemas relacionados con la confianza, la verificación de datos y la seguridad.

De allí que Blockchain se instituyera como una tecnología emergente que ha comenzado a transformar muchos sectores económicos y sociales debido a sus propiedades únicas: descentralización, transparencia e inmutabilidad. Esto ha permitido que, pese a un inicio asociado casi exclusivamente con las criptomonedas, hoy haya evolucionado hasta abarcar un espectro mucho más amplio de aplicaciones, que incluyen sectores como la justicia, la salud, las finanzas, la logística, entre otras.

Pero, para medir sus usos potenciales dentro del campo que nos convoca, es menester comprender su funcionamiento. Y eso haremos a continuación.

Estructura y funcionamiento de Blockchain

¿Qué es *blockchain*?

Para entender el objeto de nuestro estudio vamos a desentrañar su estructura y funcionamiento en el ecosistema Bitcoin. En principio, porque el bitcoin fue pionero, pero, además, para comprender que puede haber multiplicidad de cadenas de bloques, cada una con sus particularidades y características. Veamos.

La blockchain es una base de datos, un registro que, en el caso de bitcoin, se constituye en un libro de contabilidad donde se asientan todos los movimientos (transferencias) de esa criptomoneda en particular. En ese registro quedan asentadas todas y cada una de las operaciones realizadas con esta moneda desde que se creó el primer bitcoin hasta el presente. Es un registro único, solo que existen tantas copias del mismo como computadoras acepten descargarlo y guardarlo en ellas.



Es un registro porque, como estamos en presencia de una moneda sin corporeidad, sin existencia física (no es una moneda de metal ni un billete, solo es un asiento contable), para acreditar su existencia y titularidad necesita de un asiento en el cual “registrarse”.

Ahora bien, ese dinero registrado enfrenta un primer problema, que se centra en la posibilidad de poder gastar esa única moneda muchas veces, lo cual se presenta como irracional. Volvamos al mundo físico y pensemos, cuando tengo un billete estatal físico de mil pesos y lo entrego en un intercambio comercial, ese billete ya no puedo volverlo a gastar porque ya “desapareció” de mi dominio, dado que no lo tengo más. Por el contrario, si mi billete de mil pesos está asentado en mi caja de ahorros bancaria, cuando compro con mi tarjeta débito o a través de otra pasarela de pago con mi código QR, tan solo estoy transmitiendo información. En ese caso podría volver a gastar ese asiento infinitas veces si es que la entidad bancaria no se percató de ello o su sistema informático falla, pero como esto no ocurre no puedo volver a disponer de esos mil pesos, no porque hayan desaparecido de mi dominio físico, sino porque una tercera persona (el banco), asienta en sus registros que yo he ordenado transferir esa cantidad a otra persona y, por consiguiente, reduce ese monto de mi saldo. Si esta es la lógica aplicada al dinero electrónico, veremos que algo similar (aunque no igual) sucede con el bitcoin, solo que en este caso la criptomoneda, a diferencia del dinero estatal (dinero *fiat*), no otorga la posibilidad de su representación física, todo es virtual, como en nuestros depósitos bancarios.

Pero, entonces, ¿qué es lo novedoso que trae blockchain? La diferencia central con el sistema actual está dado por el hecho de que ese registro ya no lo lleva una única persona, la entidad financiera, sino que se lleva en forma colaborativa.

Registro colaborativo. Seguridad basada en el consenso mayoritario

El banco en el que tenemos depositados nuestros ahorros o salarios sabe todo lo que poseemos y lo que hemos hecho con nuestro dinero. Cada vez que pagamos un servicio, un bien, un viaje, o lo que sea con nuestras tarjetas de débito o crédito, la información vinculada a esas operaciones queda registrada en nuestra entidad, como también lo que nos ingresa y quién nos lo envía. Toda nuestra vida de consumo está allí disponible. Y la entidad bancaria no sabe eso solo respecto de nosotros, sino de todos y cada uno de sus usuarios; tiene un perfil de todos nuestros gustos y elecciones.

Ahora bien, lo que plantea la blockchain es que ese registro, en lugar de ser llevado solo por el banco, lo sea por todos aquellos que estén dispuestos a almacenar una copia en sus computadoras, decenas de miles de personas que ponen sus recursos a disposición de este proyecto colectivo con fines diversos, como habremos



de ver más adelante. En cada una de esas máquinas reposa una copia del registro de transacciones, ya no hay un único sujeto detentando toda la información, sino que la misma se “democratiza”, es como si todos los clientes del banco lleváramos la contabilidad, pero ya no solo de nuestro propio dinero sino del de todos los que somos clientes. El punto débil es que todos sabrían de nuestras finanzas, algo de lo que también Bitcoin se ha ocupado como veremos más adelante.

En el sistema de blockchain que da base a Bitcoin, no existe ningún requisito subjetivo para acceder a llevar el registro, no hay que acreditar ninguna habilidad especial, ni siquiera debe uno identificarse individualmente para actuar como “nodo” de la plataforma. Y tampoco hay condicionamiento para abandonar la actividad, ya que la idea está centrada en la libertad más absoluta de entrada y salida de todos quienes espontáneamente quieran colaborar llevando el registro. Y no hay jerarquías, es un registro llevado entre pares o iguales, *peer-to-peer*.

Esta actuación colectiva coadyuva a su vez a incrementar los índices de seguridad del sistema. En un registro centralizado, para cambiar un registro se debe atacar un único sistema, el del agente central que lleva toda la información (el banco). En cambio, en un sistema como blockchain, donde todos los usuarios llevan una copia del registro, para modificarlo se debería alterar la mayoría de esos registros, se debería atacar la mayoría de las máquinas, lo cual resulta de muy difícil factura y, además, costoso. Si muchas personas que no tienen vínculo entre sí son testigos de un hecho, es difícil que la mayoría no coincida en los elementos fundamentales. De allí que si alguien quisiese mentir para favorecer a alguno de los involucrados, quedaría en evidencia ante la concordancia de los demás. Esta es la idea que trasunta la blockchain y que ha sido comprobada matemáticamente a partir del “Problema de los generales bizantinos”. Así, entonces, si en nuestro sistema tenemos miles de nodos, habría que reunir más de la mitad de ellos para que todos actúen coordinadamente en pocos minutos para alterar el registro; por ello se habla de su fiabilidad.

Algoritmos de encriptación asimétrica

El sistema base del bitcoin se sustenta en el modelo de criptografía asimétrica, de doble clave o clave pública. La aparición de la criptografía asimétrica se debió al trabajo de Ronald Rivest y sus colaboradores Adi Shamir y Leonard Adleman, todos matemáticos del MIT, quienes, en el año 1977, publicaron un trabajo intitulado “Un método para la obtención de firmas digitales y sistema de criptografía de clave pública”. Los autores idearon un algoritmo consistía en una secuencia de operaciones que permitía generar dos claves enlazadas matemáticamente entre sí, de manera que lo que se encripta con una de las claves solo se puede descryptar con la otra y viceversa, además, las dos claves tienen la propiedad de que conocer una de ellas



no significa que se pueda deducir la otra. Esto es lo que permite utilizar una de las claves como “clave privada” que, como tal, el usuario debe mantener reservada y la otra, como “clave pública”, que se puede dar a conocer a terceros incluso por medios de comunicación inseguros, lo cual es fundamental en el sistema ideado por Nakamoto, que es lo que permite que personas desconocidas que no tienen por qué confiar entre sí, puedan trabar relaciones en internet.

El genial González-Meneses (2019) se pregunta entonces para qué sirve este tipo de criptografía de doble clave. Y enseguida responde: para transmitir mensajes de forma confidencial a través de un medio inseguro como es Internet. El remitente encripta el mensaje (cualquiera que sea, incluido una criptomoneda) aplicando la clave pública del destinatario que le ha sido informada previamente por este, por un medio que no tiene por qué ser confidencial, o que incluso puede ser de conocimiento público general. Ese mensaje encriptado solo puede ser desencriptado aplicando la clave privada, que es correlativa de la que se empleó para cifrar, cuyo titular será el único que podrá acceder al mensaje.

El citado autor explica su aplicación en el sistema Bitcoin. Sostiene que el programa informático mediante el que opera esta criptomoneda se descompone a su vez en dos: lo que se podría llamar la aplicación básica, de simple usuario o “programa cliente”, y la aplicación avanzada o completa, que se conoce como *Bitcoin core*, que es la que utilizan los nodos o mineros (de los que luego hablaremos).

En cuanto a la aplicación básica, la que utiliza el simple usuario, para operar con ella basta con descargarla en un dispositivo cualquiera con conexión a internet, como puede ser un *Smartphone*. Esta aplicación sirve para generar y manejar una *wallet* o monedero de Bitcoin, mediante el cual se pueden recibir y transferir bitcoins. Para ello, lo primero que se hace es generar el correspondiente par de claves: privada y pública.

Una vez descargada la aplicación, y sin tener que seguir conectado a internet, se hace clic en una pestaña que dice “Nueva dirección” y la aplicación automáticamente hace lo siguiente: primero genera aleatoriamente un número de 256 bits que va a funcionar como clave privada de encriptación. Partiendo de este número, se genera otro número que es la correlativa clave pública, del que se calcula a su vez el *hash*, que es lo que va a operar como dirección en Bitcoin y que aparece como una determinada secuencia o *string* de letras y números.

Es aquí entonces donde reside uno de los puntos más disruptivos de esta criptomoneda y que genera profundos debates en los Estados tradicionales, porque no existe un control nominal, sino puramente criptográfico que permite mantener el anonimato (en principio) del titular de esas claves. Este punto es de suma importancia, puesto que nos pone en crisis frente al sistema que han construido



los Estados al momento de regular la firma digital, la cual se ha pensado como un medio de imputación jurídica de una determinada declaración negocial, a una persona física o jurídica concreta, a fin de poder responsabilizarla como firmante de un negocio o documento.

Sin embargo, Bitcoin pretende ser simplemente dinero efectivo para el mundo virtual, y al igual que sucede con el físico que se entrega en mano, la identificación de quien lo da carece de todo interés. De allí que a este sistema no le interese en absoluto identificar al titular de las claves pública y privada, sino asegurar a través de ellas que el titular de los bitcoins sea el único que pueda disponer de ellos.

Por eso emerge de lo expuesto un punto central. En Bitcoin yo solo tengo “dinero” disponible o gastable mientras conserve la clave privada vinculada a la clave pública beneficiaria de transacciones anteriores. Si pierdo la clave privada, por más que en el registro de la cadena de bloques figuren bitcoins acreditados a mi clave pública, nunca podré dar la orden de su transferencia a terceros. Ergo, habré “perdido” mi dinero, porque no puedo disponer de él, aunque pueda ver el registro.

Con base en lo anterior, una consecuencia extraordinariamente importante de la vinculación de la disponibilidad de un saldo de dinero al conocimiento de una clave privada, es que los saldos de bitcoins son en principio incoercibles, inembargables e irreivindicables.

La cadena de bloques

Ahora bien, para evitar el “doble gasto” al que hicimos mención anteriormente (esto es, que yo pueda ordenar muchas veces la transferencia de los mismos bitcoins a distintas claves públicas de distintas personas), se recurre a un registro cronológico de transacciones que comprende todas las transacciones que realizan todos los usuarios de la moneda, que impide que operaciones ya empleadas como *input* (entrada) de una transacción puedan ser empleadas otra vez como *input* de transacciones posteriores.

En una red descentralizada, ello requiere comunicar cada nueva operación a la red, es decir, al conjunto de los usuarios del sistema, pero no a cada uno de los usuarios individuales de Bitcoin, sino solo a un grupo “cualificado”, que son los llamados “nodos” o “mineros”.

Estos mineros con sus máquinas conectadas a Internet las veinticuatro horas del día y “corriendo” la aplicación, recogen todos los nuevos mensajes de transacciones de bitcoins que se emiten en cualquier lugar del mundo por quienes usan la misma. Pero no solo recogen las operaciones, sino que también verifican la autenticidad de las firmas electrónicas que incorporan esos mensajes y confrontan si determinada firma no había gastado ya previamente esos bitcoins asentados en el



registro. Esto último se hace localizando en la cadena de bloques el *hash* de la transferencia anterior de cuyo saldo ahora se ordena disponer, y se verifica que la clave pública de Bitcoin a la que se habían destinado esos fondos se corresponde con la clave privada con la que se ordena la nueva transferencia, al tiempo que se valida que los fondos estén disponibles por no haber sido incluidos como *input* en una transferencia anterior. Para poder hacer esto, los mineros deben disponer del historial completo de las transacciones asentadas en la cadena de bloques de Bitcoin a fin de realizar el cotejo. Así, cada minero descarga en su equipo un ejemplar completo del registro universal e incremental de Bitcoin.

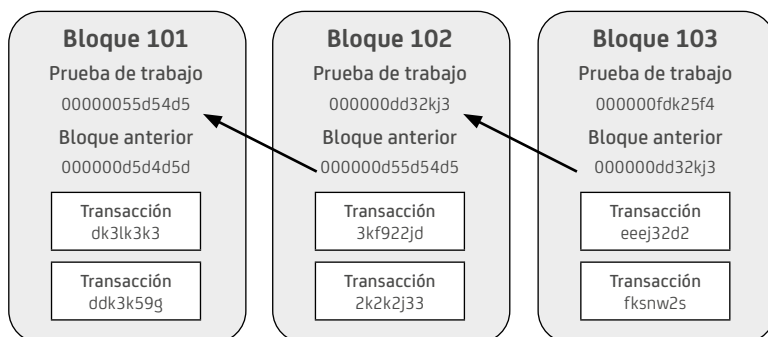
Vale recordar que este “libro mayor” de transacciones lo forman todos los mineros a la vez mediante la generación sucesiva de bloques de transacciones. Ahora bien, cuando una transacción se carga en la red, les llega a todos los mineros, porque todos los nodos recogen y validan las transacciones. Sin embargo, si esto fuera así, cada minero formaría una cadena propia y el sistema carecería de sentido.

Por eso, cada validación que realizan los nodos no queda incorporada automáticamente al historial único de Bitcoin, sino que, con el conjunto de las nuevas transacciones recibidas y validadas, en un lapso de tiempo establecido, un determinado minero que triunfe en una competencia matemática contra los restantes formará un paquete o “bloque” para su incorporación a la cadena de bloques.

Cada nuevo bloque está integrado por el texto de todas las transacciones que se hicieron en el tiempo transcurrido entre el cierre del bloque anterior y el nuevo y, como primer componente, por el *hash* del bloque inmediatamente anterior. A su vez, a partir de este nuevo bloque formado por el *hash* del bloque anterior y las nuevas transacciones recopiladas y validadas, se calcula su propio *hash* que será incorporado como primer ítem en el bloque siguiente, y así sucesivamente, de manera que se establezca la cadena. Si los bloques no se encadenaran de esa manera, la manipulación de un bloque posterior solo alteraría el *hash* de ese bloque. Sin embargo, en este caso, como cada nuevo bloque lleva el *hash* del anterior, la alteración de algún dato de cualquier bloque anterior altera el *hash* de ese bloque y de todos los posteriores a este, y por lo tanto es fácilmente detectable. Este es uno de los pilares fundamentales del sistema.

En la Figura 1 vemos cómo el bloque 102 posee en su contenido el *hash* del bloque anterior (00000055d54d5, identificado como “prueba de trabajo” en el bloque 101) y luego las transacciones registradas. Una vez cerrado el bloque 102 se genera el *hash* de ese bloque (indicado como “prueba de trabajo”), el cual, en este caso, pasará a ser registrado en el bloque siguiente (000000dd32kj3) y así sucesivamente en todos los bloques que continúen.



Figura 1. Continuidad de bloques en Bitcoin

Nota: tomado de Navarro, A. (2016, 14 de abril).

Para finalizar el recorrido, una vez que un nodo ha logrado cerrar el bloque antes que los demás nodos, porque ha resuelto con antelación la prueba matemática que propone el sistema (es decir, ha resuelto el *nonce*), acto seguido transmite ese bloque a toda la red para que sea conocido por los demás participantes. Cuando los demás reciben el bloque, proceden a verificar que se ajuste a las reglas del protocolo, para lo cual comprueban que todas las transacciones cumplen con los requisitos de autenticidad, es decir que las firmas se corresponden y que existe disponibilidad para su gasto. Surtido este paso, en un procedimiento por demás rápido, se calcula el *hash* de ese bloque y los demás nodos dejan de intentar cerrar el bloque con las mismas operaciones al haber ya un “ganador”. De inmediato todos comienzan a trabajar en un nuevo bloque con nuevas transacciones, pero tomando como dato de entrada del mismo el *hash* de ese último bloque que se ha incorporado a la cadena. Así todos los nodos actualizan su ejemplar de la cadena de bloques sumando ese nuevo bloque ya cerrado.

En síntesis, la cadena de bloques puede describirse como un “libro mayor digital”, donde cada transacción que se realiza se registra en un bloque. Estos bloques, a su vez, están vinculados de manera cronológica y lógica mediante criptografía y forman una cadena de bloques que es inmutable y segura. Cada bloque contiene tres elementos clave:

1. Datos de la transacción: esta información puede variar dependiendo de la aplicación de *Blockchain*. En Bitcoin, por ejemplo, los datos representan transacciones financieras. En otras aplicaciones, como contratos inteligentes, los datos pueden incluir términos legales o condiciones contractuales.
2. *Hash* del bloque: es un identificador único que se genera a partir de la información contenida en el bloque. Cualquier alteración en los datos del bloque cambia



su *hash*, lo que sirve como un sistema de seguridad para detectar modificaciones no autorizadas.

3. *Hash* del bloque anterior: cada bloque contiene también el *hash* del bloque que le precede, lo que asegura la continuidad de la cadena y dificulta cualquier intento de alterar o borrar registros porque todo el sistema lo detecta.

Este sistema de bloques encadenados asegura que cualquier modificación a un bloque anterior sea extremadamente difícil, ya que requeriría alterar todos los bloques siguientes y que la red lo acepte por consenso¹.

Tipos de cadenas de bloques (*blockchains*)

Poco después de entrar en funcionamiento, la comunidad descubrió que lo más destacado de Bitcoin no era la criptomoneda, sino fundamentalmente su soporte, es decir, la cadena de bloques, que no solo podía ser utilizada para registrar transacciones “monetarias”, sino que podía emplearse para registrar todo aquello que se pretendiese de manera segura y descentralizada.

Ahora bien, la *blockchain* de Bitcoin, como vimos previamente, es una plataforma pública y abierta que cualquier persona puede descargar en sus equipos. Pero esta modalidad no es la única, y a medida que la tecnología se ha ido difundiendo, han surgido diferentes tipos de cadenas de bloques con aplicaciones específicas, pudiendo identificarse tres tipos principales de ellas, a saber:

1. Cadena de bloques pública: cualquiera puede participar y realizar transacciones en la red, así como verificar los datos almacenados. Bitcoin y Ethereum son ejemplos de cadenas de bloques públicas. Estas cadenas tienden a ser más seguras, pero pueden ser más lentas por la gran cantidad de nodos que deben validar cada transacción.
2. Cadena de bloques privada: son redes controladas por una entidad central, que decide quién puede acceder y participar en la red. Este tipo de cadena de bloques es común en empresas y organizaciones, pero pierde el atractivo perseguido por la comunidad de seguidores del modelo original que es evitar que alguien detente en soledad la información. Y aunque la estructura técnica puede dar sustento a una cadena de bloques privados, replicando la existencia de cientos de nodos, todos los nodos son de una misma persona.
3. Cadena de bloques híbrida o federada: es una combinación de las anteriores. Permite que algunas partes de la red sean controladas por una entidad central, mientras que otras permanecen abiertas y descentralizadas. Estas cadenas de

¹ Para un análisis mucho más detallado, véase: Alvarez Larrondo, F. M. (2022). *Entendiendo al Bitcoin y sus desafíos jurídicos y sociales*. Buenos Aires: La Ley.



bloques son útiles para aplicaciones en las que se requiere cierta privacidad, pero también se benefician de la transparencia.

Para sintetizar, los elementos básicos que conforman una cadena de bloques son (Preukschat, 2018, p. 24):

Un nodo, que puede ser un ordenador personal o, según la complejidad de la red, una megacomputadora. El elemento fundamental es que todos los nodos deben poseer el mismo software/protocolo para comunicarse entre sí. En una cadena de bloques pública los nodos no tienen por qué identificarse, mientras que en una privada los nodos se conocen entre sí.

Un protocolo estándar en forma de software para que en una red los nodos puedan comunicarse entre sí, como lo es el TCP/IP para internet. La idea es que permita tener un estándar común entre todos los integrantes de la red.

Una red entre pares o P2P (por sus siglas en inglés), es decir, una red de nodos conectados directamente en una misma red.

Un sistema descentralizado donde, a diferencia de uno centralizado en el que toda la información la posee una única entidad (el citado ejemplo del banco), todos los ordenadores conectados a la red la controlan en un pie de igualdad y cada uno de ellos resguarda la misma información.

Así, entonces, una cadena de bloques se conforma con un conjunto de ordenadores (o servidores) llamados “nodos” que, conectados en red, utilizan un mismo sistema de comunicación (el citado protocolo) con el objetivo de validar y almacenar la misma información registrada, todo ello en una red P2P. Esta estructura es la que garantiza, a través de algoritmos criptográficos, que la información cargada no pueda ser alterada.

Establecidas las bases y su funcionamiento, analicemos entonces sus ventajas.

Beneficios generales de la *Blockchain*

Blockchain ofrece una serie de beneficios únicos que han permitido su adopción y aplicación en diversos sectores, más allá de su uso original como tecnología detrás de las criptomonedas. Estos beneficios se derivan de su diseño descentralizado, transparente y seguro, lo que la convierte en una herramienta ideal para garantizar la integridad y la veracidad de la información en redes distribuidas. A continuación, se detallan algunos de los beneficios más importantes.

Seguridad: la seguridad es uno de los pilares fundamentales de la tecnología *Blockchain*. Cada bloque de datos está asegurado criptográficamente, lo que garantiza que una vez registrada la información, no pueda ser modificada sin alterar el



historial de la cadena. Cada bloque está enlazado con el anterior a través de un *hash* criptográfico único, de modo que cualquier intento de manipular un bloque requiere modificar todos los bloques subsiguientes, lo que sería detectado inmediatamente por el resto de la red.

Además, la cadena de bloques funciona sobre una red de nodos distribuidos, lo que significa que no existe un único punto de fallo. Esta arquitectura descentralizada reduce el riesgo de ciberataques, ya que los atacantes tendrían que comprometer una gran cantidad de nodos simultáneamente para modificar el libro mayor. Tal capacidad para garantizar la inmutabilidad de los datos es particularmente relevante en sectores como la justicia, donde es crucial la integridad de los registros judiciales y de la cadena de custodia de la evidencia.

Transparencia: otro de los beneficios clave de Blockchain es su transparencia. En una red pública de cadena de bloques, cada participante puede ver todas las transacciones que ocurren en la red en tiempo real. Esta visibilidad genera un alto nivel de responsabilidad, ya que cualquier intento de alterar la información quedaría registrado y sería fácilmente detectable, una característica particularmente valiosa en sistemas donde la confianza es un problema, como en el ámbito de la justicia o en la administración pública.

En el ámbito judicial, por ejemplo, la transparencia es clave para evitar la manipulación de la información, ya que cualquier persona con acceso a la red puede auditar los registros en cualquier momento, lo cual reduce la posibilidad de corrupción y garantiza que los procesos se realicen de manera justa y abierta.

Descentralización: una de las características más importantes de Blockchain es su naturaleza descentralizada. A diferencia de los sistemas tradicionales, donde una autoridad central (como un gobierno o una empresa) controla la base de datos, la cadena de bloques opera sobre una red distribuida de nodos. Cada nodo tiene una copia del libro mayor, y todos los nodos trabajan juntos para verificar y validar las transacciones.

Esta descentralización tiene varias ventajas. En primer lugar, elimina la necesidad de intermediarios, lo que reduce los costos y los tiempos de procesamiento de las transacciones. En segundo lugar, reduce el riesgo de fraude, ya que no hay una única entidad que pueda manipular la información a su favor. En el contexto judicial, la descentralización puede reducir la burocracia, agilizar los procesos y garantizar que no haya un único punto de control que pueda ser corrompido.

Trazabilidad: la cadena de bloques permite una trazabilidad perfecta de cualquier transacción o dato que se registre en la red. Esto significa que es posible rastrear de manera clara y precisa todo el historial de una transacción, desde su origen hasta su destino. Cada bloque de información está vinculado al anterior, lo que permite



rastrear cualquier acción realizada en la red. En sectores como la logística, la salud y la justicia, esta trazabilidad es esencial para garantizar la integridad de los procesos.

Por ejemplo, en el ámbito judicial, la cadena de bloques se puede utilizar para rastrear la cadena de custodia de pruebas, y así garantizar que cada paso del proceso quede registrado de manera inmutable y transparente. Esto proporciona una seguridad adicional para los abogados y jueces que necesitan verificar la autenticidad de la evidencia presentada en un caso.

Reducción de costos y tiempo: uno de los beneficios más inmediatos de Blockchain es la reducción de costos operativos. Al eliminar la necesidad de intermediarios y automatizar muchos procesos, la cadena de bloques puede reducir drásticamente los costos relacionados con la verificación, el procesamiento y el almacenamiento de información. En el sector financiero, por ejemplo, ha permitido transacciones más rápidas y económicas, especialmente en pagos internacionales.

En el ámbito de la justicia, la cadena de bloques puede automatizar tareas como la ejecución de contratos inteligentes, la verificación de documentos y la gestión de registros, lo cual no solo reduce costos, sino que también acelera los procedimientos judiciales, lo que permite que los casos se resuelvan más rápidamente.

Confianza y autonomía: la confianza es uno de los aspectos más valiosos que Blockchain aporta a los sistemas digitales. Al eliminar la necesidad de confiar en intermediarios o en una autoridad central, la cadena de bloques permite que las partes involucradas en una transacción confíen directamente en el sistema. Cada transacción es verificada por múltiples nodos en la red, lo que garantiza que los datos son precisos y no han sido manipulados. En sectores como el de la justicia, donde la confianza en los procesos es fundamental, la cadena de bloques puede proporcionar la garantía de que los datos son auténticos y seguros.

Además, la cadena de bloques ofrece autonomía a las partes involucradas, porque pueden interactuar directamente entre ellas sin depender de terceros para verificar las transacciones o validar los datos. Esta autonomía es clave en la creación de sistemas más justos y equitativos.

Principales beneficios de Blockchain para su uso en el contexto legal

Con base en los lineamientos que hemos expuesto, es fácil advertir que la cadena de bloques posee características que resultan de sumo interés para su uso en el campo legal. Veamos:

1. **Inmutabilidad:** una vez que un dato ha sido registrado en la cadena de bloques, no puede modificarse ni eliminarse. Esto es crucial en el contexto legal,



porque garantiza la preservación de pruebas y documentos sin posibilidad de manipulación.

2. Transparencia: todas las transacciones en la cadena de bloques son visibles para los participantes de la red, lo cual es fundamental para generar confianza, especialmente en áreas como la administración de justicia.
3. Descentralización: si la cadena de bloques es de carácter público no existirá una entidad central que controle toda la red. Esto significa que la información no podrá ser manipulada por una sola parte.

Es así que la cadena de bloques ha comenzado a revolucionar el ámbito de la justicia mediante su implementación en diversas áreas clave. La inmutabilidad, transparencia y seguridad que ofrece esta tecnología son particularmente útiles en procesos legales donde la confianza, la veracidad y la integridad de los registros son cruciales. A continuación, exploramos algunas de las aplicaciones más relevantes de la cadena de bloques en la justicia.

Contratos inteligentes (*Smart Contracts*)

Los contratos inteligentes son uno de los desarrollos más destacados que ha permitido la cadena de bloques a partir de la posibilidad de instrumentación en la cadena madre de este tipo de soluciones que es la cadena de bloques de Ethereum. Los contratos inteligentes son contratos autoejecutables que se ejecutan automáticamente cuando se cumplen las condiciones predefinidas en el código, sin la necesidad de intermediarios. En lugar de depender de terceras partes para verificar y ejecutar los términos de un contrato, los contratos inteligentes automatizan el proceso, lo que resulta en mayor eficiencia, reducción de costos y eliminación de disputas.

Un ejemplo de su aplicación es en el sector inmobiliario. En una transacción de compraventa de propiedades, un contrato inteligente podría programarse para transferir la propiedad automáticamente cuando el comprador haya completado el pago. La propiedad y el dinero cambiarían de manos de forma automática y segura una vez que se cumplan las condiciones establecidas. De esta manera, se eliminan riesgos como el fraude o la demora por parte de intermediarios.

Además, los contratos inteligentes pueden ser utilizados en múltiples acuerdos legales, como alquileres, testamentos y acuerdos de negocios, para facilitar la ejecución de términos contractuales. Sin embargo, esto crea nuevos desafíos para el mundo judicial, en atención a que estos contratos se ejecutan sin considerar los cambios legales o sociales que pueden generarse entre su celebración y su ejecución. Pensemos en tal sentido en un contrato de alquiler que determine que, ante la falta de pago, todos los servicios se cortarán y la llave electrónica de acceso se bloqueará. Supongamos que fue pactado por las partes en tiempos normales, pero al año de



su ejecución sobrevino la pandemia de Covid-19 y el Estado dispuso que se podía posponer el pago de los alquileres por unos meses, como sucedió en distintos países. Pues, en ese caso, el contrato “inteligente” habrá de ejecutarse, porque está programado para actuar de esa manera, en un contexto de absoluto aislamiento: procede a constatar la falta de pago, a cortar los servicios e impedir el acceso a la vivienda. Es allí donde la solución que puede resultar práctica en ciertos escenarios, se torna lesiva para los derechos de una de las partes.

Cadena de custodia digital (evidencia judicial)

Uno de los mayores desafíos en el ámbito judicial es asegurar la integridad de la cadena de custodia de la evidencia. Los registros de la evidencia a menudo son vulnerables a manipulación o pérdida, lo que puede afectar gravemente el resultado de un juicio.

La cadena de bloques proporciona una solución eficaz a este problema, al registrar de manera inmutable cada paso de la cadena de custodia de la evidencia en una red descentralizada. Cada vez que se manipula la evidencia, ese hecho queda registrado en la cadena de bloques y permite verificar quién tuvo acceso a la evidencia, cuándo y qué cambios se realizaron. Este proceso garantiza que cualquier alteración sea visible y verificable, y de este modo brinda una capa adicional de seguridad y confianza a los registros judiciales.

Varios países, entre ellos Estonia, ya están utilizando la cadena de bloques para registrar y asegurar la cadena de custodia en procesos judiciales, lo que permite una auditoría clara y una mayor seguridad en los procedimientos legales.

Transparencia y lucha contra la corrupción

La cadena de bloques ofrece una solución única para combatir este problema, porque proporciona un registro transparente e inmutable de todas las transacciones y decisiones judiciales.

Al quedar cada transacción registrada de manera pública, se dificulta la alteración de datos, ya que otros participantes los pueden detectar. Esto generaría mayor confianza en los sistemas judiciales, porque cualquier intento de manipulación o fraude quedaría evidenciado en la cadena de bloques.

Delito de lavado de activos

El lavado de activos es un delito complejo que a menudo es difícil de rastrear, porque los delincuentes utilizan sofisticadas redes de transferencias financieras para ocultar el origen ilícito de los fondos. Sin embargo, la cadena de bloques puede ser una



herramienta poderosa en la lucha contra este delito, ya que ofrece una trazabilidad completa y verificable de todas las transacciones financieras.

En una red de cadena de bloques, todas las transacciones están registradas de manera inmutable, de modo que se pueden rastrear desde su origen hasta su destino e identificar rápidamente transacciones sospechosas y las partes involucradas en ellas, lo cual permite que las autoridades financieras sigan el rastro del dinero de manera más precisa. Además, la cadena de bloques puede ser utilizada para crear registros financieros más transparentes que faciliten la auditoría y el seguimiento de actividades ilícitas.

Países como Estados Unidos y China han comenzado a utilizar la cadena de bloques para rastrear transacciones sospechosas y redes de lavado de dinero. Esta capacidad para rastrear y verificar transacciones en tiempo real facilita las investigaciones, permite la detección temprana de delitos financieros y aumenta la efectividad de los procedimientos judiciales.

Retos y desafíos de la implementación de Blockchain en el ámbito legal

A pesar de los numerosos beneficios que ofrece la cadena de bloques, su adopción en el ámbito legal no está exenta de desafíos. La aplicación práctica de esta tecnología enfrenta diversos obstáculos tanto técnicos como regulatorios. Para que la cadena de bloques se pueda adoptar de manera masiva en los sistemas judiciales, será necesario superar una serie de retos importantes que analizaremos a continuación.

Escalabilidad. Uno de los principales desafíos técnicos que enfrenta la cadena de bloques es la escalabilidad. A medida que aumenta el número de usuarios y transacciones en una red de cadena de bloques, la capacidad de procesar dichas transacciones en tiempo real puede verse afectada. Las redes de cadena de bloques más grandes, como Bitcoin y Ethereum, solo pueden procesar un número limitado de transacciones por segundo, lo que puede resultar en retrasos significativos cuando la red está congestionada.

Este problema de escalabilidad es especialmente relevante en el ámbito judicial, donde los sistemas legales deben manejar grandes cantidades de datos, desde documentos judiciales hasta evidencias y registros legales. Para que la cadena de bloques se pueda implementar eficazmente en este contexto, será necesario desarrollar soluciones que permitan una mayor capacidad de procesamiento, sin comprometer la seguridad ni la descentralización de la red.

Privacidad y protección de datos. A pesar de los beneficios en términos de transparencia, la naturaleza pública de muchas redes de bloques plantea preocupaciones



sobre la privacidad y la protección de datos, especialmente en el ámbito legal. En una red pública de cadena de bloques, cualquier participante puede ver las transacciones que ocurren, lo que puede ser un problema cuando se trata de información sensible o confidencial, como los detalles de un caso judicial o los datos personales de los involucrados.

Aunque las transacciones en la cadena de bloques son anónimas en teoría, las investigaciones han demostrado que es posible vincular las direcciones de la cadena con identidades del mundo real, lo que representa un riesgo para la privacidad. En el contexto legal, es fundamental garantizar la confidencialidad de ciertos datos judiciales. Por lo tanto, es necesario explorar formas de integrar la cadena de bloques con tecnologías que puedan proteger la privacidad de los usuarios, como el uso de cadenas de bloques privadas o híbridas, o la implementación de soluciones de privacidad como las pruebas de conocimiento cero (*zk-SNARKs*).

Marco regulatorio y aceptación legal. El marco regulatorio que rodea a *Blockchain* sigue siendo un área gris en muchas jurisdicciones. Aunque algunos países han avanzado en la regulación de las criptomonedas y los contratos inteligentes, aún existen vacíos legales en cuanto a la adopción generalizada de esta tecnología en otros sectores, incluyendo el sistema judicial. La falta de normas claras puede generar incertidumbre y desconfianza en la adopción de esta tecnología.

Para que se pueda adoptar la cadena de bloques en los sistemas judiciales, se requiere que los gobiernos y las instituciones reguladoras desarrollen un marco legal adecuado que permita su uso en procesos judiciales. Esto incluye establecer directrices sobre cómo deben registrarse las pruebas en la cadena de bloques, cómo deben ejecutarse los contratos inteligentes, y qué criterios se deben cumplir para garantizar la validez legal de los datos almacenados en la red.

Costos de implementación. La implementación de la cadena de bloques en los sistemas judiciales implica un costo significativo, especialmente en las fases iniciales. Los sistemas judiciales de muchos países ya enfrentan restricciones presupuestarias, y la inversión en tecnología de cadena de bloques puede no ser prioritaria a corto plazo. Además de los costos de implementación, también están los costos asociados con la capacitación del personal legal y técnico que deberá operar y mantener estos sistemas.

Sin embargo, a largo plazo, la cadena de bloques tiene el potencial de reducir costos operativos al eliminar intermediarios, automatizar procesos judiciales y mejorar la eficiencia general del sistema. Por lo tanto, aunque los costos iniciales de implementación del sistema pueden ser elevados, los beneficios a largo plazo podrían justificar la inversión. Esto, sin embargo, debe ser analizado mediante cálculos técnicos que permitan determinar la relación costo-beneficio.



Adopción y resistencia al cambio. Cualquier cambio importante en un sistema tradicional enfrenta una resistencia natural, y la cadena de bloques no es la excepción. La adopción de esta tecnología en el ámbito legal requerirá un cambio cultural, ya que muchas instituciones legales están acostumbradas a métodos tradicionales de manejo de información y verificación.

Los abogados, jueces y otros profesionales del derecho se tendrán que familiarizar con los conceptos básicos de la cadena de bloques, lo que puede generar cierta resistencia inicial. Además, para las instituciones, la adaptación de sus procedimientos y sistemas a esta nueva tecnología será un proceso lento. La educación y la formación serán claves para superar esta resistencia, y será necesario demostrar con casos reales los beneficios de la cadena de bloques para convencer a los actores del sistema judicial de su valor.

El futuro de *Blockchain* en la justicia

El potencial de la cadena de bloques para transformar los sistemas judiciales es enorme, pero su adopción aún se encuentra en una fase temprana. A medida que se superan los retos técnicos, regulatorios y culturales, es probable que la cadena de bloques desempeñe un papel cada vez más importante en la administración de justicia. Las siguientes son algunas de las posibles aplicaciones futuras de esta tecnología en los sistemas judiciales y cómo podría transformar las formas tradicionales de llevar a cabo los procedimientos legales.

Automatización de los procedimientos judiciales. Una de las mayores promesas de la cadena de bloques es la automatización de ciertos procesos judiciales mediante el uso de contratos inteligentes y registros distribuidos. En el futuro, es posible que muchas tareas rutinarias, como la presentación de documentos, la verificación de la cadena de custodia y la ejecución de sentencias, puedan ser automatizadas utilizando la cadena de bloques.

Por ejemplo, los contratos inteligentes se podrían utilizar para automatizar la ejecución de acuerdos judiciales. Si las partes involucradas cumplen con las condiciones predefinidas, como el pago de una multa o la entrega de bienes, el contrato inteligente podría ejecutar automáticamente la sentencia sin necesidad de intervención humana. Esta automatización no solo ahorraría tiempo, sino que también reduciría la posibilidad de errores o manipulaciones.

Además, la transparencia inherente a la cadena de bloques garantizaría que cada paso del proceso sea verificable por todas las partes, lo que generaría un alto nivel de confianza en el sistema.



2. Juicios digitales y descentralizados. Otra de las posibles aplicaciones futuras de la cadena de bloques en la justicia es la creación de juicios completamente digitales y descentralizados. En lugar de depender de tribunales físicos y procesos tradicionales, la cadena de bloques podría permitir la creación de plataformas descentralizadas para resolver disputas de manera digital. Los casos se podrían presentar y resolver en línea, utilizando contratos inteligentes para automatizar gran parte del proceso.

Un ejemplo son los sistemas de resolución de disputas basados en la cadena de bloques que ya se están explorando en plataformas como Kleros, donde jurados descentralizados votan sobre disputas utilizando la cadena de bloques para registrar las decisiones de manera transparente y verificable. Este enfoque podría hacer que los sistemas judiciales sean más accesibles, eficientes y menos costosos, especialmente en casos de menor envergadura.

3. Registro digital global de pruebas y documentos. En el futuro, la cadena de bloques se podría utilizar para crear un registro digital global de pruebas y documentos legales, accesible a cualquier parte interesada con los permisos adecuados. Esta red permitiría almacenar de manera segura y descentralizada documentos judiciales, contratos, registros notariales y evidencia, y garantizar que los datos permanezcan inmutables y verificables durante años. Claro está, siempre y cuando no se expongan datos sensibles que puedan afectar a las partes o a terceros.

No obstante, salvados los peligros citados, esta posibilidad no solo mejoraría la seguridad y la accesibilidad de los datos judiciales, sino que también permitiría una mayor cooperación entre jurisdicciones internacionales, al facilitar el intercambio de pruebas y documentos de manera segura y sin intermediarios. Este tipo de red podría ser particularmente útil en casos transnacionales o donde se requiera la colaboración de diferentes sistemas judiciales.

4. Democratización de la justicia. Blockchain tiene el potencial de democratizar el acceso a la justicia al proporcionar un sistema más transparente y accesible para todos. Esta tecnología podría hacer que la justicia sea más inclusiva y equitativa, porque reduce la dependencia de intermediarios y burocracias y permite que las personas resuelvan disputas y accedan a servicios legales de manera directa a través de plataformas digitales.

En lugar de depender exclusivamente de costosos procedimientos judiciales tradicionales, los ciudadanos podrían acceder a mecanismos de resolución de conflictos en línea basados en la cadena de bloques, lo cual reduciría los costos y el tiempo para lograr una solución.

5. Integración con otras tecnologías emergentes. El futuro de la tecnología Blockchain en la justicia probablemente implicará su integración con otras tecnologías emergentes, como la inteligencia artificial (IA) y el Internet de las cosas (IoT). La



combinación de la cadena de bloques con IA podría permitir la creación de sistemas judiciales inteligentes para almacenar datos de manera segura, como también para analizar patrones en los casos judiciales, identificar problemas sistémicos y proponer soluciones basadas en los datos.

Por otra parte, con la integración de Blockchain con IoT se podrían crear sistemas automatizados de monitoreo y ejecución de sentencias. Por ejemplo, en el caso de una sentencia que requiera la entrega de bienes, IoT podría utilizar dispositivos conectados para rastrear el movimiento de dichos bienes, mientras que la cadena de bloques se encargaría de verificar y registrar cada paso del proceso de entrega.

Corolario

Como lo señalábamos al iniciar estas páginas, los desafíos que nos presentan tecnologías como la cadena de bloques obligan a las y los operadores del derecho y a los funcionarios con la capacidad actualmente de tomar decisiones que habrán de impactar en el futuro, a conocer los aspectos técnicos y el funcionamiento de estas tecnologías a fin de avizorar, de manera urgente, las potencialidades que ofrecen.

Un mundo nuevo y distinto se está desarrollando ante nuestros ojos, solo que nos resulta difícil verlo porque su hábitat es el mundo virtual, mundo inasible de bits e información, que día a día nos sorprende cuando sus creaciones impactan en el viejo mundo de carne y hueso en el que habita el grueso de los usuarios y hacedores del mundo judicial.

Por ello, espero que estas páginas resulten un motor de cambio de nuestros días y constituyan una invitación a bucear por las nuevas herramientas tecnológicas a fin de que nos permitan crear un nuevo servicio de justicia más eficiente y justo. Ojalá así sea.

Finis coronat opus

Referencias

- Álvarez Larrondo, F.M. (2022), "Entendiendo al Bitcoin y sus desafíos jurídicos y sociales. Buenos Aires: Ed. La Ley.
- González-Meneses, M. (2019). *Entender Blockchain: una introducción a la tecnología de registro distribuido*. 2.ª ed. Pamplona: Ed. Aranzadi.
- Navarro, A. (2016, 14 de abril). Bitcoin Mining, la generación de bitcoins. JuncotIC [Blog]. <https://juncotic.com/bitcoin-mining-la-generacion-de-bitcoins/>
- Preuschat, Á. (2018). *Blockchain: La revolución industrial de Internet*. 6.ª ed. Barcelona: Ed. Gestión 2000.



Capítulo 2

Ciberspionaje en un mundo interconectado: un análisis de la estrategia China y la respuesta de Occidente

Camilo Alberto Vargas Cano

Juan Fernando Gil Osorio

Jonnathan Jiménez Reina

Introducción

En la actualidad, vivimos en un mundo en donde la interconexión y la digitalización de herramientas, saberes y procesos son cada vez mayores y, por ende, la ciberseguridad se ha convertido en un tema esencial que, a su vez, se ha transformado en un campo de batalla crucial para todos los Estados y actores (Krieg y Rickli, 2019). Bajo esta mirada, hemos visto en los últimos años una particular escalada en las tensiones económica, comercial y de seguridad entre Occidente y China, exacerbadas principalmente por actitudes chinas, percibidas como expansionistas (Gargiulo, 2020).

En este contexto, el ciberspionaje se ha posicionado a la vanguardia de la seguridad internacional. Por esa razón, este artículo aborda la manera en la que Occidente está respondiendo a las sofisticadas tácticas de espionaje cibernético de China, que no solo amenazan la seguridad empresarial, sino también la integridad de la infraestructura nacional crítica (Romero, 2024; Unal, 2019). A través de un análisis documental de fuentes recientes, se explora la interacción entre las estrategias defensivas occidentales y las ofensivas cibernéticas chinas, subrayando la compleja dinámica que define el nuevo orden mundial tecnológico.

El objetivo de este estudio es contextualizar el ciberconflicto entre Occidente y China, destacando cómo las tensiones económicas y comerciales actuales son moldeadas por el espionaje tecnológico. Con base en este enfoque, se arroja luz sobre las tácticas y estrategias empleadas, como también se describen los marcos legales internacionales que buscan contener esta amenaza, procurando entender si este actuar, dada su naturaleza, podría considerarse como criminal. Adicionalmente, se



ofrecen medidas que podrían estimular el reforzamiento de la ciberseguridad con el fin de proteger la propiedad intelectual y los activos tecnológicos clave, y así ofrecer una perspectiva integral sobre cómo navegar este desafío global desde un enfoque político, legal y tecnológico.

Para esto, es necesario entender que la relación entre Occidente y China en las últimas décadas se ha caracterizado por una dinámica, pero compleja, interacción entre cooperación y competencia (Pereira, 2023). Esto ha llevado a crecientes tensiones, tanto económicas y comerciales como de seguridad y defensa (De León, 2024), que han influido en las políticas comerciales y las estrategias económicas, pero además han permeado el ámbito de la ciberseguridad y transformado el espacio digital en un teatro de conflictos geopolíticos y de espionaje tecnológico (Rivas, 2021).

En el corazón de estas tensiones se encuentra la rivalidad por el liderazgo tecnológico global. Prueba de esto es que China, con su ambiciosa iniciativa *Made in China 2025*, ha establecido una hoja de ruta clara con la que busca ascender en la cadena de valor tecnológico para lograr posicionarse como líder en varias tecnologías avanzadas, que incluyen inteligencia artificial (IA), semiconductores y telecomunicaciones (Zamarrón, 2023). Esta estrategia es una gran fuente de preocupaciones en Occidente, especialmente para Estados Unidos, donde se ve como una amenaza directa a su hegemonía tecnológica y económica con posibles repercusiones para la estabilidad global (Zhao, 2019).

En consecuencia, la respuesta de Occidente ha sido multifacética, y ha incluido la implementación de políticas restrictivas en comercio y transferencias tecnológicas, así como el fortalecimiento de las normativas de seguridad nacional que afectan directamente las inversiones y operaciones de empresas tecnológicas chinas (García et al., 2021). Estas medidas han repercutido de manera directa en la economía y en el comercio globales, pero también en la ciberseguridad, ya que la batalla por la supremacía tecnológica también se libra en el dominio cibernético. Por esto, en los últimos años se ha evidenciado un aumento en las prácticas de ciberespionaje, que abarcan desde la infiltración de infraestructuras críticas hasta el robo de propiedad intelectual, lo que refleja la escalada en el conflicto subyacente (García et al., 2021; Romero, 2024).

Por lo anterior, la ciberseguridad se ha vuelto un campo crítico en esta lucha tecnológica, donde el ciberespionaje se emplea como una herramienta estratégica para ganar ventajas económicas y comerciales que terminan por traducirse en ventajas estratégicas políticas y de seguridad (Stupak, 2023). Diversos incidentes de ciberataques que apuntan a la extracción de datos sensibles y secretos comerciales se han incrementado, muchos de los cuales han sido atribuidos a actores vinculados al gobierno chino (Boylan et al., 2021; García et al., 2021). Este accionar no solo busca fortalecer las capacidades tecnológicas de China, sino también



debilitar la competitividad de las empresas occidentales y ganar influencia estratégica en sectores clave, como los ya mencionados (Akoto, 2022; Mueller, 2022).

De otro lado, Occidente ha respondido buscando intensificar sus propias capacidades de defensa en el ciberespacio. Así, pues, se han establecido múltiples unidades especializadas en ciberdefensa en distintos gobiernos y se han fomentado alianzas entre el sector público y el privado para proteger infraestructuras críticas, tecnologías e información sensible (Akoto, 2024; Rowe, 2020; Stupak, 2023). Sin embargo, la alta velocidad del desarrollo tecnológico y la naturaleza transfronteriza del ciberespacio son factores que complican la implementación de medidas de seguridad efectivas. En este sentido, la proliferación de tecnologías de doble uso, que pueden ser empleadas tanto para fines civiles como militares, añade otra capa de complejidad a la regulación y supervisión del comercio tecnológico (Gioe et al., 2020; Kim et al., 2019).

Este contexto de tensiones entre China y Occidente es un reflejo de una nueva era de rivalidad estratégica, y resalta la creciente importancia del ciberespacio como un dominio de conflicto geopolítico (Dalby, 2020). Así, la capacidad de un Estado para proteger su infraestructura y datos críticos, mientras mantiene su competitividad en la innovación tecnológica, se presenta como un pilar central de su seguridad nacional y prosperidad económica (Qureshi, 2019; Rawat et al., 2021).

Por todo lo anterior, y descrito este panorama de la realidad tecnológica en el mundo, el objetivo general del presente capítulo es abordar el problema de la ciberseguridad entre Occidente y China, describiendo cómo las distintas tensiones existentes influyen en el ciberspionaje empresarial. La pertinencia radica en la necesidad y creciente importancia de estudiar la seguridad en el campo de la tecnología y la información. En consonancia, se establecieron los objetivos para cubrir de manera responsable los múltiples aspectos de esta interacción: a) describir la naturaleza y las tácticas del espionaje cibernético chino contra Occidente, especialmente el ciberspionaje empresarial; b) abordar los marcos legales internacionales que regulan la ciberseguridad y el espionaje tecnológico y empresarial; c) analizar las respuestas occidentales a los intentos de espionaje chino más recientes, y d) proponer estrategias para mejorar la protección de la tecnología y la información sensible en el contexto de las relaciones internacionales.

De esta manera, se permite entender los métodos específicos y las intenciones detrás del ciberspionaje chino, centrando la atención en cómo estas acciones impactan directamente a las empresas occidentales. Además, con este análisis se contribuye a contextualizar las acciones dentro de la legalidad internacional, poder efectuar juicios sobre su eficacia y, en ese sentido, dimensionar las amenazas actuales.



Este estudio se fundamenta en un enfoque cualitativo que integra el análisis de documentos legales, informes de inteligencia, literatura académica y artículos periódicos, para ofrecer una comprensión detallada y contextual del ciberespionaje y las estrategias de defensa empleadas. La metodología adoptada permite explorar de manera exhaustiva tanto las tácticas de espionaje como las respuestas implementadas por Occidente, así como subrayar su efectividad y las áreas susceptibles de mejora. Este enfoque mixto resalta la profundidad y el alcance del espionaje cibernético, y enfatiza la importancia de fortalecer la resiliencia de los sistemas y la seguridad de la información crítica frente a futuras intrusiones. Al proporcionar un análisis informado y basado en evidencia, este estudio busca ofrecer un panorama comprensivo y multidimensional, crucial para entender y abordar estos desafíos contemporáneos, y sugiere mejoras prácticas que se pueden implementar para proteger los activos tecnológicos clave.

Espionaje cibernético y marcos legales

Como se ha mencionado, la ciberseguridad ha emergido como un dominio crítico en el contexto de múltiples tensiones entre actores globales, particularmente entre actores occidentales y China, donde el ciberespionaje se ha posicionado en el centro de las estrategias de inteligencia y de la carrera tecnológica (Hannas y Tatlow, 2020). A medida que China toma acciones encaminadas a extender su influencia tecnológica global, el ciberespionaje se ha revelado como una herramienta esencial en su arsenal, lo que ha provocado repercusiones significativas para las empresas y la infraestructura crítica occidentales (Nasheri, 2023). Ejemplo de esto fue el impacto que tuvieron en el sector automotriz las tensiones sobre los semiconductores y, años atrás, las sanciones impuestas a la firma Huawei por Estados Unidos y Canadá, que afectaron a otros socios comerciales y proyectos de infraestructura (Innovation, 2022; Kaska et al., 2019; Martín Porras, 2022). En este escenario, los marcos legales internacionales enfrentan el desafío de adaptarse y responder a las crecientes amenazas que representan estas actividades clandestinas (Buchan y Navarrete, 2021; Stupak, 2023).

Esta sección explora la naturaleza del espionaje cibernético chino, se analizan algunas de las técnicas que mayor impacto han tenido y cómo afectan a las empresas occidentales. Además, se examina la estructura y eficacia de las regulaciones internacionales diseñadas para mitigar el impacto del ciberespionaje, y se evalúa su capacidad para mantenerse actualizadas frente a las rápidas evoluciones tecnológicas. Este abordaje busca ofrecer una visión integral del paisaje actual del ciberespionaje y su regulación, y subraya tanto los desafíos como las posibles soluciones en el ámbito de la seguridad digital global.



Naturaleza del espionaje cibernético chino

El espionaje cibernético ejecutado por China constituye una pieza angular de su estrategia geopolítica y económica, al ejercer una presión adicional considerable sobre las empresas privadas occidentales (Hannas y Tatlow, 2020). Mediante un repertorio sofisticado de técnicas de ciberspionaje, el objetivo de China no se limita solo a acumular información gubernamental y militar, sino que se extiende significativamente hacia la apropiación de secretos comerciales y tecnológicos (Lara, 2022). Este actuar está encaminado a acelerar su ascenso en la economía global y así consolidar su posición como líder tecnológico.

Bajo este entendido, se ha encontrado una táctica recurrente en el arsenal de ciberspionaje chino, el *phishing* (“Empresa China de Ciberspionaje...”, 2024; Team, 2024), que consiste en el envío de correos electrónicos que emulan ser de fuentes fiables para engañar a los destinatarios y obtener acceso a información confidencial. Esta técnica ha evolucionado hacia el *spear phishing*, caracterizado por ataques altamente personalizados dirigidos a individuos específicos, lo que incrementa dramáticamente su efectividad. Además, el despliegue de programas maliciosos (*malware*) avanzados permite a los agentes chinos mantener un acceso prolongado y no detectado a las redes empresariales occidentales y extraer información sensible de forma continua.

Otro método consiste en el uso estratégico de las redes sociales para recopilar datos personales y profesionales (Bennet, 2014; Sambaluk, 2019). Operativos chinos crean perfiles ficticios, que aparentan ser colegas o profesionales del mismo campo, para establecer relaciones de confianza con sus objetivos. A través de estas interacciones, los agentes pueden distribuir enlaces infectados o archivos comprometidos que, una vez abiertos, pueden desencadenar la infección de los sistemas informáticos de la víctima (Kara, 2022).

Estos métodos de ciberspionaje son complementados mediante la explotación de vulnerabilidades en softwares populares entre las empresas occidentales. Los *hackers* chinos buscan activamente fallos de seguridad en aplicaciones y sistemas ampliamente utilizados por empresas globales. Al identificar y explotar estas debilidades, los atacantes pueden infiltrarse en las redes corporativas y acceder a valiosa información empresarial sin necesidad de interacción directa o conocimiento de los usuarios.

El impacto de estas actividades de espionaje en las empresas occidentales es considerable. El robo de propiedad intelectual y datos de investigación y desarrollo no solo permite a China mejorar su competitividad en el mercado global, sino que además socava directamente a las empresas que han invertido recursos significativos en desarrollo e innovación (Sadok et al., 2020). Este tipo de ciberataques



representa una amenaza directa a la estabilidad financiera y estratégica de las empresas afectadas, al tiempo que plantea desafíos mayores en términos de seguridad nacional para los países occidentales (Segal, 2020).

Además, el ciberespionaje chino introduce una incertidumbre significativa y eleva los riesgos dentro de las operaciones empresariales, lo que obliga a las compañías a realizar inversiones considerables en la fortificación de sus sistemas cibernéticos y en la mitigación de posibles amenazas (Crosston, 2020; Tzenios, 2023). Este incremento en los costos de seguridad afecta los márgenes de beneficio, pero también puede distorsionar las estrategias de negocio y desarrollo tecnológico, lo cual pone en desventaja a las empresas frente a sus competidores que pueden no estar sujetos a un riesgo similar (Rugina, 2023).

El ciberespionaje, además, erosiona la confianza dentro de los ecosistemas empresariales internacionales. Las empresas que se ven afectadas por intrusiones significativas pueden sufrir daños reputacionales, pérdida de confianza por parte de clientes y socios, así como posibles repercusiones legales y regulatorias si no logran proteger adecuadamente los datos de sus usuarios (Schneider, 2022), lo cual puede llevar a un ciclo recurrente en el que la inseguridad fomenta más inseguridad, creando un ambiente empresarial global menos confiable y más volátil, propenso a caer en dinámicas especulativas (Shandler y Canetti, 2024).

Frente a este complejo escenario, la necesidad de una respuesta coordinada y robusta es más crítica que nunca. Las empresas deben mejorar sus defensas cibernéticas internas, y también deben colaborar estrechamente con los gobiernos y otras entidades para desarrollar un enfoque más holístico y multilateral hacia la ciberseguridad (Shandler y Gomez, 2023). Este enfoque debería incluir el fortalecimiento de las regulaciones internacionales, el aumento de la cooperación entre los países y el desarrollo de nuevas tecnologías que puedan ofrecer protecciones más avanzadas contra las sofisticadas tácticas de espionaje cibernético.

Por lo tanto, es imperativo que las entidades públicas y privadas trabajen juntas para abordar estos desafíos de manera efectiva, para fortalecer las defensas internas y abogar por cambios en el marco regulatorio internacional. De esta forma, se pueden establecer barreras más efectivas contra el espionaje cibernético y garantizar un entorno empresarial más seguro y equitativo.

Así, se subraya la importancia de una estrategia integrada que combata la amenaza inmediata del ciberespionaje, y que también aborde sus raíces más profundas y sus amplias implicaciones geopolíticas, para conseguir marcos vinculantes que promuevan competencias sanas y simétricas.



Regulaciones internacionales

Con respecto a las regulaciones en el terreno del ciberespacio, el marco legal internacional cumple un papel crucial en la regulación de actividades como el ciberspionaje y el cibercrimen. Los marcos legales existentes se enfrentan a desafíos significativos a medida que la tecnología se desarrolla con mayor velocidad, pues deben mantenerse al día con las innovaciones y las tácticas cambiantes de actores estatales y no estatales (Rowe, 2020).

Por ende, en el principal cuerpo de leyes internacionales que aborda el ciberspionaje se incluyen convenios como la Convención de Budapest sobre Ciberdelincuencia, el primer tratado internacional destinado a combatir los delitos informáticos mediante la armonización de las leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre los países firmantes (Council of Europe, 2001; NIC Argentina, 2017).

Adicionalmente, los ataques a infraestructuras críticas, como en el caso de Estados, dan cuenta de deficiencias en las respuestas internacionales y la aplicación de la ley (Niglia, 2016; Yong, s. f.). Este es solo uno de los ejemplos que ilustran de manera concreta los retos que enfrentan las naciones al intentar coordinar respuestas a través de fronteras y sistemas legales diversos, y cómo estos esfuerzos pueden ser socavados por falta de cooperación o de recursos suficientes.

Así, la eficacia de este y otros marcos legales se ve desafiada por varias razones. Primero, la jurisdicción es un problema importante, en tanto el ciberespacio no conoce fronteras físicas, y esto significa que un ataque puede ser iniciado desde cualquier lugar, lo que complica la trazabilidad y, en consecuencia, la debida aplicación de la ley (Kose, 2021). Esto es particularmente problemático cuando los ataques provienen de países que no tienen acuerdos de cooperación en materia de ciberseguridad o que ven el ciberspionaje como una extensión de su política exterior y seguridad nacional (Caravelli y Jones, 2019; Crosston, 2020).

Además, la velocidad de la evolución tecnológica supera con creces la capacidad de las instituciones para legislar y adaptarse. Un claro ejemplo son las tecnologías emergentes como la IA y el aprendizaje automático, que están remodelando el panorama del ciberspionaje, y permiten ataques más sofisticados y difíciles de detectar. Estos desarrollos plantean retos mayúsculos para los marcos legales, la mayoría de los cuales se redactaron cuando las capacidades tecnológicas actuales eran inimaginables (Devanny et al., 2021; Zhao, 2019).

Así, para comprender mejor el impacto de las tecnologías emergentes en el ciberspionaje, es crucial entender de qué manera herramientas como la inteligencia artificial y el aprendizaje automático facilitan la automatización de ataques a



gran escala y permiten además a los atacantes mejorar la eficacia del *phishing* y el *malware* a través del análisis y la personalización basados en *big data* (Crosston, 2020; Kara, 2022; Rawat et al., 2021). Este enfoque tecnológico avanzado significa que los marcos legales deben adaptarse tanto a lo que es tecnológicamente posible hoy, como también a lo que será posible mañana, lo cual requiere una respuesta base legislativa que pueda anticipar y moldear futuros desarrollos tecnológicos.

La eficacia de los marcos legales también se ve comprometida por la falta de un consenso global sobre qué constituye un acto de ciberespionaje. Mientras que algunos países tienen definiciones bien desarrolladas y legislación específica, otros carecen de claridad legal y recursos para hacer cumplir las leyes existentes. Esta disparidad dificulta la cooperación internacional y permite a los actores maliciosos sacar provecho de las lagunas legales (Moulin, 2023).

En respuesta a esta problemática, organizaciones internacionales y coaliciones de países han empezado a promover normas de comportamiento y a establecer directrices para la operación en el ciberespacio. Iniciativas como el Grupo de Expertos Gubernamentales de las Naciones Unidas sobre Avances en la Tecnología de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, trabajan para desarrollar un marco de comportamiento responsable de los Estados en el ciberespacio (Cristani, 2021; Pehlivan, 2018).

Sin embargo, la aplicación práctica de estas recomendaciones es irregular y, a menudo, carece de mecanismos de cumplimiento efectivos o vinculantes (Moulin, 2023; Shull, 2019). Y como la eficacia de las regulaciones internacionales en el ciberespacio depende en gran medida de la voluntad política de los países para cooperar y comprometerse con un entorno cibernético más seguro y regulado, se resalta la necesidad de que las regulaciones puedan establecer el terreno para la cooperación. Instituir normas de comportamiento con rapidez estratégica respecto a la rapidez de los avances tecnológicos y la naturaleza global del ciberespionaje, requiere enfoques más dinámicos y adaptativos para ser efectivamente gestionados (Banks, 2014).

En consonancia, resulta esencial conectar estas iniciativas con las estrategias defensivas occidentales que se mencionan en secciones subsiguientes. Por ejemplo, las directrices propuestas por grupos de expertos se pueden adoptar como parte de políticas nacionales que refuerzan la seguridad cibernética a nivel empresarial y gubernamental, lo que permitiría una sinergia entre la ley internacional y las políticas locales, crucial para formar un frente unido contra las amenazas del ciberespionaje (Banks, 2014; Jones, 2020; Pehlivan, 2018).

Dada la velocidad de las innovaciones tecnológicas y los desafíos que plantean para los marcos legales tradicionales, es imperativo que las estrategias de respuesta, que se detallan en las siguientes secciones, consideren cómo los avances



tecnológicos se pueden anticipar y regular eficazmente, ya que al hacerlo se mejora la respuesta a incidentes de ciberspionaje y se fortalece la infraestructura legal y técnica necesaria para prevenir futuros ataques.

Tácticas de espionaje y respuestas occidentales

En el ámbito de la seguridad global cibernética, las tácticas de espionaje de China han evolucionado de forma exponencial, lo que afecta profundamente a empresas y gobiernos occidentales (Frazier y Frazier, 2020; Hansen, 2020; Rugina, 2023; Tzenios, 2023). En la presente sección se aborda la manera en la que China ha puesto en práctica estrategias de ciberspionaje avanzadas, destacando incidentes recientes que ilustran la magnitud y la sofisticación de sus operaciones. Adicionalmente, se describen casos específicos que han impactado sectores críticos en Occidente, desde la tecnología y la defensa hasta la infraestructura esencial, que revelan la extensión del espionaje dirigido a apropiarse de secretos comerciales y tecnológicos vitales (Kose, 2021; Tzenios, 2023).

Además, se describen algunas respuestas de los países occidentales, que incluyen desde políticas gubernamentales actualizadas hasta colaboraciones estratégicas multisectoriales (Bogdanoski, 2022; Dalby, 2020). Estas medidas no solo buscan contrarrestar el espionaje directo, sino también fortalecer la resiliencia general frente a las amenazas cibernéticas, y resaltan la importancia de una defensa ágil, integrada y rápidamente adaptable con respecto a los desafíos que impone el ciberespacio.

Estrategias de espionaje de China

Es necesario mencionar que la sofisticación de las estrategias de espionaje cibernético por parte de China ha marcado una evolución significativa en la manera en que se llevan a cabo las operaciones de inteligencia (Crosston, 2020; Gioe et al., 2020; Layton, 2020). Más allá del *phishing* y el *malware*, que siguen siendo herramientas prevalentes, China ha puesto en práctica técnicas más avanzadas que plantean amenazas directas a la seguridad nacional y empresarial de los países occidentales y a la estabilidad económica, comercial y financiera.

Al respecto, hay que mencionar el uso de ataques de *watering hole*, una metodología que infecta sitios web visitados frecuentemente por empleados de empresas objetivo para luego comprometer las redes corporativas a través de estos usuarios incautos (Lemay et al., 2018; Lohani, 2019). Este método ha sido refinado con el tiempo, y ha permitido a los operativos chinos no solo infectar sistemas, sino también pasar inadvertidos en las redes durante períodos prolongados para la extracción continua de información.



Otra estrategia reciente es el *supply chain attack*, mediante el cual los adversarios se infiltran en los proveedores o socios comerciales que tienen conexiones menos seguras con los principales objetivos (Guacaneme, 2021; Stupak, 2023). Estos ataques han resultado en violaciones de seguridad significativas que afectan a múltiples empresas a través de un único punto de entrada comprometido. La magnitud de estos ataques fue puesta de manifiesto en el incidente con SolarWinds que, aunque no atribuido oficialmente a China, ejemplifica la vulnerabilidad de las cadenas de suministro en un contexto globalizado (Jibilian y Canales, 2021; Oladimeji y Kerner, 2023).

La IA también ha sido adoptada para mejorar las capacidades de espionaje (Montes, 2023; Rawat et al., 2021). China ha desarrollado y desplegado algoritmos de IA que automatizan la recolección y el análisis de enormes volúmenes de datos extraídos de diversas fuentes (Xu et al., 2020). Estos sistemas de IA aumentan la eficiencia del espionaje y permiten realizar ataques dirigidos con un grado de precisión antes impensable, como incluir el reconocimiento facial y el análisis comportamental en tiempo real para identificar patrones de conducta de objetivos potenciales (Sandoval-Paucar et al., 2020).

El impacto de estas estrategias de espionaje sobre la seguridad occidental es profundo y multidimensional. En términos de seguridad nacional, el espionaje chino ha afectado la integridad de la información clasificada y las operaciones de defensa y ha forzado a los gobiernos a revisar sus protocolos de seguridad y colaboración entre agencias e industrias (Rivera et al., 2022).

A nivel empresarial, la filtración de secretos industriales y propiedad intelectual ha conducido a pérdidas económicas sustanciales y ha debilitado la ventaja competitiva de numerosas compañías (Banks, 2014; Frazier y Frazier, 2020). Además, la incertidumbre que generan estas actividades de espionaje ha llevado a reevaluar las estrategias de seguridad cibernética, y ha impulsado a las empresas a invertir cuantiosas sumas en tecnologías defensivas avanzadas y en la formación de personal especializado en seguridad informática (Addington y Manrod, 2019; Gordon et al., 2015).

Estos desarrollos subrayan la necesidad de una vigilancia continua y de un enfoque proactivo para contrarrestar las estrategias de espionaje de China, lo cual implica tanto a entidades gubernamentales como a corporaciones privadas en un esfuerzo conjunto para proteger los activos críticos nacionales e internacionales y velar por un mercado simétrico y en equilibrio.



Contramedidas occidentales

En respuesta al creciente desafío del ciberspionaje chino, Occidente ha puesto en práctica una serie de contramedidas para proteger la seguridad nacional como también los intereses empresariales (Hiller y Russell, 2013; Levite et al., 2022). Estas respuestas destacan la necesidad de una colaboración estrecha entre el sector público y el privado, ya que la interconexión de infraestructuras críticas y sistemas corporativos hace que ambos sectores sean vulnerables (Niglia, 2016).

Una de las principales estrategias ha sido el fortalecimiento de la ciberdefensa nacional a través de la creación de agencias y unidades especializadas en ciberseguridad. En Estados Unidos, por ejemplo, la Cybersecurity and Infrastructure Security Agency (CISA) trabaja en estrecha colaboración con el sector privado para mejorar la resiliencia cibernética en sectores críticos, proporcionando evaluaciones de riesgo, asesoramiento sobre amenazas emergentes y apoyo en la respuesta a incidentes, lo que facilita una defensa coordinada contra operaciones de ciberspionaje complejas (CISA, 2024).

Adicionalmente, se ha fomentado la implementación de marcos normativos más rigurosos para la protección de datos y la seguridad cibernética. La Unión Europea (UE), con su Reglamento General de Protección de Datos (GDPR), ha establecido un precedente en términos de exigencias de seguridad para empresas que operan dentro de sus fronteras, incluyendo aquellas que podrían ser blancos de espionaje (Comisión Europea, 2021). Dichas regulaciones llevan a las empresas a adoptar medidas de seguridad más estrictas y a reportar brechas de datos de manera oportuna, lo que contribuye a la mitigación de los efectos del ciberspionaje.

Un pilar fundamental ha sido la colaboración público-privada en el intercambio de inteligencia sobre amenazas (Bosson y Wagner, 2018). Iniciativas como los Information Sharing and Analysis Centers (ISACs) en varios sectores industriales permiten a las empresas compartir información sobre amenazas y vulnerabilidades de manera confidencial (ENISA, s. f.). Este intercambio de información ha posibilitado, en algunos casos, anticipar y neutralizar los métodos de espionaje antes de que causen daño significativo, probando ser una herramienta eficaz en la detección y respuesta temprana a incidentes cibernéticos.

De igual forma, la cooperación internacional cumple un papel determinante en la lucha contra el ciberspionaje. Diversos países occidentales han buscado fortalecer alianzas a través de organizaciones como la OTAN y grupos de cooperación internacional en ciberseguridad, donde se comparten mejores prácticas, capacidades de respuesta y estrategias defensivas (Addington y Manrod, 2019; Montes, 2023). De esta forma, mejora la capacidad particular de cada nación para defenderse contra el espionaje cibernético y se fortalece la seguridad colectiva, lo que



permite establecer frentes unidos contra los adversarios y peligros comunes. Estas contramedidas y estrategias dan cuenta de que enfoques multinivel funcionan en la lucha para contrarrestar el espionaje cibernético chino, lo cual llama la atención sobre la importancia de la colaboración entre diferentes sectores y naciones para proteger los activos críticos de Occidente de amenazas emergentes y en evolución.

Fortalecimiento de la ciberseguridad

Ante estos desafíos, resulta crucial poder adoptar medidas robustas para fortalecer conjuntamente la ciberseguridad en el mundo. Este fortalecimiento requiere una mejora significativa en la protección de la información y el desarrollo de tecnologías de defensa avanzadas dentro de las fronteras nacionales, pero sobre todo a través de la cooperación internacional (Bogdanoski, 2022; CISA, 2024; Hiller y Russell, 2013).

Las empresas de todos los sectores están incrementando su dependencia de las tecnologías digitales, por lo tanto, se exponen a nuevas vulnerabilidades y riesgos (Caprolu et al., 2021; Nasheri, 2023). En este contexto, resulta imperativo poner en práctica soluciones tecnológicas avanzadas y estrategias de seguridad bien definidas y delimitadas que permitan la defensa integral contra amenazas cibernéticas. Además, la colaboración entre países y la integración de esfuerzos en materia de investigación y desarrollo pueden acelerar la creación de herramientas de seguridad cibernética más efectivas, para garantizar un entorno empresarial más seguro. Por ello, en el siguiente acápite se exploran propuestas para mejorar la seguridad de la información y se enfatiza en la necesidad de la cooperación internacional para hacer frente a los retos del ciberespacio.

Mejoras en la seguridad de la información

Como se ha evidenciado, la protección de la información sensible se ha vuelto una prioridad estratégica para las empresas de todos los sectores (Sadok et al., 2020; Stupak, 2023). La implementación de tecnologías avanzadas y técnicas efectivas de seguridad es fundamental para salvaguardar activos estratégicos frente a las crecientes amenazas de ciberataques (Gordon et al., 2015).

Una de las técnicas más eficaces para mejorar la seguridad de la información es la encriptación de datos, que protege la información no solo durante su almacenamiento, sino también durante la transmisión, y asegura que cualquier dato interceptado no se pueda descifrar sin la clave correspondiente. Las empresas, especialmente aquellas que operan en sectores como las finanzas y la salud, donde se manejan grandes volúmenes de información personal y sensible, están poniendo



en práctica políticas de encriptación robustas para proteger la confidencialidad y la integridad de sus datos (Akoto, 2024; Caprolu et al., 2021).

Otra tecnología clave es la autenticación multifactor (MFA, por sus siglas en inglés), que proporciona una capa adicional de seguridad al exigir múltiples formas de verificación antes de permitir el acceso a los sistemas críticos (Herrmann, 2019; Kara, 2022). Esta técnica reduce de manera significativa el riesgo de accesos no autorizados que resultan de contraseñas robadas o comprometidas. Sectores como el bancario y el gubernamental han adoptado ampliamente la MFA para proteger sus infraestructuras de información crítica (Ecclesie, 2020).

Otra estrategia efectiva es la segmentación de redes, la cual implica dividir las redes corporativas en segmentos más pequeños para controlar mejor el acceso y reducir la superficie de ataque (Sharma, 2022; Wasicek, 2020). Al aislar los sistemas críticos de las partes menos seguras de la red, las empresas pueden limitar el daño potencial en caso de una brecha de seguridad. Este enfoque es particularmente relevante en industrias como la manufactura y la energía, donde la protección de las infraestructuras críticas es vital para la continuidad operativa (CISA, 2024; Rawat et al., 2021; Warfield, 2012).

Finalmente, la implementación de sistemas de detección y respuesta a incidentes (IDR, por sus siglas en inglés) se ha vuelto esencial. Estos sistemas utilizan técnicas avanzadas de monitoreo y análisis para detectar actividades sospechosas en tiempo real y responder a incidentes de seguridad de manera rápida y efectiva (IBM, 2023). Las empresas de tecnología y telecomunicaciones lideran la adopción de estas tecnologías y las integran con IA para mejorar la precisión y la velocidad de respuesta ante amenazas cibernéticas.

La adopción de estas tecnologías y técnicas en diferentes sectores industriales mejora la protección de la información sensible y fomenta una cultura de seguridad entre las empresas, crucial para enfrentar los desafíos del ciberespacio (Addington y Manrod, 2019; Levite et al., 2022). Al invertir en tecnologías avanzadas y adaptarlas a las necesidades específicas de cada sector, las empresas pueden fortalecer significativamente su postura de seguridad cibernética.

Desarrollo de nuevas tecnologías de defensa cibernética

El desarrollo de nuevas tecnologías de defensa cibernética es crucial en un mundo donde las amenazas cibernéticas evolucionan con rapidez y presentan desafíos cada vez más sofisticados y difíciles de contrarrestar. Esta necesidad impulsa la innovación continua en áreas como la IA, el aprendizaje automático y la computación cuántica, que están redefiniendo las estrategias de defensa en el ciberespacio (Layton, 2020; Sarker, 2021).



La IA y el aprendizaje automático, en particular, se hallan a la vanguardia de esta innovación y proporcionan la capacidad de detectar amenazas en tiempo real y responder a ellas con una precisión y una velocidad que superan las capacidades humanas (Rawat et al., 2021; Rosli et al., 2021). Estas tecnologías permiten crear sistemas de defensa que identifican patrones de ataques conocidos, pero que además aprenden de interacciones pasadas y mejoran continuamente su capacidad para prever y mitigar ataques futuros (Weinberg y Faccia, 2024).

Asimismo, la computación cuántica promete revolucionar la seguridad cibernética porque ofrece nuevas formas de encriptación que podrían hacer inquebrantables los datos frente a los métodos de descifrado tradicionales (Brijwani et al., 2023; Hadi et al., 2024). Aunque esta tecnología aún se halla en sus etapas iniciales, su potencial para asegurar comunicaciones y proteger datos a una escala completamente nueva es inmenso, lo cual ha impulsado inversiones significativas en investigación y desarrollo de entidades tanto estatales como privadas.

El papel de la cooperación internacional en el desarrollo de estas tecnologías es esencial. Iniciativas globales y acuerdos bilaterales entre países facilitan el intercambio de conocimientos y recursos, al tiempo que establecen normas comunes que ayudan a combatir amenazas cibernéticas de manera unificada y efectiva (Comisión Europea, 2021; Cristani, 2021; Realpe y Cano, 2020; ENISA, s. f.). Por ejemplo, la cooperación en la UE, a través de proyectos como el Programa Horizonte 2020, fomenta la investigación y el desarrollo en ciberseguridad y apoya la creación de soluciones innovadoras que benefician a múltiples países miembros (González y Jasmontaite, 2020; Kopchev, 2019).

Estos esfuerzos colaborativos avanzan en el desarrollo técnico de nuevas tecnologías y fortalecen las relaciones políticas y económicas entre los Estados, con lo cual se genera un entorno más seguro y estable para la gestión de la ciberseguridad a nivel global (Kovács, 2018). La combinación de innovación tecnológica con estrategias de cooperación bien estructuradas es, por lo tanto, esencial para enfrentar los retos del ciberespacio en el futuro cercano.

Estrategias globales y cooperación internacional

La creciente interdependencia digital global subraya la importancia de fortalecer la cooperación internacional para combatir el ciberespionaje eficazmente (Sadok et al., 2020; Trim y Lee, 2021). A medida que el ciberespacio se convierte en un ámbito crítico de conflicto y competencia, no solo entre Estados, sino también entre entidades no estatales y sectores empresariales, la necesidad de un enfoque colaborativo y coordinado se hace más evidente (Rosli et al., 2021; Sarker, 2021; Sharma, 2022).



Esta colaboración internacional se enfoca en compartir inteligencia y recursos, como también en unificar estrategias de seguridad digital para proteger tanto los intereses nacionales como los del sector empresarial global. Al integrar esfuerzos, los países y las corporaciones pueden crear un escudo más robusto contra las tácticas de espionaje que, a menudo, sobrepasan las capacidades de un solo Estado o empresa para responder eficazmente. En este contexto, la colaboración resulta ser la piedra angular para el desarrollo de defensas cibernéticas que se anticipen a las amenazas y las neutralicen de manera proactiva, y así asegurar la integridad y la confianza en las infraestructuras críticas a nivel mundial.

Estrategias de seguridad digital global

En el contexto del ciberspionaje global, la integración de estrategias de seguridad digital sin importar las fronteras se ha vuelto imperativa (Caravelli y Jones, 2019). Las amenazas cibernéticas no reconocen límites geográficos, de ahí que la cooperación internacional sea esencial para una defensa efectiva. Esta cooperación permite compartir mejores prácticas, recursos y tecnologías avanzadas para construir una resistencia colectiva más robusta (Kovács, 2018; Montes, 2023).

Un ejemplo destacado de esfuerzos internacionales en la seguridad cibernética es la cooperación entre países miembros de organizaciones como la OTAN y la UE, donde se promueve activamente el intercambio de información y estrategias para combatir el ciberspionaje (Kovács, 2018), lo cual ha fomentado la creación de equipos multidisciplinarios y centros de respuesta ante incidentes cibernéticos que operan a través de fronteras internacionales. Esta estructura de cooperación permite respuestas más coordinadas y efectivas frente a amenazas cibernéticas y demuestra la importancia de la sinergia global para una defensa cibernética robusta.

La colaboración internacional no se limita a la gestión de crisis, también abarca el desarrollo de marcos legales y técnicos que ayuden a prevenir el ciberspionaje (Banks, 2014; Pehlivan, 2018). La Iniciativa Global de Ciberseguridad, por ejemplo, ha contribuido a establecer normas y protocolos que se han adoptado en varias jurisdicciones, y ha facilitado una acción coordinada y consistente frente a los ciberdelincuentes. Estas normativas ayudan a cerrar brechas que podrían ser aprovechadas por espías cibernéticos y fortalecen la infraestructura crítica en todos los sectores (Buchan y Navarrete, 2021).

Además, el refuerzo de la cooperación internacional va más allá del intercambio de información y tácticas defensivas. Se extiende a la inversión conjunta en tecnologías de punta y al desarrollo de recursos humanos a través de programas de capacitación y simulacros que preparan a los equipos de ciberseguridad para enfrentar y neutralizar amenazas en un entorno controlado. La colaboración



en investigación y desarrollo también ha propiciado la creación de tecnologías que pueden detectar patrones de ataques emergentes antes de que causen daño significativo (Mmaduekwe y Mmaduekwe, 2024; Rin, 2023).

Estos esfuerzos conjuntos mejoran la seguridad de las naciones individuales, elevan el estándar de seguridad digital global y crean un entorno más seguro para todos los actores en el panorama internacional. La lucha contra el ciberespionaje, por tanto, es un esfuerzo colectivo que requiere un compromiso sostenido y una estrategia bien integrada a nivel mundial.

Refuerzo de la cooperación internacional

El fortalecimiento de la cooperación internacional es crucial para abordar responsablemente la complejidad y el alcance del ciberespionaje, un desafío que trasciende las fronteras nacionales (UNODC, 2019). Esta cooperación no se debe considerar solo como un intercambio de información, sino como una plataforma integrada que involucra múltiples sectores y actores globales para desarrollar una respuesta unificada y eficaz contra las amenazas cibernéticas.

Una propuesta para mejorar esta colaboración es la creación de un marco de acción internacional que incluya protocolos de actuación rápida en caso de ataques cibernéticos que afecten a múltiples naciones (Boussi y Gupta, 2020). Este marco podría basarse en el desarrollo de centros de operaciones de seguridad cibernética compartidos, donde expertos de diferentes países trabajen conjuntamente en la monitorización de amenazas, la respuesta a incidentes y la recuperación posataque (IBM, 2023; Tropina, 2020). La eficiencia de tales centros sería mayor mediante el uso compartido de herramientas avanzadas de detección y respuesta y la implementación de programas de formación continua que preparen a los técnicos para enfrentar las tácticas cambiantes de los ciberdelincuentes.

Otra medida para tener en cuenta es la firma de tratados bilaterales y multilaterales que comprometan a los países a cooperar en la investigación y persecución de delitos cibernéticos (Tropina, 2020; Tsakalidis et al., 2018). Estos tratados deberían incluir cláusulas que faciliten la extradición rápida de ciberdelincuentes y la colaboración judicial transfronteriza para resolver los problemas de jurisdicción que a menudo complican las investigaciones de ciberespionaje (Macidov, 2023; Sekati, 2022). Además, es fundamental que estos tratados promuevan el desarrollo de normativas comunes para proteger los datos y la privacidad, con el fin de estandarizar las medidas de seguridad a nivel internacional y cerrar las brechas legales que los actores malintencionados puedan explotar (Tóth y Gáspár, 2020).

Por lo mismo, se deben fomentar alianzas más estrechas entre el sector público y el privado, ya que el rol de las empresas tecnológicas es crucial en la seguridad cibernética, al poseer la experiencia y los recursos para desarrollar soluciones avan-



zadas en materia de seguridad. En este sentido, la colaboración puede tomar la forma de asociaciones público-privadas que impulsen la innovación en tecnologías de defensa cibernética, de modo que el sector público pueda beneficiarse de las capacidades del sector privado en términos de agilidad e innovación o mejoramiento.

Estas propuestas mejorarían la capacidad de respuesta ante el ciberspionaje y fortalecerían además la confianza entre los países y entre los sectores, con lo cual la infraestructura global de información sería más resiliente y segura. Al profundizar en la cooperación y en la integración de estrategias, el mundo puede esperar un enfoque más coordinado y eficiente para protegerse contra las amenazas cibernéticas.

Conclusiones

La presente investigación ha permitido profundizar en las dinámicas del ciberspionaje chino y sus implicaciones para la seguridad y competitividad occidentales. Los hallazgos clave destacan cómo las tensiones económicas y comerciales entre Occidente y China han intensificado las actividades de ciberspionaje y han afectado gravemente a las empresas y las infraestructuras críticas occidentales. Además, se ha puesto en evidencia la necesidad urgente de reforzar los marcos legales internacionales y mejorar la cooperación global para enfrentar estas amenazas de manera más efectiva.

A continuación, se proponen algunas recomendaciones dirigidas a los responsables de la formulación de políticas, líderes empresariales y de opinión y a la comunidad internacional, enfocadas en fortalecer las estrategias de ciberseguridad y mejorar la respuesta frente al espionaje tecnológico chino. Estas recomendaciones buscan fomentar un entorno digital más seguro y resiliente, con el fin de mitigar las amenazas actuales y establecer una base sólida para la seguridad cibernética futura.

A lo largo de este estudio, se han identificado varios hallazgos cruciales que logran poner el foco sobre la magnitud y sofisticación del ciberspionaje chino, y sobre sus extensas repercusiones para la seguridad occidental y la estabilidad global. Primero, se ha descrito cómo China emplea una combinación avanzada de tácticas de ciberspionaje, que incluyen *phishing*, *malware* y explotación de vulnerabilidades de software, entre otras herramientas, lo que resalta su enfoque estratégico y adaptativo para obtener ventajas competitivas en la economía global.

Uno de los principales hallazgos es la correlación directa entre las tensiones geopolíticas y la intensificación del ciberspionaje chino, especialmente en sectores tecnológicamente avanzados y de infraestructuras críticas. Este actuar no solo busca extraer información valiosa, sino también debilitar la capacidad competitiva



de Occidente, lo cual tiene profundas implicaciones para la política internacional y la seguridad económica.

Además, se ha resaltado la necesidad imperativa de fortalecer los marcos legales internacionales y la cooperación interestatal para combatir eficazmente estas amenazas. En cuanto hay una amplia zona gris respecto a la actual legislación internacional, aunada a la falta de uniformidad en las respuestas nacionales, se hace evidente que ha habido un alto grado de permisividad que ha fomentado el florecimiento del ciberespionaje sin controles efectivos. Este estudio subraya la urgencia de establecer normativas más robustas y mecanismos vinculantes de cumplimiento que puedan adaptarse a la velocidad de la innovación tecnológica.

Estos hallazgos contextualizan sobre la necesidad significativa de formular nuevas políticas y prácticas de ciberseguridad. Por un lado, enfatizan la importancia de una vigilancia continua y la inversión en defensas cibernéticas avanzadas que puedan detectar y neutralizar amenazas en tiempo real. Por otro lado, sugieren que las estrategias de seguridad no deben centrarse únicamente en la protección y respuesta, sino también en la creación de un entorno colaborativo internacional que promueva el intercambio de información y recursos para fortalecer la resiliencia global frente a los ciberataques.

En otras palabras, este estudio ofrece una panorámica del estado actual del ciberespionaje y su impacto, y proporciona una base para el desarrollo de políticas más informadas y efectivas que puedan anticipar y contrarrestar las estrategias emergentes de espionaje cibernético. En consecuencia, para abordar los desafíos identificados en este estudio sobre el ciberespionaje y mejorar la ciberseguridad global frente a las crecientes amenazas, se recomiendan las siguientes estrategias específicas:

Fortalecimiento de las capacidades de detección y respuesta: es imperativo que los países occidentales inviertan en tecnologías avanzadas de detección de amenazas y en el desarrollo de equipos de respuesta rápida ante incidentes cibernéticos. Esto incluye la utilización de IA y aprendizaje automático para mejorar la capacidad de los sistemas de seguridad, con el fin de detectar patrones de ataque y responder de manera proactiva antes de que se materialicen los daños.

Formación y concienciación continuadas: ampliar los programas de formación en ciberseguridad para empleados de todos los niveles en las organizaciones, desde el personal ejecutivo hasta el operativo. La concienciación sobre las tácticas de ciberespionaje y la capacitación en las mejores prácticas de seguridad digital son fundamentales para fortalecer la primera línea de defensa contra los ataques cibernéticos.

Desarrollo de un marco regulatorio más robusto: promover la creación y actualización de legislaciones que persigan el ciberespionaje, y que faciliten además la



colaboración internacional en la persecución de los ciberdelincuentes. Esto incluye la revisión de tratados existentes, como la Convención de Budapest, para incluir disposiciones que aborden las nuevas tecnologías y métodos de espionaje.

Cooperación internacional mejorada: establecer y fortalecer alianzas internacionales que permitan un intercambio fluido de información sobre amenazas cibernéticas y mejores prácticas de mitigación. Esto debería incluir la creación de plataformas compartidas para el análisis de ciberamenazas y la ejecución de ejercicios cibernéticos conjuntos que preparen mejor a los países para enfrentar ataques coordinados.

En términos de investigación futura y desarrollo de políticas, se sugiere:

Investigación en ciberinteligencia adaptativa: fomentar la investigación en el campo de la ciberinteligencia para desarrollar sistemas que puedan adaptarse y responder a la rápida evolución de las tácticas de espionaje. Este esfuerzo debería centrarse en el análisis predictivo y en la modelización de amenazas basada en IA.

Evaluación de la eficacia de las políticas de ciberseguridad: realizar estudios continuos que evalúen la efectividad de las políticas y estrategias de ciberseguridad implementadas a nivel nacional e internacional, con el fin de ayudar a identificar áreas de mejora y facilitar la actualización de las estrategias en tiempo real frente a las amenazas emergentes.

Desarrollo de tecnologías de defensa avanzadas: impulsar la innovación en el desarrollo de nuevas tecnologías de defensa cibernética que puedan contrarrestar las capacidades avanzadas de ciberspionaje, lo que incluye inversiones en criptografía cuántica y seguridad de infraestructura crítica.

La aplicación práctica de estas recomendaciones requiere un compromiso coordinado entre gobiernos, la industria privada y la academia para lograr un entorno digital más seguro y resistente frente al espionaje tecnológico y otras formas de ciberataques.

Referencias

- Addington, D., y Manrod, M. (2019). Cyber security threats and solutions for the private sector. In M. Gueldry, G. Gokcek y L. Hebron (eds.), *Understanding new security threats*. London: Routledge.
- Akoto, W. (2022). Cyber economic espionage: A framework for future research. In D. Deese (ed.), *A Research Agenda for International Political Economy* (pp. 159-170). Edward Elgar Publishing. <https://www.elgaronline.com/edcollchap/book/9781800884120/book-part-9781800884120-19.xml>



- Akoto, W. (2024). Who spies on whom? Unravelling the puzzle of state-sponsored cyber economic espionage. *Journal of Peace Research*, 61(1), 59-71. <https://doi.org/10.1177/00223433231214417>
- Banks, W. (October 17, 2014). Cyber Espionage, Surveillance, and International Law: Finding Common Ground. Institute for National Security and Counterterrorism (INSCT), Syracuse University. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2558155
- Bennet, A. (Ed.). (2014). *Social Media: Global Perspectives, Applications and Benefits and Dangers*. New York: Nova Science Publishers.
- Bogdanoski, M. (2022). *Building Cyber Resilience Against Hybrid Threats*. NATO Science for Peace and Security Series - d: Information and Communication Security Series, vol. 61. Amsterdam: IOS Press.
- Bossong, R., y Wagner, B. (2018). A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union. In O. Bures y H. Carrapico (Eds.), *Security Privatization* (pp. 219-247). Springer International Publishing. https://doi.org/10.1007/978-3-319-63010-6_10
- Boussi, G. O., y Gupta, H. (2020). A proposed framework for controlling cyber-crime. 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 1060-1063). Amity University, Noida, India. <https://sci-hub.se/downloads/2020-11-02/fc/boussi2020.pdf>
- Boylan, B. M., McBeath, J., y Wang, B. (2021). US–China Relations: Nationalism, the Trade War, and COVID-19. *Fudan Journal of the Humanities and Social Sciences*, 14(1), 23-40. <https://doi.org/10.1007/s40647-020-00302-6>
- Brijwani, G. N., Ajmire, P. E., y Thawani, P. V. (2023). Future of quantum computing in cyber security. In A. K. Tyagi (ed.), *Handbook of Research on Quantum Computing for Smart Environments* (pp. 267-298). IGI Global. <https://www.igi-global.com/chapter/future-of-quantum-computing-in-cyber-security/319874>
- Buchan, R., y Navarrete, I. (2021). Cyber espionage and international law. In N. Tsagourias and R. Buchan (eds.), *Research Handbook on International Law and Cyberspace* (pp. 231-252). Edward Elgar Publishing. <https://www.elgaronline.com/edcollchap/edcoll/9781789904246/9781789904246.00021.xml>
- Caprolu, M., Cresci, S., Raponi, S., y Di Pietro, R. (2021). New Dimensions of Information Warfare: The Economic Pillar—Fintech and Cryptocurrencies. In J. Garcia-Alfaro, J. Leneutre, N. Cuppens, & R. Yaich (Eds.), *Risks and Security of Internet and Systems* (Vol. 12528, pp. 3-27). Springer International Publishing. https://doi.org/10.1007/978-3-030-68887-5_1
- Caravelli, J., y Jones, N. (2019). *Cyber Security: Threats and Responses for Government and Business*. Santa Barbara, California: ABC CLIO.
- Ciber 4 All Team (2024, abril 8). Ciberespionaje industrial y robo de secretos empresariales. Tarlogic Security. [Blog]. <https://www.tarlogic.com/es/blog/ciberespionaje-industrial/>



- Comisión Europea. (2021, junio 4). La protección de datos en la UE. Comisión Europea. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es
- Council of Europe. (2001, 11th November). Convention on Cybercrime (ETS No. 185). <https://www.coe.int/en/web/conventions/full-list> [Consultado: 23 de mayo de 2024].
- Cristani, F. (2021). *Economic Cyber-Espionage in the (Post) COVID-19 Era in Europe: Which (new) Challenges?* (PhD Thesis), National Aviation University. <https://dspace.nau.edu.ua/handle/NAU/48736>
- Crosston, M. (2020). Cyber colonization: The dangerous fusion of artificial intelligence and authoritarian regimes. *Cyber, Intelligence, and Security*, 4(1), 149-171. https://www.inss.org.il/wp-content/uploads/2020/04/Cyber4.1ENG_7-151-173.pdf
- Cybersecurity and Infrastructure Security Agency (CISA). (2024). National Security Memorandum on Critical Infrastructure Security and Resilience. America's Cyber Defense Agency. <https://www.cisa.gov/national-security-memorandum-critical-infrastructure-security-and-resilience>
- Dalby, S. (2020). *Anthropocene Geopolitics: Globalization, Security, Sustainability*. University of Ottawa Press.
- De León Nazareno, D. O. (2024). Ciberseguridad en las Relaciones Internacionales: ¿Cómo los ataques cibernéticos pueden crear tensiones internacionales? *Cuadernos de Nuestra América*, (010), 18-30. <http://www.cna.cipi.cu/cna/article/view/192>
- Devanny, J., Martin, C., y Stevens, T. (2021). On the strategic consequences of digital espionage. *Journal of Cyber Policy*, 6(3), 429-450. <https://doi.org/10.1080/23738871.2021.2000628>
- Ecclesie Agazzi, A. (2020). Phishing and Spear Phishing: Examples in Cyber Espionage and techniques to protect against them. *arXiv*. [Internet]. <http://arxiv.org/abs/2006.00577>
- “Empresa china de ciberspionaje es expuesta por filtración de documentos”. (2024, febrero 22). Devel Group [blog]. <https://devel.group/blog/empresa-china-de-ciberspionaje-es-expuesta-por-filtracion-de-documentos/>
- European Union Agency for Cybersecurity, The (ENISA). (s. f.). Information Sharing and Analysis Centers (ISACs) [Topic]. ENISA. <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing> [Consultado: 26 de mayo de 2024].
- Frazier, G. H., y Frazier, M. B. (2020). Taming the Paper Tiger: Deterring Chinese Economic Cyber-Espionage and Remediating Damage to US Interests Caused by Such Attacks. *Southern California Interdisciplinary Law Journal*, 30(33), 33-68.
- García Waldman, D. H., Ortiz Téllez, G. D., y Santos Sánchez, P. G. (2021). El ciber-espionaje como herramienta estratégica de los actores internacionales en la era digital: Una revisión desde la literatura. *Sapienza: International Journal of Interdisciplinary Studies*, 2(4), 136-153. <https://doi.org/10.51798/sijis.v2i4.145>
- Gargiulo, P. (2020). *Militarism, Economics, and Nationalism: The Russian and Chinese Expansionist Foreign Policy of the 21st Century*. (Senior Theses). Fordham University. https://research.library.fordham.edu/international_senior/50



- Gioe, D. V., Goodman, M. S., y Stevens, T. (2020). Intelligence in the cyber era: Evolution or revolution? *Political Science Quarterly*, 135(2), 191-224.
- González Fuster, G., y Jasmontaite, L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The Ethics of Cybersecurity* (pp. 97-115). Springer.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., y Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, 1(1), 3-17.
- Guacaneme Medina, S. (2021). *Fugas de información en el ciberespacio, una nueva amenaza para los Estados*. (Tesis de grado). Universidad Militar Nueva Granada, Bogotá. <https://repository.unimilitar.edu.co/handle/10654/39575> [Consultado: 28 de mayo de 2024].
- Hadi, H. J., Cao, Y., Alshara, M. A., Ahmad, N., Riaz, M. S., y Li, J. (2024). Quantum Computing Challenges and Impact on Cyber Security. In S. Goel & P. R. Nunes De Souza (Eds.), *Digital Forensics and Cyber Crime* (Vol. 571, pp. 333-343). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-56583-0_22
- Hannas, W. C., y Tatlow, D. K. (Eds.). (2020). *China's Quest for Foreign Technology: Beyond Espionage*. London: Routledge.
- Hansen, L. P. (2020). The spy who never has to go out into the cold: Cyber espionage. In *Encyclopedia of Criminal Activities and the Deep Web* (pp. 258-270). IGI Global.
- Herrmann, D. (2019). Cyber Espionage and Cyber Defence. In C. Reuter (Ed.), *Information Technology for Peace and Security* (pp. 83-106). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-25652-4_5
- Hiller, J. S., y Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review*, 29(3), 236-245.
- IBM. (2023, diciembre 11). ¿Qué es la respuesta a incidentes? IBM. [Internet]. <https://www.ibm.com/es-es/topics/incident-response>
- Innovation, Science and Economic Development Canada. (2022). Policy Statement – Securing Canada's Telecommunications System [Statements]. <https://www.canada.ca/en/innovation-science-economic-development/news/2022/05/policy-statement-securing-canadas-telecommunications-system.html>
- Jibilian, I., y Canales, K. (2021). The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal. *Business Insider*. [Internet]. <https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12> [Consultado: 28 de mayo de 2024].
- Jones, J. (May 2020). Confronting China's efforts to steal defense information. Harvard Kennedy School, Belfer Center for Science and International Affairs. Reports & Papers. <https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information>



- Kara, I. (2022). Cyber-Espionage Malware Attacks Detection and Analysis: A Case Study. *Journal of Computer Information Systems*, 62(6), 1253-1270. <https://doi.org/10.1080/108874417.2021.2004566>
- Kaska, K., Beckvard, H., y Minárik, T. (2019). Huawei, 5G and China as a security threat. NATO Cooperative Cyber Defence Center for Excellence (CCDCOE). <https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf>
- Kim, S.-K., Cheon, S.-P., y Eom, J.-H. (2019). A leading cyber warfare strategy according to the evolution of cyber technology after the fourth industrial revolution. *International Journal of Advanced Computer Research*, 9(40), 72-80. <http://dx.doi.org/10.19101/IJACR.SOC6>
- Kopchev, V. (2019). The European Union Moves Ahead on Cybersecurity Research Through Enhanced Cooperation and Coordination. *Information & Security: An International Journal*, 42, 67-81. https://procon.bg/system/files/4204_cybersecurity_centres_vkopchev.pdf
- Kose, J. (2021). Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage. *ISSA Journal*, 19(4), 12-15. <https://cdn.ymaws.com/www.members.issa.org/resource/resmgr/journalpdfs/feature0421.pdf>
- Kovács, L. (2018). Cyber Security Policy and Strategy in the European Union and Nato. *Land Forces Academy Review*, 23(1), 16-24. <https://doi.org/10.2478/raft-2018-0002>
- Krieg, A., y Rickli, J.-M. (2019). *Surrogate Warfare: The Transformation of War in the Twenty-First Century*. Georgetown University Press.
- Lara, C. (2022). *An analysis of China's cyber espionage against the United States defense industrial base*. (PhD Thesis), Utica University.
- Layton, P. (2020). Artificial intelligence, big data and autonomous systems along the belt and road: Towards private security companies with Chinese characteristics? *Small Wars & Insurgencies*, 31(4), 874-897. <https://doi.org/10.1080/09592318.2020.1743483>
- Lemay, A., Calvet, J., Menet, F., y Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, 72, 26-59. <https://www.sciencedirect.com/science/article/abs/pii/S0167404817301608>
- Levite, A. E., Kannry, S., y Hoffman, W. W. (2022). *Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance*. Washington: Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/Cyber_Insurance_Formatted_FINAL_WEB.PDF
- Lohani, S. (2019). Social engineering: Hacking into humans. *International Journal of Advanced Studies of Scientific Research*, 4(1). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329391
- Macidov, S. T. Oglu (2023). Prosecuting Cybercrimes under International Legal Frameworks: Challenges and Innovations. *Futurity Economics & Law*, 3(3), 80-95. <https://doi.org/10.57125/FEL.2023.09.25.05>



- Martín Porras, M. (2022). *Ciberseguridad y redes 5G en las relaciones internacionales: el caso de Huawei*. (Tesis de posgrado). Universidad Autónoma de Barcelona. <https://ddd.uab.cat/record/266102>
- Mmaduekwe, U., y Mmaduekwe, E. (2024). Cybersecurity and Cryptography: The New Era of Quantum Computing. *Current Journal of Applied Science and Technology*, 43(5), 41-51. <https://journalcjust.com/index.php/CJAST/article/view/4377>
- Montes Toscano, B. (2023). Inteligencia Artificial en el Espacio Ultraterrestre: ¿Un nuevo desafío para la OTAN? *Araucaria. Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales*, 25(53), 309-334. <https://doi.org/10.12795/araucaria.2023.i53.12>
- Moulin, T. (2023). *Cyber-espionage in international law. Silence speaks*. Manchester: Manchester University Press.
- Mueller, G. B. (2022). *Dimensions of Cybersecurity: Espionage, Rivalry, and Political Economy* [PhD Thesis]. University of Texas. <https://hdl.handle.net/10735.1/9678>
- Nasheri, H. (2023). State-Sponsored Economic Espionage in Cyberspace: Risks and Preparedness. In R. G. Smith, R. Sarre, L. Y.-C. Chang, & L. Y.-C. Lau (Eds.), *Cybercrime in the Pandemic Digital Age and Beyond* (pp. 87-107). Springer International Publishing. https://doi.org/10.1007/978-3-031-29107-4_5
- NIC Argentina. (2017). ¿Qué es el Convenio de Budapest? NIC Argentina (Dirección Nacional del Registro de Dominios de Internet). <http://nic.ar/es/enterate/novedades/que-es-convenio-budapest> [Consultado: 24 de mayo de 2024].
- Niglia, A. (2016). *Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges*. NATO Science for Peace and Security Series-D: Information and Communication Security, vol. 46. IOS Press.
- Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2019). Módulo 8. Seguridad Cibernética y Prevención del Delito Cibernético: Estrategias, Políticas y Programas. Serie de Módulos Universitarios: Delitos Cibernéticos. <https://www.unodc.org/e4j/es/cybercrime/module-8/index.html>
- Oladimeji, S., y Kerner, S. M. (2023, 3 de noviembre). SolarWinds hack explained: Everything you need to know. *WhatIs*. [Internet]. Tech Target. <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know> [Consultado: 28 de mayo de 2024].
- Pehlivan, O. K. (2018). *Confronting cyberespionage under international law*. New York: Routledge.
- Pereira Hernández, C. M. (2023). China vista desde Estados Unidos: entre el conflicto, la cooperación y la competencia. *Revista Política Internacional*, 5(1), 57-80. <https://rpi.isri.cu/index.php/rpi/article/view/361>
- Qureshi, W. A. (2019). Fourth- and Fifth-Generation Warfare: Technology and Perceptions. *San Diego International Law Journal*, 21(1), 187-216.



- Rawat, R., Mahor, V., Chirgaiya, S., y Garg, B. (2021). Artificial Cyber Espionage Based Protection of Technological Enabled Automated Cities Infrastructure by Dark Web Cyber Offender. In F. Al-Turjman, A. Nayyar, A. Devi, y P. K. Shukla (Eds.), *Intelligence of Things: AI-IoT Based Critical-Applications and Innovations* (pp. 167-188). Springer International Publishing. https://doi.org/10.1007/978-3-030-82800-4_7
- Realpe, M. E., y Cano, J. (2020). Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia. En V. Gauthier-Umaña, R. A. Méndez-Romero, J. Cano, J. Ramió Aguirre, y L. E. Sánchez (Eds.), *Seguridad Informática. X Congreso Iberoamericano, CIBSI 2020*. Universidad del Rosario. <https://doi.org/10.12804/si9789587844337.10>
- Rin, R. (2023). Quantum Computer Solving Crime: Is Quantum Computing the Future of Cybersecurity? <https://www.illuminatenrhc.com/post/quantum-computer-solving-crime-is-quantum-computing-the-future-of-cybersecurity-by-rita-rin>
- Rivas, S. M. (2021). El Ciberespacio como zona de control geopolítico y papel de las potencias por la supremacía cibernética: China y Estados Unidos. *Revista Relaciones Internacionales*, 3(1), 89-107.
- Rivera, R., Pazmiño, L., Becerra, F., y Barriga, J. (2022). An Analysis of Cyber Espionage Process. In Á. Rocha, C. H. Fajardo-Toro, & J. M. R. Rodríguez (Eds.), *Developments and Advances in Defense and Security* (Vol. 255, pp. 3-14). Smart Innovation, Systems and Technologies. Springer, Singapore. https://doi.org/10.1007/978-981-16-4884-7_1
- Romero, M. (2024, mayo 24). ESET publica su Informe de actividad de APT, que destaca la guerra cibernética de grupos alineados con Rusia, China e Irán. Agencia de Noticias Órbita. Agencia Órbita. [Internet]. <https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/eset-publica-su-informe-de-actividad-de-apt-que-destaca-la-guerra-cibernetica-de-grupos-alineados-con-rusia-china-e-iran/>
- Rosli, W. R. W., Kamaruddin, S., Mohamad, A. M., Saufi, N. N. M., y Hamin, Z. (2021). Governing Cyber Espionage Threats via the Integration of the Risk Society-Cyber Securitisation Theory. *2021 Innovations in Power and Advanced Computing Technologies (i-PACT)* (pp. 1-7), IEEE.
- Rowe, B. I. (2020). Transnational state-sponsored cyber economic espionage: A legal quagmire. *Security Journal*, 33(1), 63-82. <https://doi.org/10.1057/s41284-019-00197-3>
- Rugina, J. M. (2023). Economic Cyber Espionage: The US-China Dilemma. *Journal of International Relations Studies*, 3(2), 77-90. <https://dergipark.org.tr/en/download/article-file/3633972>
- Sadok, M., Welch, C., y Bednar, P. (2020). A socio-technical perspective to counter cyber-enabled industrial espionage. *Security Journal*, 33(1), 27-42. <https://doi.org/10.1057/s41284-019-00198-2>
- Sambaluk, N. M. (2019). *Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, and Technology*. Santa Barbara, California: ABC-CLIO.



- Sandoval-Paucar, G., Arango-Ospina, A., Rodríguez-Vélez, P., y Santana-Oviedo, M. (2020). Un análisis de las oportunidades laborales de los excombatientes desde la perspectiva del sector empresarial. *Sociedad y Economía*, (39), 135-155. <https://doi.org/10.25100/sye.v0i39.7378>
- Sarker, I. H. (2021). Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective. *SN Computer Science*, 2, art. 154. <https://doi.org/10.1007/s42979-021-00535-6>
- Schneider, J. (2022). A World without Trust: The Insidious Cyberthreat. *Foreign Affairs*, 101(1), 22-31. <https://hostnezt.com/cssfiles/currentaffairs/foreignaffairs/Foreign%20Affairs%20January%20February%202022%20Issue.pdf>
- Segal, A. (2020). China's pursuit of cyberpower. *Asia Policy*, 15(2), 60-66. DOI: 10.1353/asp.2020.0034
- Sekati, P. (2022). Assessing the Effectiveness of Extradition and the Enforcement of Extra-territorial Jurisdiction in Addressing Trans-national Cybercrimes. *Comparative and International Law Journal of Southern Africa*, 55(1). <https://doi.org/10.25159/2522-3062/10476>
- Shandler, R., y Canetti, D. (2024). Introduction: Cyber-conflict – Moving from speculation to investigation. *Journal of Peace Research*, 61(1), 3-9. <https://doi.org/10.1177/00223433231219441>
- Shandler, R., y Gomez, M. A. (2023). The hidden threat of cyber-attacks – undermining public confidence in government. *Journal of Information Technology & Politics*, 20(4), 359-374. <https://doi.org/10.1080/19331681.2022.2112796>
- Sharma, R. (2022). Cyber Security to Safeguard Cyber Attacks. *International Journal of Information Security and Cybercrime (IJISC)*, 11(2), 50-63. <https://www.ijisc.com/year-2022-issue-2-article-5/>
- Shull, A. (2019). Governing cyberspace during a crisis in trust. In *Governing Cyberspace during a Crisis in Trust* (pp. 4-8). Waterloo, Canada: CIGI. <https://www.cigionline.org/sites/default/files/documents/Cyber%20Series%20Web.pdf>
- Stupak, O. (2023). *Industrial cyberespionage in research and development races*. University of Cambridge. <https://www.repository.cam.ac.uk/items/19358e7d-45bc-454a-9148-938e4cc8b32d>
- Tóth, D., y Gáspár, Z. (2020). Jurisdictional Challenges of Cybercrime. *Journal of Eastern European Criminal Law*, (2), 101-118. <https://www.ceeol.com/search/article-detail?id=999903>
- Trim, P. R., y Lee, Y.-I. (2021). The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement. *Big Data and Cognitive Computing*, 5(3), 32. <https://doi.org/10.3390/bdcc5030032>
- Tropina, T. (2020). Cybercrime: Setting international standards. In E. Tikk & M. Kerttunen (eds.), *Routledge Handbook of International Cybersecurity* (pp. 148-160). London:



- Routledge. <https://www.taylorfrancis.com/chapters/edit/10.4324/9781351038904-14/cybercrime-tatiana-tropina>
- Tsakalidis, G., Vergidis, K., y Madas, M. (2018). Cybercrime offences: Identification, classification and adaptive response. In *2018 5th International Conference on Control, Decision and Information Technologies (CoDIT)* (pp. 470-475). <https://ieeexplore.ieee.org/abstract/document/8394816/>
- Tzenios, N. (2023). *Corporate Espionage and the Impact of the Chinese Government, Companies, and Individuals in Increasing Corporate Espionage* (PhD Thesis), Apollos University.
- Unal, B. (2019). Cybersecurity of NATO's Space-based Strategic Assets. Chatam House. <https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets>
- Warfield, D. (2012). Critical Infrastructures: IT Security and Threats from Private Sector Ownership. *Information Security Journal: A Global Perspective*, 21(3), 127-136. <https://doi.org/10.1080/19393555.2011.652289>
- Wasicek, A. (2020). The future of 5G smart home network security is micro-segmentation. *Network Security*, 2020(11), 11-13. [https://doi.org/10.1016/S1353-4858\(20\)30129-X](https://doi.org/10.1016/S1353-4858(20)30129-X)
- Weinberg, A. I., y Faccia, A. (2024). Quantum Algorithms: A New Frontier in Financial Crime Prevention (arXiv:2403.18322). arXiv. <http://arxiv.org/abs/2403.18322>
- Xu, T., Feng, A., Song, X., Zhengjie, G., y Zeng, X. (2020). Chinese News Data Extraction System Based on Readability Algorithm. In: X. Sun, J. Wang, & E. Bertino (eds.), *Artificial Intelligence and Security. ICAIS 2020. Communications in Computer and Information Science* (pp. 153-164), vol. 1252. Springer, Singapore. https://doi.org/10.1007/978-981-15-8083-3_14
- Yong, N. (s. f.). Cómo China consigue robarle sus secretos tecnológicos a Estados Unidos. *BBC News Mundo*. <https://www.bbc.com/mundo/noticias-internacional-64355527>
- Zamarrón, I. (2023). Made in China 2025: Así es el ambicioso plan tecnológico chino que amenaza el dominio de EU. *Forbes México*. [En línea]. <https://www.forbes.com.mx/made-in-china-2025-asi-es-el-ambicioso-plan-tecnologico-chino-que-amenaza-el-dominio-de-eu/>
- Zhao, M. (2019). Is a new Cold War inevitable? Chinese perspectives on US–China strategic competition. *The Chinese Journal of International Politics*, 12(3), 371-394. <https://doi.org/10.1093/cjip/poz010>



Capítulo 3

Por qué es necesario un (nuevo) marco jurídico para promover (las formas y los registros para) las finanzas que necesitan las empresas del siglo XXI

Sebastián Heredia Querro

Financiar para crecer

En la literatura económica se ha demostrado la importancia del desarrollo del sector financiero de un país para reducir los costos de *financiamiento externo* de compañías (el financiamiento que proviene de fuera de la generación propia de efectivo). En los estudios se encuentra que el desarrollo del sector financiero puede mejorar el crecimiento económico de un país y, además, beneficia proporcionalmente más a aquellos sectores o industrias que por su naturaleza requieren más capital (Rajan et al. 1996). Esto es notable en sectores como los bienes raíces, el turismo, la producción agrícola y ganadera, etc.

En economías emergentes como la de Argentina, con un mercado financiero de muy bajo desarrollo, el acceso a fuentes externas de financiamiento es bajo. En este país, el crédito al sector privado como porcentaje del PBI es una séptima parte del promedio de la región (5,5 % vs. 39 %), el cual se ubica muy por debajo de los niveles de los países desarrollados (BID Invest, 2021). En este contexto adverso, el uso de capital propio es casi el único recurso financiero en compañías de menor escala, lo que deja excluidas innumerables oportunidades de inversión, que no se desarrollan por falta de capital.

En otras palabras, el sector financiero cumple un rol fundamental en una economía, porque permite reubicar excedentes de capital hacia proyectos que maximicen su valor. La inexistencia de un mercado local que regule estos flujos lleva a que no se ejecuten oportunidades de inversión y que el crecimiento económico global sea menor. Por ello, generar las condiciones para fomentar el desarrollo de una industria financiera permitirá activar este proceso, y crear un flujo de los excedentes de fondos de agentes superavitarios en la economía argentina hacia proyectos de inversión



aún no desarrollados por falta de capital y, de esta manera, constituirse en un catalizador del crecimiento económico.

En efecto, la literatura económica indica lo conveniente que resulta promover la alineación entre *ciertas* políticas públicas con un foco específico y un diseño *a la medida* de las necesidades de creciente financiamiento externo de las pymes, que les permita crecer e internacionalizarse; viejas necesidades que hoy se pueden combinar con nuevas formas de inversiones *retail* que remuneren el ahorro argentino, pensando incluso en un mercado regional ampliado y con creciente interoperabilidad, al menos en términos de medios de pago digital (hoy PIX, mañana DREX).

A tan solo 33 años del lanzamiento del *one-line protocol* (Berners-Lee, 1991; también, “Evolution of HTTP”, s. f.) y el surgimiento de Internet —la llamada *Web1*²—, ya son tendencias consolidadas: (i) desmaterializar el dinero y los instrumentos de inversión, y (ii) la omnicanalidad digital, el *e-commerce*³ y la venta en línea de todo tipo de bienes y servicios —físicos y también nativos digitales como el *streaming*— a través de plataformas de la era del *Web2*.

Ahora bien, el desarrollo jurídico y tecnológico que ha experimentado el mundo financiero en los últimos quince años, especialmente en materia de finanzas portátiles, abre una enorme oportunidad que puede resolver los problemas del poco desarrollado mercado de capitales argentino a través de un nuevo enfoque: la representación digital de activos.

La representación digital de activos puede facilitar procesos de venta anticipada y financiamiento de proyectos de baja escala, ya sean fracciones de una propiedad, un caballo, un panel fotovoltaico, un árbol o una licencia de software. Diferentes activos antes ilíquidos, hoy pueden fraccionarse y negociarse en ecosistemas seguros y de fácil transacción.

Los avances legales y tecnológicos, principalmente en el desarrollo de *Distributed Ledger Technologies* (DLT, “bases de datos distribuidas”), brindan una nueva herramienta revolucionaria para el financiamiento de proyectos y para la omnicanalidad comercial y, en consecuencia, para la actividad económica en general. El principal atributo aportado por una DLT en el contexto de la representación digital de activos, es la capacidad de mantener su integridad a pesar de que diferentes actores pueden acceder a ella (Garrido, 2023), lo cual se alcanza gracias a la criptografía.

² Para un análisis de la evolución de la Web1 a la Web3, véase Voshmgir, S. (junio 2020). *La Economía del Token: Cómo la Web3 reinventa la Internet*. 2.ª ed. Berlin: Token Kitchen. <https://github.com/Token-Economy-Book/SpanishTranslation>

³ En Argentina, las ventas en línea facturaron en 2023 un total de \$7,8 billones, con un incremento del 175 % frente a los datos de 2022, según el estudio sobre comercio electrónico que publicó la Cámara Argentina de Comercio Electrónico (CACE). En 2023, se sumaron 1.419.784 nuevos compradores en línea. Así, el total asciende a 23.247.989 usuarios, alrededor de la mitad de la población argentina. Ocho de cada 10 compradores buscan información en la web para sus compras *offline*, principalmente a través de sus teléfonos. En esa interacción omnicanal, la oferta digital, por ser el imán de compras, se potencia con la presencia de las promociones, tanto las propias de las tiendas como las que se hacen a través de bancos y otras entidades financieras. (“Ecommerce: las ventas online...”, 2024).



En este contexto, en el marco de la libertad de formas, un registro en una DLT puede incorporar un derecho y permite a su titular ejercerlo o transferirlo⁴. Cualquier cambio en dicho registro implica o puede implicar un cambio en los derechos asignados. Y no solo esto, además la tecnología otorga funcionalidades antes inexistentes. Por ejemplo, modificar el registro puede cambiar la naturaleza de un derecho⁵, o bien, un derecho puede desaparecer a través del cumplimiento de una condición que se dispare de manera automática. Todo esto representa una oportunidad y un desafío. Transferir un derecho puede ser tan fácil como realizar un cambio en el registro (distribuido), lo que permite una transacción rápida, económica y con tendencia hacia la uniformidad global que facilita el intercambio comercial. Sin embargo, esto abre un importante desafío: resguardar la seguridad de los derechos representados en tal registro.

En este punto, resulta útil recordar que todo lo distinto o diferente de lo que antes había o se tenía aprendido, es disruptivo y ocasiona naturales rechazos, fricciones y desconfianza por parte del *statu quo*, en razón a que impide la posibilidad de establecer una estabilidad constante y predecible en la forma de actuar habitual. Las nuevas tecnologías instan a nuevas maneras de construcción y despliegue, y obligan a un nuevo aprendizaje y nuevas formas de vinculación.

Ante esto, corresponde preguntarse: ¿los sistemas actuales de transferencia de derechos son más seguros?, ¿brindan un diferencial de seguridad que justifique sus costos, tiempos y formalismos? Creemos que la respuesta es negativa. Basta contrastar una transmisión elaborada sobre sistemas de desarrollo de bases de datos distribuidas (DLT) contra una transmisión instrumentada en un instrumento privado en soporte impreso.

Toda normativa en esta materia debe imperativamente ser creada sobre una base de apertura, globalización y uniformidad de las normas ya existentes en otros Estados y entidades supranacionales (como la UE), pues, en caso contrario, la norma igualmente sería ineficaz; crear una norma local, extravagante y ajena a las figuras

⁴ En esta línea se orienta el trabajo de la CNUDMI desde 2017, con su ley modelo de *Documentos Electrónicos Transmisibles*, marco legal conocido como “leyes de firma digital de segunda generación”, el que, a nuestro modo de ver, recepta los registros distribuidos de la Web3. Reza: “La Ley Modelo sobre Documentos Transmisibles Electrónicos se basa en los principios de no discriminación contra el uso de medios electrónicos, **equivalencia funcional y neutralidad tecnológica**, en los que se inspiran todos los textos de la CNUDMI sobre comercio electrónico. Por lo tanto, puede dar cabida a la utilización de todas las tecnologías y todos los modelos, como el sistema registral, **el de tokens o el de registros descentralizados**.” (El resaltado es nuestro). La ley 25.506 de régimen legal de firma digital, sancionada el 14 de noviembre de 2001, corresponde a la primera generación de leyes. Véase: CNUDMI (2017).

⁵ En este sentido, véase la nota 39, el proyecto de ley con media sanción en la Cámara de Representantes de EE. UU., conocido como FIT21. El proyectado Art. 101, que regula las definiciones, define, entre otros, términos como *Blockchain*, *Código Fuente*, *Protocolo Blockchain*, *Sistema de Gobernanza Descentralizado*, *Sistema Funcional*, *Sistema Descentralizado*, *Activo Digital*, *Emisor de Activos Digitales*, *Fecha de Maduración del Activo Digital*, *Commodity Digital*, *Activo Digital Restringido* y *Sistema de Intercambio de Activos Digitales*. Cuando un Protocolo Blockchain es un Sistema Funcional que puede ser certificado como un Sistema Descentralizado y cumple las certificaciones exigidas por el Art. 302-304, los Activos Digitales en él creados pueden ser distribuidos a un usuario final y, en estas condiciones, tales ventas no se consideran un *investment contract* —confr. modificación propuesta al Art. 42(b)(3)—, aunque deben cumplirse ciertas restricciones respecto de personas que califiquen como afiliadas al emisor.



internacionales en nada contribuye a la expansión en el uso de las DLT. La situación que nos ocupa (vinculaciones sobre la base de DLT) no admite la distinción entre situaciones internas y transfronterizas, sino que responde a un fenómeno global, y, exista o no una norma, este tipo de sistemas distribuidos de gestión de la información seguirá imponiéndose en tanto demuestre ventajas de costos y reducción real —no potencial— de costos de transacción. De ahí que sea más sano para el sistema y la seguridad jurídica que el Estado cree una norma, con la cual reconozca esta nueva realidad y la regule inteligentemente, de conformidad y en consonancia con el resto de los países.

En lo expuesto hasta ahora, sobre todo esta especial naturaleza que caracteriza los registros de tipo DLT, se requiere para su desarrollo un marco legal que regule la creación, representación y negociación de estos activos y que, además, brinde seguridad jurídica para los promotores de proyectos que hacen uso de esta tecnología de alto crecimiento. Contar con fundamentos legales sólidos contribuirá al desarrollo jurídico y tecnológico y permitirá ampliar el uso de las DLT. De esta manera, diferentes sectores económicos de Argentina, que hoy se encuentran sin financiamiento, podrían encontrar una respuesta a sus necesidades a través de herramientas más económicas⁶ y seguras que las hoy existentes. Además, encontrarán nuevas oportunidades de negocios asociadas a las nuevas funcionalidades que aporta la DLT y que potencian la omnicanalidad.

En este contexto, una base legal sólida hará posible ampliar el desarrollo tecnológico vinculado al uso de las DLT y masificar su uso a través de los diferentes sectores económicos, al tiempo que permitirá reducir costos transaccionales y mejorar su seguridad (Garrido, 2023). De esta manera, incentivar el uso de las DLT promueve no solo el crecimiento económico mediante la mejora del financiamiento y la liquidez, sino también la innovación.

La seguridad jurídica como una condición necesaria

Los activos criptográficos se diferencian en ciertos aspectos clave de los activos digitales tradicionales. Desde un punto de vista técnico, se registran en una base de datos descentralizada cuya seguridad se encuentra respaldada por la criptografía. Desde un punto de vista económico, replican de una manera más rápida y económica las funciones típicas de los activos digitales tradicionales, o bien incorporan nuevos usos que resuelven problemas históricos de ciertos sectores.

⁶ "Increased use of asset tokenisation could have widespread potential benefits in terms of cost and speed efficiencies, increased transparency, liquidity and more inclusive participation of retail investors in assets of constraint access to them in traditional forms. Although the use of tokenisation is currently limited, its potential is significant. Careful consideration of the possible impact on financial markets of a proliferation in the use of asset tokenisation will allow policy makers to anticipate potential perils linked to the wider use of such mechanisms". (OECD, 2020, p. 10) (El resaltado es nuestro).



Por esta naturaleza innovadora que dispara nuevos usos, es necesario un nuevo marco normativo específico que incorpore esta naciente tecnología.

Como es sabido, la norma o la regulación de un hecho siempre llegarán después del fenómeno⁷, pero este es un extremo que en ocasiones produce problemas de aplicación, lenguaje y método. Sin embargo, esto no implica que no deba darse una regulación, si es una buena oportunidad para hacerlo, ya que la demora en ello no evitará su uso, pero sí ocasionará trabas y dificultades a quienes utilicen esta tecnología, e impedirá su implementación plena con las ventajas que trae aparejadas, muchas de las cuales se predicen sobre el sector público. Los emprendedores, empresas y personas se desenvuelven en entornos digitales, transnacionales, sin espacios físicos, donde las transacciones y los derechos pueden crearse y destruirse en segundos.

Sumado a lo anterior, en este mundo digital rápido, eficiente y económico, cada transacción ocasiona una torsión entre los intereses de los particulares y las normas de orden público vinculadas con el uso de datos personales, derechos del consumidor, derechos de incidencia colectiva, etc. De ahí que una legislación tardía no tendrá utilidad práctica, porque el dinamismo del cambio en las tecnologías haría obsoleta la nueva norma; mientras que si se dictara a tiempo, permitiría un despliegue y un uso más eficaz de las tecnologías.

Para alcanzar el objetivo de fomentar el uso de las DLT no solo es necesario un código de programación, también se requiere un marco normativo claro que fije las reglas de juego. Desarrollar este marco jurídico brindará claridad y certeza en relación con los riesgos vinculados a llevar a cabo proyectos que hagan uso de las DLT.

Una regulación incompleta o poco clara impide la implementación de nuevas tecnologías (G7, 2019) y reduce la propensión a invertir en sectores específicos. Diferentes antecedentes muestran que la expectativa de cambios regulatorios desincentiva a empresas a invertir en el largo plazo (Fabrizio, 2013), y no solo esto, también la percepción de discrecionalidad regulatoria es un factor que desincentiva la inversión (Fernández-Méndez et al., 2023).

En un contexto con iniciativas de regulación internacionales y regionales respecto de los posibles usos de una tecnología con bajas (cuando no nulas) barreras geográficas por su naturaleza digital, es urgente que Argentina lleve adelante todos los esfuerzos regulatorios necesarios para brindar reglas de juego claras que mitiguen la incertidumbre jurídica, que hoy recae en general sobre todos los sectores de la

⁷ En 1949 (tres años después de la invención de la primera computadora digital electrónica ENIAC), se publicaba el artículo: Loevinger, L. (1949). "Jurimetrics: the next step forward". *Minnesota Law Review*. <https://scholarship.law.umn.edu/cgi/view-content.cgi?article=2795&context=mlr>. Se lee allí: "The important matter for understanding is not the mechanics of the law, but the human problem which it is the business of the law to solve, and the actual results which are achieved". Se cita también al *great dissenter*, quien dijo: "The life of the law has not been logic. It has been experience". Desde el 3 de enero de 2009, se han acumulado ya 15 años de experiencia gestionando información —datos, representen o no derechos— de manera distribuida, y de acuerdo con Gartner, todo indica que se inicia una etapa conocida como *slope of enlightenment*. Véase: Gartner. (s. f.). Gartner Hype Cycle. <https://www.gartner.com/en/research/methodologies/gartner-hype-cycle>



economía, y en particular sobre el sector Fintech, de modo que permita y promueva la experimentación de *startups* locales, pero que también atraiga el interés de promotores de proyectos innovadores extranjeros dispuestos a desarrollarse en nuestro país. Si esto se da, se mejoran las condiciones necesarias que van a permitir jalonar la oferta y la demanda locales del sector de la economía del conocimiento⁸ y, *vis-à-vis*, a exponer el talento del país a los desarrollos más innovadores del mundo financiero global.

Rápida adopción global de las DLT

Llevar adelante políticas y prácticas que fomenten el uso de DLT permitiría a la Argentina alinearse internacionalmente con la adopción de esta herramienta. En el mundo, la tokenización avanza a un ritmo continuo, con una aceleración esperada a medida que los efectos de red ganen impulso.

Dadas sus características, es probable que ciertos tipos de *asset class* alcancen una adopción significativa —definida como más de 100 mil millones de dólares de capitalización de mercado tokenizada— para finales de la década. Se espera que los principales pioneros incluyan efectivo y depósitos, bonos y pagarés cotizados en bolsa (ETN, por sus siglas en inglés), fondos mutuos y fondos cotizados en bolsa (ETF, por sus siglas en inglés), así como préstamos, securitización y otros activos. Para muchos de estos, las tasas de adopción ya son significativas, sustentadas por una mayor eficiencia y ganancias mayores de valor derivadas de la cadena de bloque (especie de DLT), junto con una mayor viabilidad técnica y regulatoria (McKinsey, 2024).

Se estima que la capitalización de mercado tokenizada en todas las clases de activos podría alcanzar alrededor de 2 billones de dólares para 2030 (excluyendo criptomonedas y criptomonedas estables, en adelante *stablecoins*), impulsada principalmente por los activos mencionados anteriormente. Los escenarios pesimistas y optimistas oscilan entre aproximadamente USD 1 billón y USD 4 billones, respectivamente. Esta estimación excluye las *stablecoins* y los depósitos tokenizados, las *stablecoins* mayoristas y las monedas digitales de bancos centrales (en adelante, CBDC) para evitar la doble contabilización, ya que a menudo se utilizan como el efectivo correspondiente en la liquidación de operaciones que involucran activos tokenizados (McKinsey, 2024).

⁸ Al comparar 2023 contra 2022, el sector de la Economía del Conocimiento (EdC) se comportó de modo contracíclico, e incrementó sus exportaciones en un 2,9 % anual, mientras que el crecimiento del empleo fue del 3,6 %. Durante el mismo periodo, aumentó la participación de la EdC en el desarrollo nacional, con el 9,7 % del total de exportaciones y el 7,3 % en el empleo registrado. La EdC alcanzó, durante el último trimestre de 2023, los 494.000 puestos de trabajo, donde los servicios informáticos crecieron un 4,7 % más que en igual trimestre del 2022 y los servicios profesionales, un 3,4 %. Sin embargo, a pesar de haber aumentado el mercado laboral, el sector de Software y servicios de informática mostró una caída del -6,8 % en sus exportaciones (Lesta, 2024).



Sobre los tókenes criptográficos

Alcanzar un marco regulatorio robusto ayudará a mejorar la competitividad de Argentina en esta industria de alto crecimiento. A tal fin, esta nueva regulación debiera establecer los requisitos para la emisión de criptoactivos vinculados a activos reales (en adelante, RWA, *Real World Assets*). Armonizar los criterios y requisitos necesarios para la emisión de activos es un desafío, ya que existen diferentes tipos de derechos representados e incluso tókenes que no representan un activo.

Por lo tanto, es necesario tipificar el alcance de esta regulación hacia aquellos activos digitales criptográficos que se encuentren vinculados a RWA, para lo cual, a continuación, se presenta una clasificación de los diferentes tipos de tókenes que pueden ser emitidos y, principalmente, cuáles son de interés en esta propuesta.

La revolución digital ha traído consigo una variedad de nuevos conceptos y tecnologías, entre las que destacan los activos digitales y, en particular, los tókenes criptográficos. En este sentido, apelar a la taxonomía, *o la ciencia de la clasificación*, resulta *crucial en la comprensión y organización de estos elementos*. Una adecuada clasificación basada en los caracteres de un elemento *no solo facilita su estudio, sino que también permite una mejor regulación y, en consecuencia, su adopción por parte de los múltiples grupos de interés afectados*.

De esta manera, en cualquier campo de estudio es fundamental la taxonomía, ya que proporciona un marco estructurado para identificar, nombrar y clasificar elementos en categorías lógicas. En este contexto, donde aún hoy nos movemos, ante la presencia de palabras difusas (*buzzwords*) o incluso frente al empleo de la misma palabra para denominar dos elementos que en esencia son distintos (homonimia), una buena clasificación es esencial para entender los diferentes tipos y usos, así como para diseñar regulaciones adecuadas y proteger a los *tokenholders* (inversores adquirentes). Según Shermin Voshmgir (2020), una taxonomía clara y precisa es crucial para la evolución de la economía de tókenes y para la implementación eficaz de esta tecnología en diversos sectores.

Resulta entonces pertinente comenzar por preguntarnos: ¿qué es un token?, ¿qué tipos de tókenes existen? ¿Qué sucede cuando un token se corresponde con una entrada de datos en una blockchain?, ¿si implica o no la representación de un elemento tipificado como activo? Y, de ser así, ¿*todos los activos resultan iguales en cuanto a su naturaleza*? Frente a estos interrogantes, proponemos las siguientes respuestas que, a juicio de quienes participamos de este artículo, ayudan a esclarecer este escenario borroso de conceptos.



Figura 1. Clasificación Taxonómica de tokens



Nota: tomado de Herrera y Bertoni (2022).

Como se ha mencionado, “un token criptográfico es la representación digital de algo que se encuentra almacenado en una base de datos distribuida” donde, gracias a la integración con las funcionalidades de las DLT y los contratos inteligentes, estos tokens pueden conectarse con derechos de diferente índole (Garrido, 2023).

Sin embargo, esta representación puede ser de diversa naturaleza. Los tokens más conocidos son aquellos vinculados a activos, como la representación de un mt² de una propiedad, un árbol (conocidos como *asset tokens*), o hasta una acción de una compañía debidamente constituida (conocidos como *tokenized securities* o *valores tokenizados*). Sin embargo, existen también tokens que pueden representar algo que no es un activo, como una identidad digital de una persona y varios tipos de *datos personales*⁹, un certificado de cumplimiento ambiental¹⁰ e incluso la representación del ejercicio de derechos políticos¹¹. Este estudio y, en particular, nuestra

⁹ Véase, por ejemplo, el desarrollo del Gobierno de la Ciudad de Buenos Aires sobre la Identidad Digital Auto Soberana (SSDI, por sus siglas en inglés) en <https://quarkid.org>

¹⁰ Confr. [https://ambienteycomerio.org/archive-portfolio/subasta-de-certificados-de-carbono-en-la-provincia-de-cordoba-argentina/#:~:text=Programa%20de%20Reducci%C3%B3n%20y%20Compensaci%C3%B3n%20de%20Emisiones%20de%20GEI.&text=En%202022%2C%20la%20provincia%20de,asociadas%20a%20la%20transici%C3%B3n%20energ%C3%A9tica. // https://ministeriodeserviciospublicos.cba.gov.ar/wp-content/uploads/2022/10/PROGRAMA-DE-REDICCON-Y-COMPENSACION-DE-EMISIONES-DE-GEI.pdf](https://ambienteycomerio.org/archive-portfolio/subasta-de-certificados-de-carbono-en-la-provincia-de-cordoba-argentina/#:~:text=Programa%20de%20Reducci%C3%B3n%20y%20Compensaci%C3%B3n%20de%20Emisiones%20de%20GEI.&text=En%202022%2C%20la%20provincia%20de,asociadas%20a%20la%20transici%C3%B3n%20energ%C3%A9tica.)

¹¹ Véase Faruk, J. H. et al. (2022). Development of Blockchain-based e-Voting System: Requirements, Design and Security Perspective. *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 959-967). Wuhan, China. Doi: 10.1109/TrustCom56396.2022.00132. Véase también: H. Timeline, D. Recording, E. Voting, T. Australian, A. S. Ballot and H. Hollerith, “Historical Timeline Electronic Voting Machines and Related Voting Technology”, Chief Eng, pp. 1-7, 2011; B. Simons and D. W. Jones, “Internet voting in the U.S”, *Commun. ACM*, vol. 55, no. 10, pp. 68-77, 2012; U. Madise and E. Maaten, “Internet Voting in Estonia”, pp. 301-321, 2010; M. Górný, “I-voting - opportunities and threats. Conditions for the effective implementation of Internet voting on the example of Switzerland and Estonia”, *Przegld Politol*, no. 1, pp. 133-146, 2021; T. Differences, “Difference Between Client-Server and Peer-to-Peer Network”, Website, 2017, [online] Available: <https://techdifferences.com/difference-between-client-server-and-peer-to-peer-network.html>; Brennan Centre, “Debunking the Voter Fraud Myth”, Brennan Cent. Justice New York Univ. Sch. Law, 2014, [online] Available: https://www.brennancenter.org/sites/default/files/analysis/Briefing_Memo_Debunking_Voter_Fraud_Myth.pdf; S. Debnath, M. Kapoor and S. Ravi, “The Impact of Electronic Voting Machines on Electoral Frauds Democracy and Development”, *SSRN Electron. J*, 2017; R. M. Alvarez, T. E. Hall and S. D. Hyde, “Introduction: Studying Election Fraud”, *Elect. Fraud Detect. Detering Elect.Manip*, pp. 1-17, 2008, [online] Available: https://www.brookings.edu/wp-content/uploads/2016/07/electionfraud_chapter.pdf; R. Shivers, M. A. Rahman, M. J. H. Faruk, H. Shahriar, A. Cuzzocrea and V. Clincy, “Ride-Hailing for Autonomous Vehicles: Hyperledger Fabric-Based Secure and Decentralize Blockchain Platform”, *Proc. - 2021 IEEE Int. Conf. Big Data Big Data 2021*, pp. 5450-5459, 2021; H. F. Md Jobair, M. Islam, F. Alam, H. Shahriar and A. Rahman, “BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework”,



visión de aquello que debe regularse se centran en los tókenes criptográficos que representan activos (en adelante, *criptoactivos*).

Clasificación de los criptoactivos: naturaleza de la representación. Finalidad perseguida

Los criptoactivos se pueden subclasificar según el tipo de activo representado (es decir, su *naturaleza*). En primer lugar, los llamados *security tokens* pueden representar, como se adelantó, valores negociables desmaterializados y, en general, otros instrumentos de inversión. Asimismo, existen dos tipos posibles de *security tokens*: los nativos de esta nueva era digital¹² (propriadamente dichos *security tokens*), y los ya preexistentes a la puesta en valor de la tecnología DLT, cuando nos valemos de ella para su representación (*tokenized securities*, uno de los casos de RWA de mayor crecimiento global). Ejemplos de estos últimos son la tokenización de acciones de una compañía, mientras que, con relación a los primeros, podrían serlo las representaciones directas sobre activos que no admiten fraccionabilidad en el mundo real (en tanto pierden su condición de activo como tal, p. ej., un caballo de polo), pero sí admiten fraccionabilidad en el ámbito digital sin alterar sus atributos esenciales que les confieren valor, y de este modo constituyen un activo digital que se asemeja, de

Fourth Int. Conf. Blockchain Comput. Appl. (BCCA 2022), 2022, [online] Available: <https://www.researchgate.net/publication/357861285>; M. J. H. Faruk, H. Shahriar, M. Valero, S. Sneha, S. I. Ahamed and M. Rahman, "Towards Blockchain-Based Secure Data Management for Remote Patient Monitoring", Proc. - 2021 IEEE Int. Conf. Digit. Heal. ICDH 2021, pp. 299-308, 2021; M. J. Hossain Faruk, S. Hossain and M. Valero, "EHR Data Management: Hyperledger Fabric-based Health Data Storing and Sharing", Fall 2021 Symp. Student Sch, 2021; M. J. Hossain Faruk, S. Hossain and M. Valero, "Students Certification Management (SCM): Hyperledger Fabric-Based Digital Repository", CCSE Comput. Showc. Day, 2021; R. Bulut, A. Kantarci, S. Keskin and S. Bahtiyar, "Blockchain-Based Electronic Voting System for Elections in Turkey", UBMK 2019 - Proceedings 4th Int. Conf. Comput. Sci. Eng, pp. 183-188, 2019; D. R. Joseph, "Hyperledger Architecture Volume II- Smart Contracts", Gene, vol. 17, no. 3, pp. 341-344, 1982, [online] Available: creativecommons.org/licenses/by/4.0/; K. Yamashita, Y. Nomura, E. Zhou, B. Pi and S. Jun, "Potential Risks of Hyperledger Fabric Smart Contracts", IWBOSE 2019 - 2019 IEEE 2nd Int. Work. Blockchain Oriented Softw. Eng., pp. 1-10, 2019; Z. Zhao, "Comparison of Hyperledger Fabric and Ethereum Blockchain", 2022 IEEE Asia-Pacific Conf. Image Process. Electron. Comput. IPEC 2022, pp. 584-587, 2022; S. Al-Maaitah, M. Qatawneh and A. Quzmar, "E-Voting System Based on Blockchain Technology: A Survey", 2021 Int. Conf. Inf. Technol. ICIT 2021 - Proc, pp. 200-205, 2021; K. Wisessing, P. Ekthammabordee, T. Surasak, S. C. H. Huang and C. Preuksakarn, "The prototype of thai blockchain-based voting system", Int. J. Adv. Comput. Sci. Appl, vol. 11, no. 5, pp. 63-68, 2020; U. Jafar, M. J. A. Aziz and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges", Sensors, vol. 21, no. 17, 2021; S. Sumner, "Biometrics and The Future", You Sale, pp. 183-198, 2016; A. A. M. Al-Shiha, "Biometric Face Recognition Using Multilinear Projection and Artificial Intelligence", 2013, [online] Available: <http://theses.ncl.ac.uk/jspui/handle/10443/2207>; Sikender Mohsienuddin Mohammad, "Facial Recognition Technology", SSRNElectron. J, 2020; L. Li, X. Mu, S. Li and H. Peng, "A Review of Face Recognition Technology", IEEE Access, vol. 8, pp. 139110-139120, 2020.

¹² En el ecosistema DeFi, los tókenes de gobernanza que contienen derechos de participación y voto (p. ej., el token MKR de MakerDAO, que crea el stablecoin Dai, que en ciertas condiciones puede ser depositado —*staked*— en otros protocolos para obtener beneficios financieros), pueden, a nuestro criterio, ser considerados *security tokens* propriadamente dichos. Para participar en la gobernanza de un protocolo, los usuarios deben depositar (*stake*) sus tókenes, lo que implica "bloquear" una cierta cantidad de tókenes depositándolos en un *smart contract*. El *smart contract* sirve como un sistema automatizado que garantiza la integridad del programa de *staking*. No solo registra las cantidades depositadas de los participantes, también dicta la distribución de las recompensas y el plazo durante el cual éstas se desembolsarán. El *staking* brinda a los participantes una oportunidad de participar activamente en la gobernanza del protocolo mientras obtienen recompensas. Cuando los usuarios depositan sus tókenes, el contrato inteligente los recompensa creando nuevos tókenes de gobernanza y enviándolos a sus billeteras. La cantidad de tókenes de gobernanza recibidos depende del total de tókenes depositados por cada participante y de la duración del período del depósito. Cuantos más tókenes se depositen y más tiempo estén bloqueados, mayores recompensas se obtendrán (Joe, 2023).



acuerdo a la posición de la Securities and Exchange Commission (SEC) más reciente de “*es lo que es*” (United States District Court, 2024)¹³ en un todo a los caracteres comúnmente aceptados de, por ejemplo, un instrumento de renta variable. En segundo lugar, los llamados *asset tokens*, que pueden representar tanto bienes físicos fungibles (p. ej., granos, una fracción de una propiedad, y hasta una fracción de un campo que lleva adelante un agronegocio) o no fungibles (p. ej., vinilos únicos y autografiados [v. https://www.instagram.com/yonfrula/p/Cm9ZkamO-d7/?img_index=1]), como también activos “nativos digitales” (p. ej., cryptoarte [Browne, 2021]). En tercer lugar, los llamados *utility tokens*, los cuales otorgan una utilidad específica, como el acceso a una comunidad, el derecho a voto e incluso representar la forma de pago de servicios (de uso o acceso *off-line*) comercializados de manera digital (p. ej., NFTickets [<https://flybondi.com/ar/ticket3puntocero>]), y también la forma de pago de ciertos servicios en línea que admiten como método de pago, por el consumo de servicios, un token nativo (p. ej., Ether, XRP [Lazic, 2024]), y, por último, los tokens con finalidad de pago, o *payment tokens*, que pueden representar el dinero con curso legal (p. ej., e-CYN [People’s Bank of China, 2022], próximamente DREX), que incluye el dinero electrónico (USDC [Browne, 2024]), que se puede convertir en *dinero programable que permite también pagos preprogramables* (BIS, 2023; Lee, 2021; J.P. Morgan, s. f.), o incluso un medio de pago distinto con algún mecanismo de estabilidad subyacente (p. ej., Dai [Maker, 2017]), o una forma de dinero electrónico sin mecanismo de estabilidad, pero con tipicidad social (p. ej., BTC).

Todos los usos potenciales de los tokens criptográficos mencionados se pueden y se deben regular específicamente (o excluirse de la regulación, con sujeción a ciertas condiciones en forma de *Safe Harbours* [Kramer, 2020] o en el marco de un *sandbox* regulatorio [Bains y Wu, 2023]), sea de manera directa (por regulación específica, cuando la tipicidad del nuevo uso dado lo requiera por ausencia de marco regulatorio) o indirecta (cuando la tipicidad del uso dado implique una nueva forma de practicar viejas y conocidas transacciones), para así poder alcanzar mayor claridad y estabilidad jurídicas.

Sin embargo, alcanzar este objetivo requiere un proceso prolongado de estudio y adaptación de la legislación a las características de cada tipología de token. La implementación de la tokenización (específicamente con foco en los *Security Tokens* y los *Payment Tokens*) la constituirían aquellas funcionalidades que mayor impacto potencial podrían tener en Argentina, dadas las limitaciones de nuestro actual sistema financiero. Esto adquiere aún mayor relevancia cuando de la representación digital de un RWA (p. ej., un caballo de polo) podemos caer en escenarios diametralmente opuestos, dependiendo de los atributos relativos a la representación digital (*tokenización*) diseñada. De esta manera, representar un RWA, de forma tal que su

¹³ Véase nota al pie 30.



representación digital admita fraccionabilidad y transferencia de todos los riesgos y beneficios relativos a la cosa bajo administración de un tercero (agencia), da lugar a una nueva forma de inversión pasiva asociada que, en función del tipo de beneficios conferidos, podrá tener más atributos de instrumento de renta fija, de renta variable, o bien de algún instrumento derivado. Por el contrario, si se representa el mismo RWA de manera única, no fraccionable y como tal absolutamente no fungible, se elimina la posibilidad directa de captación de fondos de forma abierta y masiva, por lo tanto, dicha representación se parecerá mucho más a cualquier efecto resultante de una transacción analógica que implique el mencionado RWA. Este nivel dirimente, con respecto a los *asset tokens*, resulta una de las cuestiones más vidriosas que no tienen suficiente claridad en materia de marco regulatorio doméstico.

Dicho esto, priorizar la implementación de un marco normativo para estas tipologías de tókenes por encima de otro tipo de criptoactivos puede derivar en mayores beneficios en el corto plazo. Con respecto al empleo generalizado de *asset* y *utility tokens*, en tanto solo encarnan (nuevas) formas (distribuidas) de omnicanalidad comercial para la venta de bienes y servicios, las normas ya existentes (normas sobre protección de consumidores y usuarios, protección de datos personales, antilavado, etc.) los regulan de forma conveniente y deberá controlarse su adecuado cumplimiento.

En este contexto, es estratégico priorizar la reglamentación de criptoactivos con el objetivo de fomentar y acelerar su desarrollo mediante la clarificación y armonización de los requisitos para la emisión y uso de distintas especies de criptoactivos de interés, y de esta manera otorgar seguridad regulatoria a emisores y usuarios, pero, al mismo tiempo, regular la validación de los proyectos subyacentes¹⁴, utilizando de manera inteligente las tecnologías de supervisión más adecuadas a las tecnologías de registros distribuidos (p. ej., *compliance by design*, *KYT*, etc.), y de este modo incrementar el cumplimiento normativo y mejorar la seguridad de los compradores de estos activos.

¹⁴ Con el fin de implementar regulaciones efectivas que eviten o disminuyan la repetición, nuevamente, de los casos y modos de fraude ya muy conocidos: como con *reentrancy bugs* en el caso *TheDAO* que produjo un polémico *hard fork* en la red Ethereum (Immunefi, 2023); recientemente, con créditos de carbono (Wenzel, 2024); con “stablecoins” como Terra (Singh, 2024); con *insider traders* de NFT (Godoy, 2023); con Exchanges centralizados (Del Valle y Morrow, 2024); en protocolos DeFi vulnerados con *flash attacks* (Heredia, Bertoni y Santamaría, 2022), y con juegos P2E con NFT (Jha, 2022). Debe también prestarse debida atención a ciertas prohibiciones ya existentes (James, 2021), y anticipar las tendencias emergentes en los países desarrollados, especialmente los más comparables, como España (La Moncloa, 2023) e Italia (Digital Found Foundation, 2024), pero especialmente de los líderes como Japón (Koning, 2022) y Alemania, con su *Future Financing Act* (Gesley, 2023).



La importancia de ciertas definiciones para la seguridad regulatoria: los casos de EE. UU. y Alemania

Más arriba se adelantó la necesidad de ciertas definiciones claras para facilitar la adopción y acelerar la tokenización de distintos tipos de activos. La ausencia de reglas y definiciones claras en EE. UU. ha permitido a la *Securities and Exchange Commission* (SEC), pertrechada con un plantel de 4.800 empleados, frente a 800 de la *Commodity Futures Trading Commission* (CFTC), que en diez causas relevantes¹⁵ se aplique el *Howey Test*¹⁶ a distintos tipos de tokens criptográficos que son, en muchos casos, evidentemente *security tokens*¹⁷, como también, en otras ocasiones, puede tratarse de *utility tokens*¹⁸ y hasta de

¹⁵ Confr. U. S. Security and Exchange Commission (SEC). (2024). Statement on the Financial Innovation and Technology for the 21st Century Act. Statement. Chair: Gary Gensler. <https://www.sec.gov/news/statement/gensler-21st-century-act-05222024>.

¹⁶ La doctrina especializada, basada en un estudio de la jurisprudencia aplicable a nivel de cámaras federales —266 apelaciones— y fallos de la Corte Suprema, concluía lo opuesto a lo afirmado por Gary Gensler de la SEC, al sostener que los criptoactivos fungibles no son valores negociables. Véase Cohen, Strong, Lewin, & Chen (2022).

¹⁷ Se comparte el criterio de la SEC en su análisis del caso “TheDAO” en 2017. Véase *TheDAO Report* (SEC, 2017). En el caso “Coinbase”, un tribunal le dio la razón a la SEC respecto de trece tokens en litigio que son considerados valores negociables ofertados sin registro previo (cfr. Latham & Watkins, 2024).

¹⁸ En este sentido, véase la decisión de julio de 2024 en el caso “Binance” (District of Columbia, SEC v. Binance Holdings, 2024). Allí la jueza Berman Jackson sostiene: “[...] it is worth noting that intangible digital assets do not fit neatly into the rubric set forth in the mere seven pages that comprise the Howey opinion. Also, the agency’s decision to oversee this billion dollar industry through litigation – case by case, coin by coin, court after court – is **probably not an efficient way to proceed, and it risks inconsistent results that may leave the relevant parties and their potential customers without clear guidance** [...] The question as to **what motivated the reasonable purchaser at the time** may prove to be a close one. As the court observed in the Telegram case, “[a] transaction does not fall within the scope of the securities laws when a reasonable purchaser is motivated to purchase by a consumptive intent.” In that case, **the existence of an extended lockup period** was one aspect of the first round of the offering that in the court’s view “tend[ed] to negate the likelihood that a reasonable [purchaser] purchased [the tokens] for consumptive use.” (“Simply put, a rational economic actor would not agree to freeze millions of dollars for up to 18 months... if the purchaser’s intent was to obtain a substitute for fiat currency.”); Ripple Labs I, 682 F. Supp. 3d at 328 (**the Institutional Buyers’ agreement to lock up the tokens was viewed as an additional factor supporting the reasonable expectation of profit element, as it was not consistent with the use of the tokens as currency**). While that does not mean that the converse is true, i.e., that the absence of a lockup period shows that consumption was the motivation for the purchases, it is notable that **there were no restrictions on even the first purchasers’ use of their BNB**. It is also significant that one key selling point of the BNB coin detailed in the Whitepaper was that **purchasers could use BNB to pay for any fees on the platform, including exchange fees, withdrawals fees, listing fees, and any other fees, and that when they used BNB to pay those fees, they would receive significant discounts: 50% the first year, 25% the second year, 12.5% the third year, and 6.75% in year four**. This could support a contrary finding at a later stage in these proceedings that it was the ability to utilize the BNB to obtain discounts that served as the incentive for participation in the ICO [...] Will an evaluation of the totality of the circumstances surrounding sales after the ICO support the requisite finding that Binance’s representations created an expectation on the part of the reasonable purchaser of profits in the form of a financial return on the investment? Or **was the company urging the reasonable purchaser to acquire the coins to use them?** While it is not necessary that each offeree purchase the asset that is the subject of an investment contract as an investment [...] **it does matter how the asset was sold and what a purchaser in the marketplace would have reasonably understood it to be**, and the complaint contains very little concerning how BNB was actually promoted and sold after the ICO [...] The Court is inclined to agree with the approach of the court in Ripple Labs, since **the “it-is-what-it-is” approach of the SEC appears to be inconsistent with the clear Supreme Court directives quoted in its pleadings, which hold that it is the economic reality of the particular transaction, based on the entire set of contracts, expectations, and understandings of the parties, that controls**. (“[E]ven if these assets have some inherent use ... [w]hat matters are the ‘economic inducements’ used to encourage the transaction. [...] **All of the relevant circumstances surrounding the sale of the asset must be analyzed**.”). The SEC repeatedly hearkens back to “the circumstances under which the assets in this case were offered and sold,” **but those do not go so far as to establish its contention that “BNB is offered and sold an investment contract**.” One cannot argue with the general proposition that once a thing is deemed to be a security, it remains a security; the thing has not changed its nature. **But the SEC is not alleging or asking the Court to find that the thing in question – the BNB token – is a security. Its allegation is that during the ICO and after, it was offered as, or sold as, a security**. That determination, the SEC has explained, does not depend on the nature of the thing. It does not depend on what the thing represented. It depends on the economic reality of the transaction. SEC, Strategic Hub for Innovation & Fin. Tech., Framework for “Investment Contract” Analysis of Digital Assets (2019), <https://>



*asset tokens*¹⁹. Incluso en una acción de clase, sin participación de la SEC, un tribunal certificó que ciertos *asset tokens* digitales y únicos son equivalentes a un valor negociable ilegalmente ofrecido al público (Drylewski, Levi y Michael, 2023).

Es evidente cómo la ausencia de acción legislativa adecuada y oportuna y la ausencia de definiciones claras, han puesto en cierta desventaja al pujante sector Fintech norteamericano con relación al sector Fintech europeo, que ya sancionó regulaciones para un *sandbox* (espacio controlado de pruebas) financiero comunitario (Ledger Insights, 2024), que permite la tokenización de instrumentos de inversión (“ESMA clarifies...”, 2024), como también reguló la emisión y el uso de *utility tokens* (*tókenes de utilidad*), *stablecoins* y *tókenes de dinero electrónico* (González, 2022) (aunque de momento no regula los *asset tokens* ni DeFi²⁰), e incluso promueve un régimen de identidad digital autosoberana en el reciente Reglamento eIDAS2 (“The European Digital...”, 2024).

Luego de años de debate en el Congreso de los EE. UU.²¹, un proyecto de ley conocido como FIT21 obtuvo media sanción en mayo de 2024 (Financial Services Committee, 2024), y probablemente se apruebe o fusione con otro proyecto en el Senado durante 2025. Se trata del proyecto impulsado por la industria de los activos

perma.cc/46KZ-P5EA (“Framework Analysis”) (“Whether a particular digital asset at the time of its offer and sale satisfies the Howey test depends on the specific facts and circumstances.”) [...] It may be that the SEC can establish that sales after the ICO or certain groups of secondary sales meet the criteria of an investment contract. e.g., Telegram, 448 F. Suppl. 3d at 380–81 (finding based upon all of the surrounding facts and circumstances that secondary sales of the crypto currencies at issue were an offering of securities under Howey because the crypto currencies were initially sold with the intent that the institutional buyers re-sell them on the secondary market; Telegram did not intend for the assets to “come to rest with the 175 Initial Purchasers but to reach the public at large via post-launch resales by the Initial Purchasers” and built incentives into the initial sales to ensure that the initial purchasers resold soon after launch). **But the government’s reliance on the assertion that “[t]he crypto assets are the embodiment of the investment contract,” and its argument at the hearing about the nature of the technology and the interdependence of the platform and the performance of every token, is not enough, standing alone, to bring secondary sales of BNB under the investment contract rubric.** Moreover, the agreement is somewhat inconsistent with the singular theory the government has been advancing since this action was filed: we aren’t saying that the coins are securities – we are talking about investment contracts [...] **Insisting that an asset that was the subject of an alleged investment contract is itself a “security” as it moves forward in commerce and is bought and sold by private individuals on any number of exchanges, and is used in any number of ways over an indefinite period of time, marks a departure from the Howey framework that leaves the Court, the industry, and future buyers and sellers with no clear differentiating principle between tokens in the marketplace that are securities and tokens that aren’t. It is not a principle the Court feels comfortable endorsing or applying based on the allegations in the complaint, particularly since the only term among the approximately twenty options included in the statutory definition of “security” that is being relied upon in this case is “investment contract [...].** For these reasons, the Court will apply the only test the government has offered for assessing for whether a non-traditional asset is a security, and it finds that **the complaint does not include sufficient facts to support a plausible inference that any particular secondary sales satisfy the Howey test for an investment contract.** The SEC argues in its opposition and at the hearing that there were ongoing representations about the superiority of the platform that allegedly gave the tokens their value, but more is needed. It may well be, as the government maintains, that the “common enterprise” is ongoing, since the fortunes of all token holders rise and fall together and that their fortunes are largely tied to those of the company and its platform or “ecosystem,” but that element alone is not sufficient. What about the investment of money? Other courts have not been troubled by payments made to an exchange instead of the issuer, see, e.g., SEC v. Coinbase, Inc., 2024 WL 1304037; Terraform I, 684 F. Supp. 3d at 197; In re Ripple Labs, Inc. Litig., (declining in a private securities class action to find, based on those decisions, that there was no “investment of money” as a matter of law). **And more importantly, the facts needed to plausibly allege an “expectation of profits” in the form of a return on an investment have not yet been alleged.**” (Ampliar en Paul K. Drexler, 2023) (los resultados son nuestros).

¹⁹ Para la CFTC, Bitcoin es un commodity. Véase: https://www.cftc.gov/sites/default/files/2019-12/oceo_bitcoinbasics0218.pdf

²⁰ Sin embargo, la Comisión Europea trabaja ya en MiCA 2.0 (Heredia, 2023).

²¹ Para una revisión de los principales proyectos de ley presentados al Congreso de EE. UU., véase <https://blockworks.co/news/crypto-bills-in-house-and-senate>



digitales en su conjunto. En procura de una mayor claridad regulatoria, FIT21 trae consigo algunas definiciones clave: (i) eliminaría de la definición legal de valores los contratos de inversión que se registran en una cadena de bloques; (ii) se abandonaría el Howey Test, que toma en cuenta las realidades económicas de una inversión para determinar si está sujeta a las leyes federales de valores negociables; (iii) se excluyen de la definición de *Exchanges* los *crypto asset trading systems*; (iv) se permite que los *crypto asset trading systems* aglutinen varias funciones²²; (v) expresamente decide no regular a cualquier entidad u organización que califique dentro de la definición de “Finanzas Descentralizadas”, y, finalmente, (vi) crea un nuevo régimen de oferta privada, y exenta de registro, para tóquenes de seguridad (*security tokens*), donde inversores minoristas (*retail*) pueden invertir hasta el 10 por ciento de su patrimonio neto o de sus ingresos anuales.

Del otro lado del Atlántico, en Alemania, se sancionó a finales de 2023 una nueva ley de financiamiento *startup*, conocida como *Future Financing Act*²³, que habilita la tokenización de acciones (ya se permitía la tokenización de deuda desde 2022 [Heise, 2021]). A esta renovación legislativa, se suma un regulador muy proactivo (BaFin), presidido por Mark Branson, quien liderara FINMA durante 10 años (Bafin, s. f.), que excluyó de su competencia y jurisdicción, por ejemplo, ciertos tipos de NFT²⁴ y los *utility tokens* (Garrido, 2023). Estas reformas inteligentes le han permitido a Alemania ser, en 2024, el lugar de la mayor emisión tokenizada de un bono por parte de un banco público (Ledger Insights, 2024).

Por otro lado, es notable el rasgo holístico del enfoque reformista alemán, porque también ha modificado otros aspectos normativos en claro beneficio de las

²² Este ha sido un punto crítico que la SEC ha sostenido en varias de sus demandas: “These regulations have generally led to the separation of key intermediaries in the securities markets including the **separation of brokers and dealers from exchanges and clearing agencies** thereby protecting investors and their assets from the **conflicts of interest and risks that can arise when these functions merge**” ... Asimismo, al demandar a Kraken, la SEC sostuvo que este tipo de empresas “perform various other functions, in that they also typically solicit, accept, and handle customer orders for securities; allow for the interaction and intermediation of multiple bids and offers resulting in purchases and sales; act as an intermediary in making payments or deliveries, or both; and maintain a central securities depository for the settlement of securities transactions. (...) In U.S. securities markets, the functions of “exchanges,” “broker-dealers,” and “clearing agencies” described above are **typically carried out by separate legal entities that are independently registered and regulated by the SEC**. Separation of these core functions aims to minimize conflicts between the interests of securities intermediaries and the investors they serve. Registration and concomitant disclosure obligations allow the SEC to oversee the business of intermediaries and their relationship with investors, in order to, among other things, protect investors from manipulation, fraud, and other abuses” (District of California, SEC vs. Payward, Inc. 2023).

²³ Confr https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Financial_markets/Articles/financing-for-the-future.html#:~:text=On%20the%20opportunities%20for%20growth%2Dstage%20companies

²⁴ “To date, BaFin is not aware of any NFTs that would have to be classified as securities for supervisory purposes. One reason is that the tokens have so far lacked embodied rights comparable to securities. Another reason is that NFTs are usually given individual rights and contents, and this rules out standardisation and thus negotiability in terms of the supervisory definition of securities” [...] “The use of NFTs that is currently to be observed, however, especially in cases where they are used to tokenise digital works of art, does not necessarily point to designation as a financial instrument in the form of a capital investment or a debt security. These NFTs generally lack further financial rights; where individual tokens have individual contents, the necessary level of standardisation is missing. Without this interchangeability, there can also be no classification as a unit of account. In the case of fragmented NFTs, where fungible tokens each represent an equivalent share of an NFT, this interchangeability requirement would generally be met, however” (Heinrich et al., 2023).



startups, al otorgar beneficios impositivos mediante el diferimiento del hecho imponible cuando se otorgan acciones para empleados (en el marco de *Employee Stock Option Plans* —ESOP— [Bosse, 2020; Washington College, s. f.]) o cuando se *vestean* para los socios fundadores, es decir, cuando el diferimiento impositivo se aplica también a las acciones liberadas que solo podrán transferirse si la empresa da su aprobación (acciones nominativas con transmisibilidad restringida), lo que permite aplazar impuestos sobre las acciones transferidas hasta que efectivamente se vendan, además de prever una desgravación fiscal específica de 2.000 € al año.

También se facilita a las *startups* la salida al mercado de capitales, reduciendo a un millón de euros el capital mínimo requerido para una oferta pública inicial (IPO) (como ya lo hacen las bolsas de Madrid [BME, 2023] y Santiago [Scalex, s. f.]), y ya se piensan nuevas formas de bajar los costos de una IPO²⁵. Finalmente, se admite en Alemania la emisión de acciones con voto múltiple, con derechos de voto de hasta 10 votos por acción, lo que permitiría a los fundadores retener el control de la *startup*, a medida que diluyen o apalancan el capital social en los mercados de capitales. Así, los emprendedores están en mejores condiciones de conservar la influencia sobre las empresas que fundaron y, como resultado, de seguir utilizando su experiencia para facilitar su crecimiento.

Brasil

Con la renovación de importantes aspectos de su derecho privado en los últimos tres años, Brasil se ha convertido en un gigante Fintech, usina de innovación y experimentación que debe seguirse atentamente.

La Ley 182 de 2021 (ley de *startups* [Mattos Filho's Corporate, 2022; v. t. Dos Santos, 2021]), que permitió la tokenización de acciones, y la Ley 14.478 de 2022²⁶, que regula a los proveedores de servicios de activos virtuales, y define los activos virtuales como representaciones digitales de valor que pueden ser intercambiados o transferidos por medios electrónicos y son usados como medios de pago o de inversión. Esta regulación excluye el dinero electrónico o fiduciario tokenizado, también los tókenes de utilidad (*utility tokens*, definidos como instrumentos que brindan a sus titulares el acceso a productos o servicios específicos, o a cualquier beneficio de los mismos, como puntos y recompensas en programas de lealtad), así como los valores y activos financieros, regulados en otras normas (Ley 14.478, art. 3). Existen

²⁵ Se han constatado eficiencias y ahorros de hasta 25 bps en el costo de securitización de ciertos activos en China. Véase: Liu, J., Shim, I., & Zheng, Y. (August, 2023). Absolute blockchain strength? Evidence from the ABS market in China. *BIS Working Papers*, 1116. <https://www.bis.org/publ/work1116.htm>

²⁶ Law No. 14,478, of December 21, 2022, Mattos Filho. <https://www.mattosfilho.com.br/wp-content/uploads/2022/12/law-no-14478-of-december-21-2022.pdf>



además varios usos de *sandbox* regulatorios desde 2020, tanto en el Banco Central de Brasil (s. f.) como también en la Comisión de Mercados y Valores (Wright, 2023).

En el ámbito del sector público, en Brasil no solo se experimenta con el DREX (Banco Central do Brasil, s. f.), sino también con la búsqueda de la tokenización del gasto público federal²⁷, y la utilización de cadena de bloques (*blockchain*) e inteligencia artificial en distintos experimentos que buscan optimizar las compras públicas a nivel subnacional (Oliveira et al., 2022; Souza et al., 2023; TCU, s. f.).

La necesidad de avanzar hacia la libertad de formas y de registros

Ya habíamos afirmado en otra parte (Heredia y Bertoni, 2024) que el impulso reformista liberal libertario plasmado en el DNU 70/23 no ha llegado con tanta euforia y fuerza a la materia de las formas libres de los actos jurídicos (Heredia y Bertoni, 2024). Ya es reconocido que, si bien nuestro sistema consagra la libertad de formas (art. 284 CCC) como regla, en los hechos esta libertad se transforma en la excepción en razón de la reglamentación de contratos y de las prácticas diarias.

La forma en la relación jurídica es la manera como el ordenamiento permite que se exteriorice la voluntad de la persona respecto del objeto, y se la ha caracterizado tanto como elemento esencial del acto, como aspecto ineludible de la voluntad del agente. Es la *puesta en escena de la voluntad* del agente que se produce de diversos modos, aunque la ley puede exigir ciertas formas en función de la trascendencia económica o social de un acto dado, por ejemplo: las formas *ad solemnitatem* de escritura pública para donar inmuebles o muebles registrables, la presencia del oficial público para el matrimonio, o la redacción, firma y fecha de puño y letra del testamento bajo forma privada (Herrera y Bertoni, 2024).

Históricamente, la forma desempeñó un papel muy importante en los sistemas antiguos, y prácticamente llegó a suplir el consentimiento de las partes. Posteriormente, la forma comenzó poco a poco a convertirse en un elemento de prueba de la relación jurídica, que permite proteger tanto a las partes del acto, como a terceros interesados. Si bien forma y prueba son conceptualmente distintas, en tanto la prueba demuestra la existencia de un acto y la forma exterioriza la voluntad del sujeto del acto, las formas pueden clasificarse, en relación con la prueba, en formas *ad probationem* y *ad solemnitatem*, pues solo estas exteriorizan una voluntad intrínsecamente vinculada con la existencia misma del acto (Conte-Grand, 2016, p. 791, citado en Herrera y Bertoni, 2024, p. 20).

²⁷ Véase el Acuerdo de Cooperación (Nº D-121.2.0014.22) que celebraron entre sí el Banco Nacional de Desenvolvimento Econômico e Social (BNDES) y el Tribunal de Contas da União (TCU), "para cooperação com vistas à formação da Rede Blockchain Brasil (RBB). (Processo No. TCU: TC 039.840/2021-2)". <https://github.com/RBBNet/rbb>; <https://github.com/RBBNet/rbb/blob/master/documentos/ACT%20-%20Documento%20firmado%20entre%20BNDES%20e%20TCU.pdf>



Entre todas las formas, la instrumental se transformó en la manera de exteriorizar la voluntad por antonomasia, y se reconocieron dos especies de instrumentos: los públicos y los privados (y los instrumentos particulares no firmados, Art. 287, CCyCN), según se cumplan los recaudos para cada caso. En los instrumentos públicos, la presencia del oficial o del agente público dotaba de eficacia probatoria *erga omnes*, salvo redargución civil o querella criminal. En los instrumentos privados, la eficacia probatoria entre partes y sus sucesores universales nace una vez reconocida la firma, y respecto de sucesores singulares, cuando el documento obtiene fecha cierta (véase Arts. 287, 314 y 317, CC y CN). Cabe preguntarse si el sellado de tiempo (*time stamping*), tan usado en las redes de registro distribuido, no es un hecho tecnológico cuya consecuencia ineludible es determinar la firma fechada de un documento digital con firma electrónica.

Como hemos dicho, en nuestro derecho, la libertad de formas está basada en el Art. 284, CCyCN, que postula: “Libertad de formas. Si la ley no designa una forma determinada para la exteriorización de la voluntad, las partes pueden utilizar la que estimen conveniente. Las partes pueden convenir una forma más exigente que la impuesta por la ley”.

Siguiendo esta línea, puede afirmarse que la forma jurídica es actualmente un recurso del Derecho para resguardar: (i) a quien firma, ológrafa o electrónicamente²⁸, un instrumento cuyo contenido se encuentra legalmente determinado, (ii) a su contraparte —si existe—, y (iii) a los terceros que tengan un interés legítimo, incluyendo al Estado. En este último caso, por razones fiscales o de prevención de lavado de activos, o por lucha contra la corrupción, el Estado y el tercer sector tienen un interés legítimo en conocer las partes de ciertos actos jurídicos y a sus beneficiarios finales; esta es también una exigencia del Grupo de Acción Financiera Internacional (GAFI). Tanto en el ámbito bancario como en el mercado de capitales, las nuevas infraestructuras tecnológicas permitirán, con el tiempo, demostrar que “la confianza es un sustituto imperfecto de la información”. Las redes de registro

²⁸ Ya se ha referido antes en la nota 4(13) a la segunda generación de leyes de firma electrónica, basadas en la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre documentos transmisibles electrónicos, del 13 de julio de 2017, cuyo objetivo es hacer posible el uso de los documentos transmisibles electrónicos en el marco del derecho, tanto a nivel nacional como internacional. La Ley Modelo se aplica a los documentos transmisibles electrónicos que son funcionalmente equivalentes a los documentos o títulos transmisibles emitidos en papel. Estos últimos son documentos o títulos en papel que facultan a su tenedor para reclamar el cumplimiento de la obligación indicada en ellos y que permiten transmitir el derecho a obtener el cumplimiento de esa obligación mediante la transmisión de la posesión del respectivo documento o título. Entre los documentos o títulos transmisibles emitidos en papel más usuales se encuentran los conocimientos de embarque, las letras de cambio, los pagarés y los certificados de depósito, que son instrumentos comerciales esenciales. Su disponibilidad en forma electrónica puede contribuir enormemente a facilitar el comercio electrónico, por ejemplo, aumentando la velocidad y la seguridad de la transmisión, permitiendo la reutilización de los datos y automatizando determinadas operaciones mediante “contratos inteligentes”. Los documentos transmisibles electrónicos pueden tener especial relevancia en el comercio, como el transporte y la logística, y en *fintech*, especialmente para crear un mercado de certificados de depósito electrónicos para facilitar el acceso del agro al crédito. “La Ley Modelo sobre Documentos Transmisibles Electrónicos se basa en los principios de no discriminación contra el uso de medios electrónicos, equivalencia funcional y neutralidad tecnológica. Puede dar cabida a la utilización de todas las tecnologías y todos los modelos, como el sistema registral, el de tokens o el de registros descentralizados”.



distribuido no solo facilitan el acceso a la información relevante, sino que también pueden servir como *data sets* para entrenar modelos de *machine learning* supervisado o no supervisado con distintas finalidades, y además usar DLT para registrar transacciones financieras que pueden ser identificadas de una manera única, incluyendo a las partes de la operación, y la dirección del *smart contract* en redes públicas (ESMA, 2023). En sintonía con ello, se ha definido que la *blockchain* sería la “nueva arquitectura de confianza” (Werbach, 2018).

Ahora bien, aun lógicamente antes de firmar un documento, repárese en que el CCyCN dispone que la “expresión escrita —lo que se firmará— puede constar en cualquier soporte”, siempre que su contenido sea representado con algún tipo de texto inteligible y aunque su lectura exija medios técnicos (p. ej., el código de un *smart contract*, o la vinculación de *data sets* que lleven el registro de saldos y consumos transables, y que permitan microtransacciones automatizables condicionales, por ejemplo, condicionando el pago de una carga de energía para un vehículo eléctrico a la preexistencia de saldo o a la apertura de crédito en una billetera digital). También dispone el CCyCN que una firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde, aunque su lectura exija medios técnicos.

En los instrumentos electrónicos, el requisito de la firma queda satisfecho si se utiliza una firma digital, que asegure sin duda alguna la autoría e integridad del instrumento —p. ej., un documento tokenizado, es decir, un tipo de documento electrónico, incluyendo sus agregados y modificaciones—, registrado en una red pública, híbrida, o privada de registros distribuidos —una red de tipo *blockchain*, especie de DLT—, e inmutablemente asociado a una dirección y a una llave pública existentes en dicha red, las cuales ya han sido asociadas a una identidad de una persona humana o jurídica previamente identificada, y que cuando es modificado deja huellas digitales cronológicamente inmutables (sellado de tiempo).

El hecho actual de que tales actos y contratos estén en un registro digital, centralizado y administrado por una jurisdicción dada, con el fin de dar publicidad y seguridad jurídica a terceros, se puede contrastar con la posibilidad, a opción del interesado, de habilitar el uso de potenciales registros alternativos²⁹, también digitales, pero que se usan para otro tipo de información —p. ej., la red pública de *blockchain* de Bitcoin orquestada con una red privada, Exonum, usadas en tándem para registrar títulos de inmuebles en Georgia³⁰—.

Al final del día, independientemente de quién cree, opere o mantenga el registro, los registros quizás sean públicos siempre y cuando permitan que se identifique perfectamente al firmante y que el momento de la firma quede registrado

²⁹ Como se permite, por ejemplo, en Delaware desde 2017. Véase: Eggert, A., and Eraso, Y. (2017). Delaware Blockchain Initiative: Revitalizing European Companies' Funding Efforts. Harvard Law School Forum on Corporate Governance. <https://corpgov.law.harvard.edu/2017/09/21/delaware-blockchain-initiative-revitalizing-european-companies-funding-efforts/>

³⁰ Véase: “Improving the security of a government land registry”. Exonum. <https://exonum.com/story-georgia>



en una red inmutable de registros distribuidos públicamente visibles (o visibles con ciertos permisos³¹).

Ahora bien, el mismo CCyCN dispone en su artículo 969 que cuando la ley o las partes no imponen una forma determinada, esta debe constituir solo un medio de prueba de la celebración del contrato.

Puesto todo lo anterior en perspectiva, cabe preguntarse si la forma es, contemporáneamente, una cuestión probatoria (incluyendo la publicidad de ciertas circunstancias, a través de decimonónicos sistemas de registro a los que acceden los instrumentos públicos): ¿por qué no podrían las partes convenir una forma tecnológicamente más exigente —o más robusta, incluso inmutable— que las formas tradicionales que la ley designa para los contratos formales³²?

En este sentido, desde el sector Fintech argentino, a su turno, se ha propuesto legislar nuevos servicios profesionales de constatación (notarial o de valuación a mercado) de activos digitalizados, lo que permitiría una reconversión profesional de escribanos y profesionales de las ciencias económicas de cara a la nueva economía digital³³.

³¹ En materia aduanera, un interesante uso piloto de la tecnología permite a las aduanas del Pacífico coordinar mejor el servicio dispensado a los llamados Operadores Económicos Autorizados. Se trata de una aplicación de Blockchain al sistema aduanero a través de un proyecto piloto realizado con el BID y Microsoft, que utiliza esta tecnología para mejorar la seguridad y la eficiencia de sus acuerdos de reconocimiento mutuo (ARM) aduaneros y de sus programas de operador económico autorizado (OEA). Las aduanas de Colombia, Chile, México y Perú, que conforman la Alianza del Pacífico, firmaron un ARM; también se están negociando otros ARM entre países de Centroamérica, de la Comunidad Andina y del Mercosur. Estos acuerdos implican que los participantes comparten los datos relacionados con las certificaciones más recientes de OEA, algo muy difícil de lograr y que típicamente se realiza mediante intercambios de correos electrónicos entre las aduanas. Al utilizar Blockchain, dichas aduanas tendrán acceso a la misma información, almacenada de un modo seguro y cargada una sola vez en un único lugar. Esto también les asegura a los operadores de comercio el acceso a los beneficios del ARM desde el momento en que reciben la certificación de OEA. Véase: Proyecto Cadena, IDBLab, Lacchain, 2020. <https://publications.iadb.org/es/revista-integracion-comercio-ano-24-no-46-diciembre-2020-blockchain-y-comercio-internacional-nuevas-tecnologias>.

³² En cuanto a la equivalencia funcional de registros distribuidos en relación con registros centralizados, sirven como antecedentes la reciente legislación alemana, que permite usar registros distribuidos públicos o privados para emitir deuda o acciones tokenizadas, y la Ley Modelo de Uncitral sobre DET (respecto de documentos que no se consideren valores negociables), que propone interpretar que cuando la ley requiera que la información conste por escrito, ese requisito se dará por cumplido respecto de un documento transmisible electrónico, si: (i) la información contenida en él es accesible para su ulterior consulta —Art. 8—; (ii) si la firma en relación con un documento transmisible electrónico utiliza un método fiable para determinar la identidad de esa persona y para indicar la voluntad que tiene esa persona con relación a la información contenida en el documento transmisible electrónico —Art. 9—; (iii) si la fecha y hora o el lugar con respecto a un documento o título transmisible emitido en papel, se obtiene con un método fiable para indicar la fecha y hora o el lugar con respecto a un documento transmisible electrónico; y (iv) el endoso de un DET se considerará cumplido si la información exigida para el endoso está incluida en él, y esa información cumple los requisitos establecidos en los artículos 8 (forma) y 9 (firma). Véase: Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). (2018). Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/mletr_ebook_s.pdf

³³ Véase: Cámara Argentina Fintech (2023). Tokenización de activos: análisis y propuestas para el desarrollo de la industria en Argentina. <https://camarafintech.org/tokenizacion-de-activos-reales-propuestas-y-analisis-para-impulsar-el-desarrollo/>. El artículo propone modificar la legislación de fondo para permitir el desarrollo de servicios de constatación física de activos físicos reales, de modo que se permita asegurar *erga omnes* su real existencia y su naturaleza, gravámenes, los antecedentes de su valuación, y los requisitos especiales para su custodia física, previo a poder ser tokenizados con plenos efectos legales, siguiendo el régimen de Liechtenstein creado por la ley conocida como TVTG, y su licencia de "Validador Físico", la que podría ser adaptada a nuestro país, de modo tal que los notarios puedan ofrecer servicios de constatación y los contadores, servicios de valuación del activo previo a su tokenización.



También hemos afirmado antes (Heredía y Bertoni, 2022a) que las *nuevas formas* que envuelven viejas sustancias no necesariamente crean nuevas sustancias. Téngase presente, además, que el fin último de las formas ha sido y es proteger a quien dispone o adquiere algo de valor y hacerle oponible la adquisición (o disposición) al resto de la comunidad.

Si se acepta el argumento anterior como hipótesis, cabe preguntarse entonces si es válido afirmar que, al menos en el ámbito de los activos digitales criptográficos, los datos almacenados en registros (sean públicos y distribuidos, híbridos, o sean centralizados en los clásicos registros “públicos”, digitalizados o no³⁴) son *per se* una forma más de potencialmente dar a conocer a la comunidad una situación de hecho en un momento dado en el que, curiosamente, el dominio (i.e. el control de las llaves privadas de un activo criptográfico) y la posesión (i.e. la publicidad en y de un registro distribuido) se funden en un solo atributo, propio e inmanente a los criptoactivos. Sostener la tesis anterior implica también afirmar que, en el ámbito de los activos criptográficos, no podrían existir los viejos conflictos analógicos de poseedores sin derechos (o dueños sin posesión).

Sin embargo, a tenor de los hechos, en el ámbito de los activos criptográficos se pueden aún replicar ciertos conflictos por la afectación del dominio (i.e. robo de llaves privadas por ciberataques a los proveedores de servicios que las “custodian”), aunque en esta nueva época, el despojo dejará rastros *on-chain* en registros distribuidos, generalmente inalterables (Chainalysis, 2024). Esto puede, sin duda, implicar una revolución en la forma de crear, representar e intercambiar valor en una comunidad, pero también en la forma de gestionar, auditar y controlar los fondos y flujos, en tanto estos y aquellos se representen al amparo de la economía del token.

Conclusiones

Los activos digitales (en general) y los tókenes criptográficos (en particular) representan una innovación fundamental en la economía del naciente siglo XXI, es indiscutible su potencial para transformar diversos sectores económicos, sin embargo, enfrentan desafíos significativos en términos de regulación, seguridad y adopción. Con el avance de la tecnología y la evolución de los marcos regulatorios, es muy probable que los activos criptográficos cumplan un papel cada vez más importante en la economía global.

En Argentina actualmente el desarrollo empresarial es bajo. En 2021 el promedio de empresas activas era de solo 1.195 por cada 100.000 habitantes, siendo

³⁴ Véase, en este sentido, el análisis con relación a un registro de la propiedad ya digitalizado, en el dictamen emitido por la Sala Blockchain e Inteligencia Artificial del Instituto de Gestión en Sistemas de Justicia de la Facultad de Derecho y Ciencias Sociales de la Universidad Católica de Córdoba. <https://finanzas.cba.gov.ar/wp-content/uploads/2021/03/DICTAMEN-de-la-SALA-BIA-UCC-al-RGP-CÓRDOBA-firmado.pdf>



significativamente menor a Brasil y Chile, con 2.219 y 6.696 empresas por cada 100.000 habitantes, respectivamente (Observatorio Pyme, 2022). Sin embargo, Argentina es el país de Latinoamérica con más unicornios por cantidad de habitantes, y lidera en el ámbito *DeepTech* (Lacube, 2021; Reinhold, 2023).

No obstante lo anterior, son las Mipymes las que mueven la economía³⁵, y generalmente eligen sociedades por acciones simplificadas (SAS) como vehículo jurídico. A fines de 2023, según AFIP, el 76 % de todas las SAS se concentró en apenas cinco provincias: el 29,3 % de todas las SAS constituyó su sede en la provincia de Córdoba; el 19,8 %, en la Ciudad de Buenos Aires; 12,4 %, en la provincia de Buenos Aires; 10,6 %, en la provincia de Mendoza, y 3,9 %, en la de Santa Fe (Lukin y Marano, 2023, p. 7).

Sin dudas, las *nuevas formas de omnicanalidad* comercial impactarán en muchas industrias y sectores (i.e. desde modelos de *Play-to-Earn* y *Learn-to-Earn*, hasta NFT en formato PoAP³⁶ y NFT usados para representar derechos asociados al origen 100 % digital de créditos con y sin garantías, etc.), y las *nuevas formas de financiamiento* empresarial pueden ser útiles herramientas para aumentar las pobres métricas patrias, por ejemplo, desde la tokenización de acciones, ONs y avales, la creación de un micropanel bursátil para *startups*, como los que ya existen en Chile, España y Alemania, hasta las Finanzas Descentralizadas que experimentan con *DAO-based crowdlending/funding*³⁷, etc.

Es más, estas nuevas tecnologías, especialmente las DLT, pueden incluso ser una condición necesaria, pero no serán condición suficiente, para multiplicar la cantidad de empresas del país. Son también necesarias ciertas reformas tributarias (un buen precedente es el ejemplo alemán con relación a beneficios fiscales para ESOP) que incentiven y estimulen la inversión *de riesgo* (especialmente en el segmento de *inversión ángel*, que es el que asume *el mayor riesgo*, y donde los esquemas de beneficios fiscales para inversión ángel de Noruega e Israel son buenos ejemplos [Daher y Davidovich, 2023; Norwegian Tax Administration, s.f.]), como también la continua utilización *inteligente* de fideicomisos públicos que co-inviertan (*matching funds*) con fondos privados de capital emprendedor (los ejemplos de CORFO con StartUp Chile [CORFO, 2024] y la experiencia de Israel con YOZMA [Avnimelech, 2009] son prácticas ya conocidas).

Sin embargo, lo más urgente y necesario es dinamizar el crédito, tanto para las empresas como para sus clientes, usuarios y consumidores. A tal fin, de ser necesario

³⁵ Véase: Gigli, P. (2022). ASEA (<https://www.eldiarioweb.com/2022/09/los-unicornios-son-una-gran-referencia-pero-son-las-pymes-las-que-mueven-la-economia/>): "Si tuviera que destacar problemas concretos que existen actualmente, podemos mencionar lo relativo a la formalización de una empresa, el tema impositivo, la burocracia, los trámites y conseguir efectivamente financiamiento para poder desplegar un proyecto y que emprender sea más fácil".

³⁶ Véase: <https://wiki.lemon.me/nfts/que-significa-poap-proof-of-attendance-protocol/>

³⁷ El caso Societé Generale, que obtiene un préstamo en el criptoactivo estable Dai, provisto por MakerDAO, aceptando los tokens OFH como garantía, es un primer paso hacia la vinculación del mundo financiero centralizado y el descentralizado. Los fondos VC estructurados como DAO, autogestionados por sus inversores, pero pertrechados de un ropaje jurídico societario robusto, son también un avance promisorio, como ilustra el caso TheLAO (véase: <https://thelao.io>).



o conveniente, también se deberán redefinir las *garantías bancarias preferidas*³⁸ (habida cuenta de la manifiesta utilidad de los *smart contracts* [Heredia, 2020] originalmente pensados para servir como *garantías inteligentes auto-ejecutables*); ello mientras se sigue promoviendo la innovación en materia de una mayor apertura hacia nuevos medios de pago (Crawley, 2023), ampliando las inversiones tradicionales, regulando las inversiones alternativas (Amaya, 2022; v.t. OECD, 2024)³⁹, pero también impulsando las microinversiones y el *open banking*⁴⁰.

Con mejor financiación y con nuevas formas de comercialización, las empresas nacientes pueden mejorar su probabilidad de supervivencia, en parte por más y mejores formas de financiar su nacimiento y crecimiento y el desarrollo y la adaptación tecnológicos que requieren los nuevos sistemas de gestión de la información, mientras se ingresa en otra era de la Internet con la computación cuántica como servicio —QaaS— (Nature Research Custom Media, s. f.) acelerando aún más los desarrollos actuales de inteligencia artificial impulsados por los llamados *Modelos de Fundación* (o Modelos Fundacionales) (v. <https://crfm.stanford.edu>), la *GenAI*

³⁸ Véase: Heredia Querro, S. (2017). Financiación de la construcción con “preventas” y “préstamos puente”. *Comercio y Justicia*. https://comercioyjusticia.info/opinion/financiacion-de-la-construccion-con-preventas-y-prestamos-puente/#google_vignette En 2017, el Banco Central de la República Argentina permitió que los bancos financiaran la compra de viviendas en pozo o en obra —que no son todavía aptas para ser asiento de una hipoteca—, aceptando como garantía preferida “B” el boleto de compraventa y el contrato de fideicomiso (Comunicación A-6250), permitiéndose que los boletos de compraventa y participaciones en fideicomisos se tomen como collateral aforados a 75% o al 50%, según el destino del bien. Esta norma permitió que el banco financiara directamente a los adquirentes finales, y la constructora-vendedora pudiera ceder en garantía todos los derechos que tuviera contra ellos, debiendo acompañar el plano de obra aprobado del cual surgiría la totalidad de unidades proyectadas y los instrumentos de venta certificados (preventas), obteniendo a cambio el financiamiento intermedio necesario para el proyecto. También permitió a las constructoras y desarrollistas obtener financiamiento bancario para construir, ofreciendo como garantías un contrato de fideicomiso de garantía en el cual un fiduciante inmobiliario aporta un terreno libre de gravamen para la ejecución de un desarrollo inmobiliario, y el fiduciario y primer beneficiario es el banco que otorga el financiamiento intermedio para construir, garantizándose el préstamo con el mismo fideicomiso, *step-in rights* y ciertas previsiones contractuales indispensables (que parte del producido de las “preventas” se aplique a cancelar el “préstamo puente”), subordinándose los otros beneficiarios del fideicomiso (por ejemplo: constructora, proveedores y adquirentes) al crédito bancario y consintiendo anticipadamente que el fiduciario pueda disponer del bien en caso de impago del préstamo bancario (garantía autoliquidable por excelencia). Esta reforma permitió la cesión en garantía a favor del banco de (a) boletos de compraventa de grandes superficies o inmuebles ya construidos, donde el cedente ya haya pagado 100% del precio, esté en posesión y tenga un poder irrevocable para escriturar otorgado a su favor por el vendedor; (b) boletos de compraventa con antigüedad no mayor de seis meses, en el cual el cedente haya pagado al menos 60% del precio del inmueble adquirido, tenga permiso de edificación y esté contratado el seguro del Art. 2071 del Código Civil y Comercial de la Nación (CCCN); y (c), derechos beneficiarios en fideicomisos de construcción, cuando surja del contrato la obligación fiduciaria de realizar la obra que el banco financiará, el dominio del inmueble conste a nombre del fiduciario, se haya otorgado permiso de edificación y esté contratado el seguro del Art. 2071 del CCCN. Imagínese la fluidez que se podría imprimir a esta operatoria si se utilizan tokens criptográficos y registros distribuidos para instrumentar, causar, ceder y en su caso ejecutar (vía smart contracts reconocidos como nuevas “garantías preferidas”) los derechos de las partes intervinientes.

³⁹ Con relación a la demanda de finanzas climáticas y el rol de las Fintechs, la OECD (2024) hace una advertencia relevante: “Financial institutions increasingly need and seek out granular data on their clients’ sustainability performance to manage risks, develop financing instruments and meet reporting requirements. Yet SMEs are not as well equipped to provide these data as large entities due to their relatively limited capacities to identify, measure and report on their environmental performance. This poses potential risks to SMEs’ ability to access financing in the future. SMEs also risk losing access to finance if they cannot advance (sufficiently rapidly) on the journey to net zero and/or cannot demonstrate credible transition plans. This is a particularly strong risk for SMEs in high-emitting and hard-to-abate sectors”.

⁴⁰ El reporte del Foro Económico Mundial y la Universidad de Cambridge de 2024 afirma que el primer factor de transformación del sector Fintech será el impacto de la Inteligencia Artificial, y el segundo factor será la Economía Digital, las Finanzas Embebidas y el Open Banking (University of Cambridge y World Economic Forum, 2024). El BIS define al Open Banking como el intercambio y el uso de un esquema de intercambio de datos autorizado por el cliente que permite a los bancos compartir datos con desarrolladores y proveedores de servicios externos autorizados para crear aplicaciones y servicios (BIS, 2019).



(García-Peñalvo y Vázquez-Ingelmo, 2023) y los grandes modelos de lenguaje preentrenados (AWS, s. f.).

Como se dijo al inicio, en nuestro país el crédito al sector privado como porcentaje del PBI es una séptima parte del promedio de la región (5,5 % vs. 39 %). El uso de capital propio es casi el único recurso financiero en compañías de menor escala, lo que deja excluidas innumerables oportunidades de inversión no desarrolladas por falta de capital. A su vez, el salto a la oferta pública de las compañías domésticas es privativo solo de grandes compañías y/o industrias de naturaleza oligopólica/monopólica⁴¹.

Por todo ello, se afirma que fomentar, por un lado, la inversión de riesgo en etapas tempranas de empresas nacientes con beneficios fiscales inteligentes (para el ámbito europeo, v. European Commission, 2017), y adecuar, por otro, las normativas para facilitar y abaratar el acceso al financiamiento dinamizando el crédito en todas sus formas, facilitando y abaratando los regímenes de oferta pública y privada (CNV, 2024) en el mercado de capitales, mediante la adopción de tecnologías más eficientes que las ya empleadas, puede permitir a nuestro país retomar el crecimiento y aumentar drásticamente la cantidad de nuevas empresas, a la vez que se apoya, se financia, el mayor crecimiento y expansión internacional de las ya existentes.

Referencias

- Amaya, T. (2022). Regulating the crypto assets landscape in Japan. <https://www.fsa.go.jp/en/news/2022/20221207/01.pdf>
- Avnimelech, G. (January, 2009). VC Policy: Yozma Program 15-Years perspective. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2758195
- Bafin. (s. f.). Prersident. Mark Branson. Curriculum vitae. https://www.bafin.de/EN/DieBaFin/Leitung/Praesident/praesident_artikel_en.html
- Bains, P., y Wu, C. (June 26, 2023). Institutional Arrangements for Fintech Regulation: Supervisory Monitoring. In *Fintech Notes*. International Monetary Fund. <https://www.imf.org/en/Publications/fintech-notes/Issues/2023/06/23/Institutional-Arrangements-for-Fintech-Regulation-Supervisory-Monitoring-534291>
- Banco Central do Brasil (s. f). Drex - Digital Brazilian Real. Confr. https://www.bcb.gov.br/en/financialstability/Drex_En
- Banco Central do Brasil (s. f). Regulatory Sandbox. <https://www.bcb.gov.br/en/financialstability/regulatorysandbox>

⁴¹ En 2021, CNV creó un Régimen Diferenciado Intermedio de oferta pública, orientado especialmente a emisoras que desarrollen actividades productivas e industriales, buscando impulsar alternativas de financiamiento, a través de la emisión de obligaciones negociables y acciones, para emisoras "Pymes" y/o empresas familiares.



- Bank for International Settlements (BIS). (November, 2019). Report on open banking and application programming interfaces (APIs). Basel Committee on Banking Supervision. <https://www.bis.org/bcb/publ/d486.pdf>
- Bank for International Settlements (BIS). (20 de junio, 2023). Blueprint for the future monetary system: Improving the old, enabling the new. In: *BIS Annual Economic Report*. <https://www.bis.org/publ/arpdf/ar2023e3.pdf>
- Berners-Lee, T. (1991). World Wide Web Project. <https://www.w3.org/People/Berners-Lee/1991/08/art-6484.txt>
- Bolsas y Mercados Españoles (BME). (Diciembre, 2023). BME Growth. Un impulso al crecimiento de las empresas. <https://www.bmegrowth.es/docs/docsSubidos/Presentaciones/Presentacion-BME-Growth-Impulso-crecimiento-empresas.pdf>
- Bosse, M. (30 de septiembre, 2020). Employee Stock Option Program (ESOP) — Best Practices for Startups. <https://mathias-bosse.medium.com/employee-stock-option-program-esop-best-practices-for-startups-e3248795e773>
- Browne, R. (2021). Visa jumps into the NFT craze, buying a ‘CryptoPunk’ for \$150,000 <https://www.cnn.com/2021/08/23/visa-buys-cryptopunk-nft-for-150000.html>
- Browne, R. (2024). Crypto firm Circle gets approval to issue stablecoin in EU under bloc’s strict rules. *CNN*. <https://www.cnn.com/2024/07/01/eu-mica-law-crypto-firm-circle-gets-french-license-for-stablecoin.html>
- Chainalysis Team (enero, 2024). Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises. <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/>
- Cheng Y-H, Hong EY-H, Leung M-Y, Lai S-L, y Yam VW-W. (2021). *Synthesis of benzo[b] phosphole-based alkynylgold(I) complexes with resistive memory properties modulated by donor–acceptor chromophores*. *SmartMat*. <https://doi.org/10.1002/smm2.1065>
- Cohen, L. and Strong, G. and Lewin, F. y Chen, S. (November 10, 2022). *The Ineluctable Modality of Securities Law: Why Fungible Crypto Assets are not Securities*. SSRN. <http://dx.doi.org/10.2139/ssrn.4282385>
- Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). (2017). Ley Modelo de la CNUDMI sobre documentos transmisibles electrónicos (2017). https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_transferable_records
- CORFO (2024). Start-Up Chile. ¿Qué es? <https://www.corfo.cl/sites/cpp/inf/startup-chile>
- CORPORACIÓN INTERAMERICANA DE DESARROLLO (BID Invest) (2022) Informe Anual para el año 2021, junto con los estados financieros para los años finalizados el 31 de diciembre del 2020 y 2021, respectivamente, en cumplimiento de lo estipulado en el Convenio Constitutivo de la Corporación Interamericana de Inversiones, cuya marca es BID Invest. <https://idbinvest.org/es/publicaciones/informe-anual-2021>
- Crawley, J. (abril, 2023). El banco de inversiones de Brasil BTG Pactual lanzó su stablecoin respaldada por el dólar. *CoinDesk*. <https://www.coindesk.com/es/>



- business/2023/04/05/el-banco-de-inversiones-de-brasil-btg-pactual-lanzo-su-stablecoin-respaldada-por-el-dolar/
- Daher, H., y Davidovich, A. (August 16, 2023). Israeli High-Tech: “Angels Law” Grants Tax Benefits to Investors. *Lexology*. <https://www.lexology.com/library/detail.aspx?g=50ea861f-4950-4150-a05d-fb8a90b7cb06>
- Del Valle, L., y Morrow, A. (28 de marzo, 2024). Dictan 25 años de prisión para Sam Bankman-Fried por fraude y conspiración en escándalo de criptomonedas y FTX. *CNN Mundo*. <https://cnnespanol.cnn.com/2024/03/28/25-anos-prision-sam-bankman-fried-fraude-conspiracion-escandalocriptomonedas-y-ftx-trax/>
- Digital Found Foundation. (10 de junio, 2024). *Italian Banking Association Reports Success in Wholesale CBDC Trial Project Leonidas*. <https://digitalpoundfoundation.com/italian-banking-association-reports-success-in-wholesale-cbdc-trial-project-leonidas/>
- Dos Santos, R. A. (6 de junio, 2021). Principales disposiciones de la Ley que estableció el marco legal para las startups en Brasil. <https://es.rastaxlaw.adv.br/post/principales-disposiciones-de-la-ley-que-estableci%C3%B3-el-marco-legal-para-las-startups-en-brasil>
- Drexler, P. K. (2023). Token Wars: How the SEC Can Learn to Embrace Utility Tokens. *Duke Law Journal*, 72(5), 1123. <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=4152&context=dlj>
- Drylewski, A. C., Levi, S. D., y Michael, D. (Feb. 27, 2023). Suit Alleging NBA ‘Top Shot’ NFTs Were Securities Survives Motion To Dismiss. Skadden Publication: *The Distributed Ledger: Blockchain, Digital Assets and Smart Contracts*. <https://www.skadden.com/insights/publications/2023/02/suit-alleging-nba-top-shot-nfts-were-securities-survives>
- Ecommerce: las ventas online facturaron \$7,8 billones y crecieron 175% en 2023 (19 de marzo de 2024). *Ámbito*. <https://www.ambito.com/negocios/e-commerce-las-ventas-online-facturaron-78-billones-y-crecieron-175-2023-n5967746>
- ESMA clarifies which crypto-assets might qualify as financial instruments in the EU. (Feb., 2024), *Delloitte.com* [Internet].
- European Commission (2017). *Effectiveness of tax incentives for venture capital and business angels to foster the investment of SMEs and start-ups*. https://taxation-customs.ec.europa.eu/system/files/2017-06/final_report_2017_taxud_venture-capital_business-angels.pdf
- European Securities and Markets Authorities (ESMA). (6 de octubre, 2023). *Report on the DLT Pilot Regime. Study on how financial instrument transactions are registered in various Distributed Ledger Technologies*. Paris: ESMA. <https://www.esma.europa.eu/document/report-dlt-pilot-regime-study-how-financial-instrument-transactions-are-registered-various>
- Evolution of HTTP. (s. f.). *mdn web docs*. [Internet]. https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/Evolution_of_HTTP



- Financial Services Committee. (22 de mayo, 2024). Passes Financial Innovation and Technology for the 21st Century Act with Overwhelming Bipartisan Support. <https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409277>
- Focus 2030 (2019). *El G7 y las Políticas de Desarrollo*. https://focus2030.org/IMG/pdf/es.note_d_analyse_g7_focus_2030.pdf
- Fundación Observatorio Pyme (2022). “Convergencia productiva entre Pymes y Grandes empresas.Transformación digital,educación técnica y eficiencia energética en cada nivel territorial”. Conferencia Bienal 2022, 25° Aniversario. https://www.observatoriopyme.org.ar/_files/ugd/bdab5e_1cbd9faa295048b383b70c250e912e3b.pdf
- García-Peñalvo, F. y Vázquez-Ingelmo, A. (diciembre, 2023). *What Do We Mean by GenAI? A Systematic Mapping of The Evolution, Trends, and Techniques Involved in Generative AI*. <https://reunir.unir.net/handle/123456789/15134>
- Garrido, J. M. (2023). *Digital Tokens: A Legal Perspective*. International Monetary Fund. IMF, WP/23/151. <https://www.imf.org/en/Publications/WP/Issues/2023/07/28/Digital-Tokens-A-Legal-Perspective-537041>
- Gesley, J. (Dic. 21, 2023). Germany: Act to Make Germany More Attractive for Investments Enters into Force. Library of Congress. [Web page]. <https://www.loc.gov/item/global-legal-monitor/2023-12-20/germany-act-to-make-germany-more-attractive-for-investments-enters-into-force/>
- Godoy, J. (August 22, 2023). Ex-OpenSea manager sentenced to 3 months in prison for NFT insider trading. Reuters. <https://www.reuters.com/legal/ex-opensea-manager-sentenced-3-months-prison-nft-insider-trading-2023-08-22/>
- González Rossi, A. (Coord.). (29 de diciembre, 2022). Especial *Blockchain* y derecho. *La Ley*. <https://colabogmza.com.ar/wp-content/uploads/2022/12/Diario-29-12-22.pdf>
- Heinrich, J., Bouy, F., Mümken, P., Trossen, T., y Scholz, Y. (April 14, 2023). Non-fungible tokens: what matters is the content. https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2023/fa_bj_2303_NFT_en.html
- Heise, C. (31 de agosto, 2021). Now also in electronic form: securities. *BaFin* [Internet]. https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2021/fa_bj_2107_eWpG_en.html
- Heredia Querro, S. (2020). *Smart Contracts: Qué son, para qué sirven y para qué no servirán*. IJ Editores. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3875645
- Heredia Querro, S. (28 de noviembre, 2023). *MiCA 2.0., la regulación de las Finanzas Descentralizadas y la certificación de Smart Contracts*. <https://abogados.com.ar/mica-20-la-regulacion-de-las-finanzas-descentralizadas-y-la-certificacion-de-smart-contracts/33885>
- Heredia Querro, S., y Bertoni, M. (2022a). *De prospectos y white papers... El deber de información del emisor de tokens criptográficos. La posición europea*. Suplemento Especial *Diario La Ley: Blockchain y Derecho*. https://colabogmza.com.ar/wp-content/uploads/2022/12/1672252050521_Diario-28-12-22.pdf



- Heredia Querro, S., y Bertoni, M. (2022b). Taxonomía de los tokens criptográficos. *Revista Consejo Digital*, 11(67). <https://www.consejo.org.ar/servicios/medios-del-consejo/revista-consejo-digital/edicion-67>
- Heredia Querro, S., Bertoni, M., y Santamaría, M. (2 de agosto, 2022). Proof of Stake, Gobernanza Descentralizada y Ataques Relámpago. Abogados.com.ar. <https://abogados.com.ar/proof-of-stake-gobernanza-descentralizada-y-ataques-relampago/30955?tech=1>
- Heredia Querro, S., y Bertoni, M. (2024). Apuntes sobre el DNU 70/2023: Bases para la Reconstrucción de la Economía Argentina. Thomson Reuters La Ley AR/DOC/111/2024. <https://www.fundaciondhi.com.ar/post/analisis-dnu-70-2023>
- Immunefi. (23 de mayo, 2023). The Ultimate Guide to Reentrancy. <https://medium.com/immunefi/the-ultimate-guide-to-reentrancy-19526f105ac>
- James, L. (New York State Attorney General), (23 de febrero, 2021). Consumer Alert: Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities in New York. <https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal>
- Jha, p. (13 de abril, 2022). Las consecuencias del hackeo de USD 650 millones de Axie Infinity. Cointelegraph en español. <https://es.cointelegraph.com/news/the-aftermath-of-axie-infinity-s-650m-ronin-bridge-hack>
- Joe, K. (30 de octubre, 2023). The Power of Staking and Governance Tokens in Decentralized Protocols. <https://medium.com/@kweeniejoe4/the-power-of-staking-and-governance-tokens-in-decentralized-protocols-c075d68ade53>
- J. P. Morgan Paymentes. (s. f.). *Understanding Programmable Payments, Programmable Money and Purpose-Bound Money*. [On Line]. <https://www.jpmorgan.com/onyx/programmable-payments-purpose-bound-money>
- Koning, J. P. (13 de diciembre, 2022). Japón era el lugar más seguro para ser cliente de FTX. CoinDesk. <https://www.coindesk.com/es/opinion/2022/12/13/japan-was-the-safest-place-to-be-an-ftx-customer>
- Kramer, S. (2020). SEC's Safe Harbor for Tokens Is an Incomplete Solution. [Internet]. Bloomberg Law. <https://www.bloomberglaw.com/external/document/X6UBS2N0000000/capital-markets-professional-perspective-sec-s-safe-harbor-for-t>
- Lacube, G. (7 de diciembre, 2021). "Argentina, tierra de unicornios". *Forbes*, Argentina. <https://www.forbesargentina.com/summit/argentina-tierra-unicornios-n10671>
- La Moncloa. (9 de marzo, 2023). La nueva Ley del Mercado de Valores aumenta su competitividad, facilita la financiación y refuerza la protección de los inversores. <https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2023/090323-nueva-ley-mercado-valores.aspx>
- Latham & Watkins (2024). Ruling for SEC Clears Path for Continued Litigation in SEC v. Coinbase. Global Fintech and Digital Assets Blog. Latham & Watkins' Litigation & Trial Practice. <https://www.fintechanddigitalassets.com/2024/04/ruling-for-sec-clears-path-for-continued-litigation-in-sec-v-coinbase/>



- Lazic, N. (March 20, 2024). Ripple is a Utility Token, Says European Governance Institute — XRP Price In A Major Downtrend. [Internet]. <https://www.ccn.com/analysis/crypto/ripple-utility-european-governance-institute-xrp-major-downtrend/>
- Ledger Insights (28 June, 2024). Government-owned KfW bank unveils €4 billion digital bond. <https://www.ledgerinsights.com/government-owned-kfw-bank-unveils-e4-billion-digital-bond/>
- Lee, A. (June 23, 2021). *What is programmable money?* <https://www.federalreserve.gov/econres/notes/feds-notes/what-is-programmable-money-20210623.html>
- Lesta, J. (24 de abril de 2024). “Economía del Conocimiento: pese al cepo cambiario, empresas esperan que crezcan exportaciones y empleo en 2024”. *Ámbito*. <https://www.ambito.com/economia/del-conocimiento-pese-al-cepo-cambiario-empresas-esperan-que-crezcan-exportaciones-yempleoen2024-n5986617>
- Loevinger, L. (1949). Jurimetrics: the next step forward. *Minnesota Law Review*, 33(5), 1796. <https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=2795&context=mlr>
- Lukin, T., y Marano, M. E. (diciembre, 2023). *Economía y Finanzas: las sociedades por acciones simplificadas en la Argentina. A seis años de su creación, ¿impulso a los emprendedores o vehículo para el abuso fiscal?* <https://library.fes.de/pdf-files/bueros/argentinien/20945.pdf>
- McKinsey y Company (2024). *¿Qué es la tokenización?* <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-tokenization>
- Maker, Equipo de (diciembre de 2017). El sistema Dai Stablecoin. Informe técnico. <https://makerdao.com/whitepaper/Dai-Whitepaper-Dec17-es.pdf>
- Mattos Filho's Corporate/M&A (28 de enero, 2022). Changes to the Brazilian Corporations Law. <https://www.mattosfilho.com.br/en/unico/changes-brazilian-corporations-law/>
- Ministerio de Economía, Comisión Nacional de Valores (CNV). (12 de julio, 2024). CNV reglamenta la oferta privada. *Argentina.gob.ar*. Confr. <https://www.argentina.gob.ar/noticias/cnv-reglamenta-la-oferta-privada>
- OECD. (2020). *The Tokenisation of Assets and Potential Implications for Financial Markets*. OECD Blockchain Policy Series. www.oecd.org/finance/The-Tokenisation-of-Assets-and-PotentialImplications-for-Financial-Markets.htm
- Norwegian Tax Administration, The. (s. f.). Income deduction in connection with investments in start-up companies (private limited liability companies) – tax incentive scheme. <https://www.skatteetaten.no/en/person/taxes/get-the-taxes-right/shares-and-securities/about-shares-and-securities/tax-deductions-in-connection-with-investments-in-start-up-businesses---the-tax-incentive-scheme/>
- OECD. (2024). *Financing SMEs and Entrepreneurs 2024: An OECD Scoreboard*. Policy Highlights. https://www.oecd.org/content/dam/oecd/en/publications/support-materials/2024/03/financing-smes-and-entrepreneurs-2024_015c0c26/Policy-Highlights-2024-Financing-SMEs-Scoreboard.pdf



- Oliveira Farias, D., Teixeira Coutinho, E., Monteiro, M., y Jocundo Loureiro, T. C. (2022). *Revista do TCU*, (150), 22-48. <https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/1921>
- People's Bank of China, The. (2022). "E-CNY: main objectives, guiding principles and inclusion considerations", BIS Papers chapters. In: Bank for International Settlements (ed.), *CBDCs in emerging market economies*, vol. 123 (pp. 45-48). Bank for International Settlements.
- Rajan, R. G., y Zingales, L. (1996). Financial dependence and growth (Working Paper No. 5758). *National Bureau of Economic Research*. <https://www.nber.org/papers/w5758>
- Reinhold, M. (6 de julio, 2023). La Argentina tiene la mayor cantidad de startups de alto impacto en toda América Latina. *La Nación*, Argentina, <https://www.lanacion.com.ar/economia/negocios/la-argentina-tiene-la-mayor-cantidad-de-startups-de-alto-impacto-en-toda-america-latina-nid06072023/>
- Scalex (s. f.). Santiago Venture Exchange. El match perfecto entre inversión y financiamiento. <https://www.scalex.cl>
- Securities and Exchange Commission (SEC). Release No. 81207/July 25, 2017. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO. <https://www.sec.gov/files/litigation/investreport/34-81207.pdf>
- Singh, A. (30 de mayo, 2024). Terraform, Do Kwon Agree in Principle to Settle Fraud Case With SEC: Court Filing. *Coin Desk*. [Internet]. <https://www.coindesk.com/policy/2024/05/30/terraform-do-kwon-agree-in-principle-to-settle-fraud-case-with-sec-court-filing>
- Souza Burite, A., Silva Sacramento, A. R., & Maury Raupp, F. (2023). Possíveis implicações da aplicação combinada da *blockchain*, *smart contract* e inteligência artificial nas contratações e no orçamento público. *Revista CGU*, 15, (27), 203-221. <https://doi.org/10.36428/revistadacgu.v15i27.534>
- The European Digital Identity Regulation (April 30, 2024). Cyber Risk GmbH. <https://www.european-digital-identity-regulation.com/>
- Tribunal de Contas da União TCU – Relatório de Levantamento. (s. f.). Levantamento de auditoria. identificação de oportunidades e riscos na adoção da tecnologia blockchain/ DLT. Descrição de fatores críticos de sucesso e arvore de decisão de apoio a gestores. Possíveis impactos para o controle. Recomendações. Arquivamento. Relator: Aroldo Cedraz. <https://www.jusbrasil.com.br/jurisprudencia/tcu/1718870386>
- United States District Court. Northern District of California. San Francisco Division. SEC vs. Payward, Inc., Payward Ventures, Inc. Complaint. 11/20/23. <https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-237.pdf>
- United States District Court for the District of Columbia. SEC vs. Binance Holdings. Civil Action No. 23-1599 (ABJ). Case 1:23-cv-01599-ABJ-ZMF. Document 248 Filed junio 28 de 2024. https://storage.courtlistener.com/recap/gov.uscourts.dcd.256060/gov.uscourts.dcd.256060.248.0_1.pdf



- University of Cambridge, & World Economic Forum. (January, 2024). *The Future of Global Fintech: Towards Resilient and Inclusive Growth*. Insight Report. https://www3.weforum.org/docs/WEF_The_Future_of_Global_Fintech_2024.pdf
- Voshmgir, S. (junio, 2020). *La Economía del Token: Cómo la Web3 reinventa la Internet*. 2.ª ed. Berlin: Token Kitchen. <https://github.com/Token-Economy-Book/SpanishTranslation>
- Washington College of Law Clinical Program (s. f.). ESOPS. <https://www.american.edu/wcl/academics/experientialedu/clinical/theclinics/elc/tlcc/for-businesses-nonprofits/upload/esops-info-sheet.pdf>
- Wenzel, F. (28 de junio, 2024). Policía detiene a involucrados en proyectos de créditos de carbono problemáticos en la Amazonía brasileña. Centro Latinoamericano de Investigación Periodística (Clip). <https://www.elclip.org/policia-detiene-involucrados-proyectos-creditos-carbono-problematicos-amazonia-brasilena/>
- Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. MIT Press.
- Wright, T. (9 de oct., 2023). Regulador de valores de Brasil planea establecer un sandbox para la tokenización en 2024. *Cointelegraph*. <https://es.cointelegraph.com/news/brazilian-securities-regulator-sandbox-tokenization>.



Capítulo 4

Protección de los datos personales en la era cibernética: un enfoque constitucional y procesal⁴²

Juan Esteban Aguirre Espinosa

Dany Steven Gómez Agudelo

Sebastián Díaz Bolívar

Introducción

En la era cibernética, la protección de los datos personales se ha convertido en un tema crucial en el ámbito del derecho constitucional y procesal. Este artículo examina los desafíos y avances en la regulación de la protección de datos personales y subraya las implicaciones legales y tecnológicas que emergen en el entorno digital.

Se exploran las medidas adoptadas por diversas jurisdicciones para salvaguardar la privacidad de los individuos, así como las innovaciones tecnológicas que facilitan o complican esta tarea, desde una perspectiva constitucional y procesal. A partir de este enfoque, la pregunta que se desarrolla en este texto es: ¿cómo puede el marco regulatorio colombiano en materia de protección de datos personales, adaptarse de manera efectiva a los rápidos avances tecnológicos y garantizar la protección de los derechos fundamentales desde una perspectiva constitucional y procesal?

La importancia de esta investigación radica en que ofrece una visión comparativa de las normativas de protección de datos personales, identificando buenas prácticas y áreas de mejora. Los objetivos específicos son:

- Identificar las principales amenazas y desafíos tecnológicos en la protección de datos personales.
- Evaluar la efectividad de las legislaciones actuales en proteger la privacidad de los individuos.
- Proponer recomendaciones para fortalecer las políticas de protección de datos.

⁴² Este capítulo se deriva de la investigación denominada "Implicaciones de las publicaciones falsas en redes sociales: legitimidad de la comunicación política y la justicia en el escenario digital", la cual fue financiada por la Universidad Católica Luis Amigó - Sede Medellín, Colombia, en el año 2024. Research Organization Registry: <https://ror.org/055d5bf90>



El enfoque de la investigación es cualitativo y descriptivo, basado en un análisis documental de la legislación colombiana, la jurisprudencia e informes de expertos y literatura académica sobre la protección de datos personales en distintos contextos cibernéticos. La investigación también se ocupa de analizar cómo diferentes jurisdicciones abordan la protección de datos personales y qué innovaciones tecnológicas se están aplicando para este fin.

Las legislaciones objeto de estudio comprenden una amplia gama de países con legislaciones avanzadas en protección de datos, como la Unión Europea con el Reglamento General de Protección de Datos (GDPR), los Estados Unidos con la Ley de Privacidad del Consumidor de California (CCPA) y regiones donde estas normativas están en desarrollo y evolución constante, como América Latina y Asia. En el caso específico de Colombia, se ha observado un significativo avance en la implementación de leyes y regulaciones que buscan salvaguardar y proteger la privacidad de los ciudadanos en el ámbito digital, “sin perjuicio de que determinada normativa nacional y de la Unión Europea pueda servir de guía al poder judicial y legislativo en un futuro” (Gutiérrez García, 2023, p. 9).

Además, para llevar a cabo este estudio, se realizó un análisis exhaustivo de la legislación colombiana en materia de protección de datos, comparándola con las normativas de otros países. Asimismo, se entrevistaron expertos legales y tecnológicos en Colombia para obtener una perspectiva más profunda sobre los desafíos y oportunidades en la aplicación práctica de estas normativas. Los datos recopilados se analizaron utilizando técnicas de codificación cualitativa para identificar temas y patrones emergentes.

El marco teórico de la Protección de Datos Personales

La protección de datos personales se ha convertido en un tema controvertido por el aumento exponencial en la cantidad de información que se comparte y el creciente poder de las herramientas tecnológicas para analizar, transferir y comercializar estos datos sensibles, por lo que se debe “prestar atención a factores clave como la seguridad, la experiencia, la confianza” (Vela Reyna et al., 2024, p. 12). Es esencial que el marco jurídico constitucional y procesal se adapte a la realidad tecnológica para garantizar los derechos fundamentales de los ciudadanos, especialmente en cuanto a su privacidad y protección de datos personales, derecho que busca garantizar el “goce de protección y resguardo suficiente para poder decidir qué información comparte cada sujeto sobre su vida privada” (Machuca et al., 2022, p. 7). En este contexto, las regulaciones sólidas y exhaustivas son cruciales para abordar las implicaciones legales y éticas derivadas del uso creciente de la tecnología.



Reviste especial importancia que el marco jurídico constitucional y procesal evolucione en sintonía con los avances tecnológicos, para garantizar la protección de los derechos fundamentales de los ciudadanos, en especial su privacidad. Las regulaciones deben ser robustas y adaptativas para abordar eficazmente las complejas implicaciones legales y éticas del uso extensivo de la tecnología. Cobra especial relevancia contar con regulaciones sólidas y exhaustivas que aborden de manera eficiente y proactiva las numerosas implicaciones legales y éticas que surgen ante el uso creciente y omnipresente de la tecnología en la sociedad actual, teniendo en cuenta que “invertir en el desarrollo de estrategias específicas en materia de privacidad mejora la imagen corporativa e inspira confianza en los clientes” (Albornoz, 2021, p. 229). Asimismo, se ha puesto de manifiesto de manera contundente que la rápida y constante evolución de la tecnología ha provocado que los datos personales sean considerados en la actualidad uno de los activos más valiosos y preciados (Hernández, 2018).

Ante este panorama, resulta indispensable abordar de manera decidida y sistemática los desafíos significativos que plantea la protección de la privacidad de los individuos, así como la necesidad impostergable de establecer mecanismos sólidos y efectivos de control y regulación. No se puede obviar la necesidad de desarrollar estrategias integrales y eficaces que permitan equilibrar el avance tecnológico y el resguardo de los derechos fundamentales de los ciudadanos. Esto incluye medidas rigurosas y actualizadas que aborden, entre otros aspectos relevantes, el consentimiento informado y el acceso transparente a los datos personales, la seguridad cibernética, el tratamiento y almacenamiento responsable de la información y las sanciones en caso de incumplimiento de las normativas de protección de datos, que además prioricen “la protección de la dignidad, las libertades y los derechos de las personas, en especial el derecho a la protección de datos personales” (Bernal y Gómez, 2022, p. 392).

Se hace indispensable impulsar la generación de políticas públicas sólidas y flexibles, acompañadas de regulaciones claras y actualizadas, que atiendan y anticipen los constantes avances tecnológicos y resguarden los derechos individuales. También no puede pasarse por alto en la medida de las posibilidades “usar datos anonimizados, encriptados, o recolectar información que al ser cruzada no permita la identificación de las personas” (Gómez et al., 2020, p. 19). Para lograrlo, se requiere fomentar la colaboración entre los diversos actores involucrados, incluyendo gobiernos, instituciones académicas, empresas y organizaciones de la sociedad civil, a fin de desarrollar soluciones integrales y colectivas que respondan de manera responsable y efectiva a los desafíos y oportunidades planteados por la era digital. Se debe reconocer la necesidad de adaptar el marco jurídico constitucional y procesal a esta nueva realidad tecnológica, con el objetivo primordial de garantizar la protección y salvaguarda de los derechos fundamentales de los ciudadanos, en cuanto a su pri-



vacidad y protección de datos personales. Esto requiere implementar regulaciones sólidas y efectivas, así como promocionar políticas públicas y estrategias integrales que permitan conciliar el avance tecnológico con la defensa de los derechos individuales en la sociedad actual y futura.

En este sentido, en el marco teórico de este estudio se analizan a fondo las implicaciones jurídicas y las posibles soluciones en relación con la privacidad y la protección de datos personales, lo cual implica considerar aspectos como la limitación de la recopilación y el uso de datos, la necesidad de consentimiento informado y la adopción de medidas técnicas y organizativas que garanticen la seguridad de la información. En este orden de ideas, se debe analizar de forma detallada cómo el marco jurídico constitucional y procesal puede adaptarse a esta nueva realidad tecnológica, para garantizar los derechos fundamentales de los ciudadanos en cuanto a su privacidad y protección de datos personales, que terminan vulnerados por “la cantidad de medios por los cuales se recolectan los datos y las medidas de seguridad que se utilizan para evitar su alteración o divulgación no deseada” (Cabezas, 2023, p. 22).

En este contexto, resulta pertinente resaltar la importancia de contar con regulaciones sólidas que aborden de manera efectiva las implicaciones legales y éticas que surgen ante el uso de la tecnología en la sociedad actual. El marco teórico de este estudio tiene como base abordar los desafíos que plantea la tecnología en relación con la privacidad y la protección de datos personales. Es indispensable contar con marcos regulatorios adecuados y efectivos que garanticen los derechos fundamentales de los ciudadanos en este ámbito. Para ello, se deben analizar las implicaciones jurídicas y éticas que surgen de la utilización de la tecnología, así como identificar las posibles soluciones que permitan proteger la privacidad y la seguridad de los datos personales en la sociedad actual (Becerra y Waisbord, 2021).

Desde un punto de vista constitucional, la salvaguarda de la información personal está directamente vinculada a los derechos fundamentales establecidos en la Constitución Política de Colombia, en particular el derecho a la privacidad, el *habeas data* y el debido proceso. La teoría de la soberanía de los datos postula que las personas deben tener el control de su información personal y que los Estados deben establecer leyes que protejan este control. Esta teoría se opone a la idea de que las empresas tecnológicas tienen derechos ilimitados sobre la información que recopilan, y plantea la necesidad de equilibrar los derechos de las personas y los intereses comerciales (Cerrillo y Casadesús, 2021).

La teoría de los derechos digitales pone énfasis en la redefinición de los derechos tradicionales, como la privacidad, y su adaptación a las nuevas realidades tecnológicas en la era digital. Se destaca la importancia de diseñar la arquitectura de internet y las tecnologías digitales, teniendo en cuenta la protección de estos dere-



chos. Esto cobra relevancia en el contexto colombiano, donde la rápida adopción de tecnologías digitales contrasta con la evolución de las leyes de protección de datos.

La teoría de la privacidad contextual sugiere que la protección de los datos personales debe adaptarse al contexto en el que se recopila y utiliza la información, atendiendo a las normas culturales y regionales específicas. En un país como Colombia, con su diversidad cultural, esto implica la necesidad de enfoques personalizados para la protección de datos. Por ejemplo, la variedad de idiomas y costumbres en diferentes regiones del país dificulta la aplicación de normativas uniformes en materia de protección de datos (Hummel et al., 2021).

En el entorno actual, se hace cada vez más evidente la importancia de comprender y abordar adecuadamente las cuestiones de privacidad en el manejo de datos personales.

La teoría de la privacidad contextual surge como una respuesta a esta necesidad, y proporciona un marco sólido para el tratamiento de la información personal en diferentes escenarios. De acuerdo con Nissenbaum (2010) la privacidad contextual implica “evaluar en función del contexto en que se recopilan los datos y las expectativas de los individuos en relación con su información” (p. 89), por lo que es apropiado reconocer que “este enfoque ha sido clave para el desarrollo de regulaciones modernas que establecen principios de minimización de datos y propósitos específicos para su recolección” (Barreno, 2025, p. 3).

En el caso de Colombia, un país con una amplia diversidad cultural y regional, la privacidad contextual enfrenta desafíos únicos. La protección de datos en un entorno tan heterogéneo requiere enfoques personalizados que tengan en cuenta las particularidades culturales, las formas de comunicación y el uso específico de la información en cada región. Es importante destacar que la privacidad contextual no descarta la protección de la privacidad como un derecho fundamental, sino que la amplía y la adapta a las necesidades y realidades de cada contexto específico, lo cual supone que, si bien existen principios generales de protección de datos que deben seguirse, también se deben considerar las particularidades y peculiaridades de cada situación.

Así las cosas, la teoría de la privacidad contextual invita a adoptar un enfoque más integral y flexible en la protección de datos personales. Reconocer que la privacidad no es un derecho absoluto, sino una expectativa contextual, nos permite abordar los desafíos de la diversidad cultural y regional de manera más efectiva, y así garantizar un equilibrio adecuado entre la protección de datos y el uso legítimo de la información (Nissenbaum, 2010).

Otros expertos han resaltado la importancia de la educación y concienciación en el ámbito de la protección de datos, de esta manera “las campañas de sensibilización



y programas educativos sobre la privacidad, son necesarias para fomentar una cultura de protección de datos” (Oña, 2025, p. 4-5).

Sin embargo, es decisivo comprender que la protección de datos no se limita a cumplir con una obligación legal, sino que involucra una responsabilidad ética y moral hacia las personas cuya información está en nuestras manos. Por lo tanto, adquirir conciencia sobre este tema es sumamente relevante, ya que el desconocimiento puede tener consecuencias negativas tanto para los individuos como para las organizaciones.

Por lo tanto, es clave fomentar una cultura de protección de datos en la sociedad, donde se promueva la educación y el diálogo sobre este tema. Además, resulta fundamental reforzar los mecanismos de formación y capacitación, tanto para los ciudadanos como para los profesionales que trabajan con datos personales, con el fin de garantizar una protección efectiva y responsable de la privacidad. La sensibilización debe empezar desde una edad temprana, incluyendo la educación escolar, para que los futuros ciudadanos sean conscientes de la importancia y los riesgos al momento de compartir su información.

En este sentido, la educación y concienciación en protección de datos constituyen un pilar clave para lograr un equilibrio entre la innovación tecnológica y el respeto hacia la privacidad individual. Solo a través de la información y el conocimiento es posible garantizar una sociedad digital segura y comprometida con la protección de los derechos fundamentales.

Marco regulatorio en la legislación colombiana

La Ley Estatutaria 1581 de 2012 establece claramente los principios y procedimientos necesarios para garantizar el pleno ejercicio y respeto al derecho fundamental a la protección de datos personales en el país. La protección de datos personales es un tema de suma relevancia en el contexto actual de la era cibernética, donde la adquisición, procesamiento y divulgación inapropiados de información sensible, como “la identidad y salud de [un] paciente” (Barajas y Ramos, 2024, p. 110), pueden tener graves implicaciones para la seguridad e integridad de las personas.

En el marco jurídico colombiano, se debe tener en cuenta que el artículo 15 de la Constitución Política consagra el derecho a la intimidad y la protección de los datos personales como garantías fundamentales para todos los ciudadanos. Asimismo, la Ley Estatutaria 1581 de 2012 regula de forma detallada el tratamiento y manejo de la información personal y establece derechos y deberes, tanto para las entidades públicas como para las empresas privadas, las cuales “tienen una serie de



obligaciones que rebasan el simple cuidado de la información y datos personales de sus empleados, clientes y proveedores” (Meraz, 2018, p. 16).

Además, la Ley 1273 de 2009 otorga carácter penal a los delitos informáticos, lo que demuestra la intención del país de sancionar cualquier actividad ilegal relacionada con el uso indebido de datos y sistemas electrónicos, sin embargo “han sido casos muy difíciles de identificar, así como llegar a judicializar a los responsables” (Niño, 2022, p. 85). De esta manera, se puede afirmar con certeza que Colombia tiene la intención de establecer un marco normativo completo, sólido y actualizado en materia de protección de datos en la era cibernética, con el fin de garantizar el pleno cumplimiento de los derechos de los ciudadanos en relación con la privacidad y el control sobre sus datos personales.

El Reglamento General de Protección de Datos (GDPR) de la Unión Europea es, por su parte, una legislación clave, implementada en mayo de 2018, que ha tenido un impacto significativo, tanto para los individuos como para las organizaciones que operan dentro del territorio de la UE. Sus normas y principios buscan empoderar a los ciudadanos, otorgándoles un mayor control sobre sus datos personales, y generar un marco regulatorio más claro y armonizado para las empresas.

La legislación colombiana, así como el marco regulatorio internacional representado por el GDPR, hacen parte de un esfuerzo conjunto de los gobiernos y organizaciones para salvaguardar los derechos y la privacidad de los individuos en el entorno digital. Estos avances legales brindan una base sólida para abordar de manera efectiva y responsable los desafíos y amenazas que surgen en la era cibernética y promueven un ecosistema digital seguro y confiable para todos.

La Ley 1581 de 2012, conocida como Ley de Protección de Datos Personales, ha sido central para establecer en Colombia un marco normativo que proteja los datos personales. Esta ley define los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, que rigen el tratamiento de datos personales. La Superintendencia de Industria y Comercio (SIC) es la entidad encargada de velar por el cumplimiento de la ley 1581 y ha emitido diversas resoluciones para complementar su aplicación (SIC, 2023).

Un análisis detallado de la aplicación de la Ley 1581 de 2012 revela varios desafíos. Muchas empresas y organizaciones en Colombia todavía están en proceso de adaptar sus prácticas a las exigencias de la ley, también es posible que “se reconozcan nuevas facultades en cabeza de los titulares respecto de sus datos personales” (Osuna, 2024, p. 50). Además, el uso de nuevas tecnologías, como el big data y la inteligencia artificial, que “recopilan, almacenan y procesan datos para extraer conocimientos de valor” (Jara Fuentealba, 2021, p. 39), amplía los riesgos de los titulares, de manera que fortalecer la educación conlleva a que los titulares puedan ejercer de



manera efectiva sus derechos, más aún con el desarrollo de algoritmos y sistemas automatizados, que en muchos casos, constituyen un desafío para la transparencia y el control sobre la información personal.

Garantías y mecanismos de protección de derechos desde la óptica del derecho procesal

De acuerdo con el derecho procesal, la protección de los datos personales se debe garantizar a través de diversos mecanismos y procedimientos legales que aseguren la efectividad del derecho al *habeas data* y a otros derechos conexos. Como ya se dijo, la Constitución Política de Colombia establece el *habeas data* como un mecanismo procesal para garantizar tales derechos. La importancia de proteger los datos personales radica en la preservación de la dignidad e intimidad de las personas, así como en evitar posibles vulneraciones a sus derechos fundamentales, y esta protección se logra si se cuenta con regulaciones claras y eficaces que garanticen el respeto y la confidencialidad de la información personal.

En el ámbito legal, el *habeas data* es un instrumento que vela por la privacidad de las personas y asegura que sus datos personales no sean utilizados de manera indebida. En términos procesales, el *habeas data* se configura como una acción constitucional que permite a los individuos solicitar la corrección, actualización o eliminación de sus datos personales cuando estos sean inexactos, incompletos o vulneren sus derechos fundamentales. Como mecanismo procesal, es una herramienta para garantizar la privacidad y el control sobre la información personal.

El *habeas data* les permite a las personas, no solo acceder a la información que sobre ellas se haya recogido en archivos y bases de datos de entidades públicas y privadas, sino también conocerla, actualizarla y rectificarla. En el contexto de la era digital, resulta esencial contar con este mecanismo, ya que gracias al *habeas data* se pueden corregir errores o eliminar datos inexactos que puedan vulnerar la privacidad de las personas, así como actualizar la información que se posee sobre cada individuo. A través de él se puede solicitar a las entidades responsables eliminar, bloquear o corregir información inexacta, incompleta o desactualizada. En este sentido, se trata de un recurso efectivo para salvaguardar la privacidad y controlar el uso que se hace de los datos personales.

Pero el *habeas data* no tiene la función solo de proteger los datos personales, también abarca otros derechos conexos, como el derecho al olvido y el derecho a la autodeterminación informática. El derecho al olvido se refiere a la posibilidad de solicitar que cierta información publicada en Internet que resultare perjudicial o inexacta sea eliminada. Por su parte, el derecho a la autodeterminación informática



implica que cada persona pueda tener el control sobre la información que comparte y decide divulgar. Gracias al *habeas data*, las personas pueden ejercer un mayor control sobre sus datos personales y asegurarse de que su tratamiento se realice de manera adecuada y respetando sus derechos.

En una sociedad cada vez más tecnológica y conectada, la protección de los datos personales se torna imperativa. Es inevitable que los sistemas legales y las regulaciones se adapten a los avances tecnológicos y permitan una protección efectiva de los derechos, con el fin de asegurar un equilibrio entre el desarrollo tecnológico y el respeto a la intimidad y los datos personales de cada individuo.

Por medio de esta acción constitucional, cualquier persona puede exigir el respeto a sus derechos fundamentales. El *habeas data* constituye una herramienta de defensa jurídica directa para los individuos, un procedimiento legal que salvaguarda los derechos de las personas en relación con el tratamiento de sus datos personales. Su importancia radica en su papel clave para garantizar la protección de la privacidad en un entorno cada vez más digitalizado y expuesto, en una época en la que la información personal es tan valiosa y vulnerable.

Por otra parte, la tutela, conocida en el derecho comparado como acción de amparo, es otro mecanismo procesal importante en el ordenamiento jurídico colombiano que puede ser utilizado para proteger los derechos relacionados con la privacidad, confidencialidad y seguridad de los datos personales. Mediante la acción de tutela cualquier persona, sin importar su condición o estatus, puede solicitar la protección inmediata y efectiva de sus derechos fundamentales cuando estos sean vulnerados o amenazados, su “naturaleza ius-fundamental constituye una característica transversal en la esfera latinoamericana” (Sanz, 2025, p. 4).

Además, en relación con la protección de datos personales en la era cibernética y digital, la acción de tutela se ha convertido en un importante mecanismo para garantizar la privacidad, integridad y control sobre la información personal de los individuos. La creciente digitalización, el avance tecnológico y el hecho de que “el monopolio de la digitalización cae en las manos de unas pocas compañías” (Fraiola, 2023, p. 14), han dado lugar a nuevos riesgos y amenazas para la privacidad y protección de los datos, por lo que es forzoso contar con herramientas legales sólidas que permitan a las personas hacer valer sus derechos en este contexto.

La acción de tutela, al ser un recurso accesible y ágil, se ha erigido como una vía efectiva para enfrentar estas problemáticas y asegurar que tanto el Estado como los actores privados cumplan con las obligaciones legales y éticas de respetar y proteger la información personal. Su carácter ágil y expedito le confiere la facultad de ser un mecanismo eficaz para la prevención, control y sanción de acciones que puedan afectar la intimidad y la dignidad de las personas. Además, su aplicación abarca



tanto el ámbito público como el privado, lo que garantiza la protección integral de los derechos individuales frente a las actuaciones arbitrarias o negligentes de cualquier entidad o persona, ya sea esta de naturaleza estatal o no. En el contexto del derecho colombiano, la acción de tutela es una herramienta valiosa para frenar y corregir cualquier vulneración de los derechos fundamentales relacionados con la privacidad y la protección de datos personales.

Reviste especial importancia que las personas conozcan y ejerzan este recurso legal para salvaguardar sus derechos y contribuir a la consolidación de una sociedad justa, equitativa y respetuosa de los principios constitucionales. Al hacerlo, nos acercamos a una cultura de protección de datos en la que el respeto por la privacidad y la seguridad sea una prioridad para todos.

También se debe resaltar la labor de la Superintendencia de Industria y Comercio (SIC), entidad estatal cuyas funciones de inspección, vigilancia y control, tienen un papel crucial en la protección de los datos personales desde una perspectiva procesal. La SIC regula y supervisa rigurosamente el cumplimiento de la Ley 1581 de 2012, que establece las disposiciones generales para la protección de datos personales en Colombia, y actúa como una instancia administrativa que puede imponer sanciones y medidas correctivas en casos de incumplimiento de las normativas de protección de datos en el país, para garantizar la aplicación efectiva de estas regulaciones y promover una cultura de respeto y seguridad en el manejo de la información personal.

La SIC no escatima esfuerzos en su labor de supervisar y controlar el cumplimiento de las obligaciones establecidas por la Ley 1581 de 2012. Sus funciones van más allá de la mera vigilancia, ya que tiene la facultad de investigar y recopilar pruebas en casos de presunta violación de la privacidad de los colombianos. De esta manera, no solo se limita a detectar y sancionar las infracciones, sino que también contribuye a fortalecer un ambiente propicio para la adecuada salvaguardia de los datos personales.

La importancia de la SIC en la protección de datos radica en su capacidad para aplicar sanciones y medidas correctivas ejemplares. Las sanciones pueden variar desde multas económicas significativas hasta la imposición de medidas que obligan a las organizaciones a implementar nuevas políticas y prácticas para garantizar la privacidad y seguridad de los datos personales de los ciudadanos. Además, la SIC puede emitir órdenes de cese y rectificación en casos de violación comprobada, para contribuir a corregir y prevenir futuras vulneraciones de la privacidad.

Gracias a la labor de la SIC, los ciudadanos colombianos pueden tener la tranquilidad de que sus datos personales estarán protegidos y se les brindará un mecanismo efectivo para reclamar sus derechos en caso de violación. No obstante, se



debe subrayar que la responsabilidad de la protección de datos no recae únicamente en la SIC, también implica un compromiso por parte de las organizaciones y ciudadanos en general, para adoptar buenas prácticas en el tratamiento y resguardo de la información personal.

A través de sus funciones de regulación, supervisión y sanción, la SIC garantiza el cumplimiento de las normativas de protección de datos y promueve una cultura de respeto y seguridad en el manejo de la información personal. Su labor contribuye en gran medida a proteger el derecho a la privacidad de los ciudadanos colombianos y a prevenir posibles vulneraciones de sus datos personales.

Conclusiones

En la era digital, para proteger los datos personales se requiere la aplicación práctica de un marco regulatorio sólido y flexible que pueda adaptarse a las constantes innovaciones tecnológicas. Conceptos como la soberanía de los datos y los derechos digitales son fundamentales para garantizar que las personas conserven el control sobre su información personal. En este sentido, la privacidad contextual surge como un enfoque altamente adaptable, capaz de ajustarse a las características culturales y regionales, lo que permite una protección mucho más efectiva de los datos personales.

Se debe asegurar que los individuos tengan el poder de decidir cuándo y cómo se comparte su información y contar con mecanismos adecuados para ejercer sus derechos en el entorno digital. Además, se debe educar y concienciar a todos los usuarios de internet sobre la importancia de la privacidad y la seguridad de los datos personales. Esta conciencia puede fortalecer la confianza en el uso de servicios digitales y generar un ambiente de respeto y protección hacia la información de las personas.

En definitiva, proteger los datos personales en la era digital es un desafío constante que requiere un enfoque adaptativo y proactivo, así como la colaboración entre los diferentes actores involucrados, lo que incluye a gobiernos, empresas y sociedad civil. Solo a través de un esfuerzo conjunto y una preocupación colectiva es posible garantizar el respeto por la privacidad de las personas y que los beneficios de la era digital puedan disfrutarse plenamente, sin comprometer la seguridad y el control sobre los datos personales.

La creciente digitalización de la sociedad y el avance de las tecnologías de la información y la comunicación plantean nuevos retos en materia de protección de datos. Es preciso adaptar constantemente las normativas y políticas existentes para hacer frente a estas realidades cambiantes y garantizar la seguridad de los datos en un entorno cada vez más complejo. Solo a través de un enfoque integral



y colaborativo se podrán abordar eficazmente los desafíos actuales y futuros en la protección de datos.

La adopción de normativas flexibles y adaptables se presenta como una necesidad fundamental para responder de manera efectiva a los rápidos desarrollos tecnológicos que surgen en relación con la protección de datos. En la actualidad, nos encontramos en un entorno en constante evolución impulsado por avances tecnológicos cada vez más innovadores. Mantenerse al día y adaptarse a estos cambios se ha vuelto esencial para garantizar la seguridad y privacidad de los datos en un mundo cada vez más digitalizado.

Es evidente que la cooperación internacional desempeña un papel crucial en este escenario. Los desafíos relacionados con la protección de datos no se limitan a fronteras nacionales, ya que la naturaleza global de Internet y las tecnologías digitales no conocen límites geográficos. Por lo tanto, la colaboración y un enfoque coordinado entre países y organismos internacionales se vuelven indispensables para abordar de manera efectiva estos desafíos, más si se tiene en cuenta que “los países periféricos no actúan en bloque regional y no tienen mecanismos efectivos de obligatoriedad” (Mendoza Enríquez, 2021, p. 26).

La creación de estándares comunes y de marcos legales flexibles y adaptables va a permitir armonizar las políticas de protección de datos en diferentes jurisdicciones. De este modo, se puede facilitar la interoperabilidad y la transferencia de datos de manera segura, para fomentar el intercambio de información y conocimiento en un entorno global.

La cooperación internacional también es necesaria para hacer frente a las amenazas cibernéticas transnacionales y la delincuencia en línea. La protección de datos implica salvaguardar la seguridad de la información personal, así como prevenir y combatir ataques cibernéticos que pueden tener un impacto significativo en la economía y la seguridad de los países. El trabajo conjunto en la detección temprana, el intercambio de buenas prácticas y el fortalecimiento de la capacidad de respuesta será fundamental para proteger la privacidad y la seguridad de los ciudadanos en un mundo cada vez más conectado.

En el contexto colombiano, la Ley 1581 de 2012 ha sido un avance significativo, pero su implementación efectiva requiere mayores esfuerzos en términos de educación y sensibilización. Desde una perspectiva procesal, los mecanismos como el *habeas data* y la acción de tutela son esenciales para proteger de manera efectiva los derechos fundamentales relacionados con la privacidad y la protección de datos personales.

Además, la Superintendencia de Industria y Comercio (SIC) tiene un papel relevante en la regulación de estas normativas y en la supervisión de su cumplimiento,



para asegurar que se respeten y protejan los derechos de los ciudadanos. En un mundo cada vez más digitalizado y conectado, es de vital importancia que los ciudadanos colombianos estén plenamente informados sobre sus derechos y responsabilidades en materia de privacidad y protección de datos personales.

Referencias

- Albornoz, M. (2021). El titular de datos personales, parte débil en tiempos de auge de la Inteligencia Artificial. ¿Cómo fortalecer su posición? *Revista IUS*, 15(48), 209-242. <https://doi.org/10.35487/rius.v15i48.2021.715>
- Barajas-Ochoa, A., y Ramos-Remus, C. (2024). Publicar datos personales sensibles en las redes sociales: oportunidades de mejora. *Gaceta Médica de México*, 160(1), 110-112. <https://doi.org/10.24875/gmm.23000342>
- Barreno, M. (2025). El derecho a la privacidad en la era digital: desafíos y garantías frente a la vigilancia masiva desde una perspectiva de derechos humanos. *Revista Internacional de Cultura Visual*. 17 (1), 1-11. <https://doi.org/10.62161/revvisual.v17i5769>
- Becerra, M., y Waisbord, S. R. (2021). The curious absence of cybernationalism in Latin America: Lessons for the study of digital sovereignty and governance. *Communication and the Public*, 6(1-4), 67-79. <https://doi.org/10.1177/20570473211046730>
- Bernal Camargo, D., y Gómez Córdoba, A. I. (2022). El derecho a la protección de datos personales en la investigación biomédica en Colombia: Una mirada desde el soft law y el hard law. *Revista Chilena de Derecho y Tecnología*, 11(1), 361-395. <https://dx.doi.org/10.5354/0719-2584.2022.66319>
- Cabezas Azuero, J. S. (2023). Tratamiento de datos personales y compliance en Colombia. *Revista de la Facultad de Derecho y Ciencias Políticas*, 53(138), pp. 1-25. <https://doi.org/10.18566/rfdcp.v53n138.a2>
- Cerrillo-Martínez, A., y Casadesús-de-Mingo, A. (2021). Data governance for public transparency. *Profesional de la información*, 30(4), e300402. <https://doi.org/10.3145/epi.2021.jul.02>
- Fraioli, G. (2023). Regímenes de propiedad posibles para los datos digitales. *Desde el Sur*, 15(3), e0046. <https://dx.doi.org/10.21142/des-1503-2023-0046>
- Gómez-Córdoba, A., Arévalo-Leal, S., Bernal-Camargo, D., y Rosero de los Ríos, D. (2020). El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia. *Revista de Bioética y Derecho*, (50), 271-294. http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872020000300017&lng=es&tlng=es
- Gutiérrez García, E. (2023). El derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad. *Estudios Constitucionales*, 21(1), 308-317. <https://dx.doi.org/10.4067/S0718-52002023000100308>
- Hernández López, J. M. (2018). *Reglamento General de Protección de datos*. Tirant lo Blanch.



- Hummel, P., Braun, M., Tretter, M., y Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, 8(1). <https://doi.org/10.1177/2053951720982012>
- Jara Fuentealba, N. (2021). El derecho de propiedad sobre los datos. *Revista chilena de derecho privado*, 101-142. <https://dx.doi.org/10.4067/S0718-80722021000300101>
- Machuca Vivar, S. A., Vinuesa Ochoa, N. V., Sampedro Guamán, C. R., y Santillán Molina, A. L. (2022). Habeas data y protección de datos personales en la gestión de las bases de datos. *Revista Universidad y Sociedad*, 14(2), 244-251.
- Mendoza Enríquez, O. A. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS*, 15(48), 179-207. <https://doi.org/10.35487/rius.v15i48.2021.743>
- Meraz Espinoza, A. I. (2018). Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales. *Revista IUS*, 12(41), 293-310. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100293&lng=es&tlng=es.
- Niño García, D. (2022). Los datos personales y sus riesgos jurídicos a partir de la transformación digital en el comercio electrónico. *Revista CES Derecho*, 13(1), 70-89. <https://doi.org/10.21615/cesder.6386>
- Nissenbaum, H. (2010). *Privacidad en contexto: Tecnología, políticas y la integridad de la vida social*. Stanford University Press.
- Oña, O., Parrales Reyes, L., Vera Celi, M., y Zhigue López, F. (2025). La protección de datos personales en la era digital - Retos y oportunidades. *Revistalexenlace*, 2(1), 38-45. <https://revistalexenlace.com/index.php/ojs/article/view/5>
- Osuna, A. (2024). El derecho fundamental a la protección de datos personales en Colombia. (Trabajo de maestría). Universidad Externado de Colombia. <https://bdigital.uexternado.edu.co/server/api/core/bitstreams/b81636f6-857a-4c14-a01b-b324acec4d80/content>
- Sanz Salguero, F.J. (2025). Derecho fundamental a la protección de los datos personales en América Latina: desafíos ante el alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea. *Revista derecho del Estado*. 62, 143-169. <https://doi.org/10.18601/01229893.n62.06>.
- Superintendencia de Industria y Comercio (SIC). (2023a). *Resolución Número 20115 de 2023 (20 de abril de 2023): Por la cual se impone una sanción y se imparten órdenes administrativas*. Ministerio de Comercio, Industria y Turismo. <https://www.sic.gov.co/sites/default/files/files/2023/RE20115-2023.pdf>
- Superintendencia de Industria y Comercio (SIC). (2023b). *Resolución Número 35435 de 2023 (27 de junio de 2023): Por la cual se impone una sanción y se imparten órdenes administrativas*. Ministerio de Comercio, Industria y Turismo. <https://www.sic.gov.co/sites/default/files/files/2023/RE35435-2023.pdf>
- Superintendencia de Industria y Comercio (SIC). (2023c). *Resolución Número 61609 de 2023 (09 de octubre de 2023): Por la cual se impone una sanción y se imparten órdenes administrativas*. Ministerio de Comercio, Industria y Turismo. <https://www.sic.gov.co/sites/default/files/files/2023/RE61609-2023.pdf>



- Superintendencia de Industria y Comercio (SIC). (2023d). *Resolución Número 68753 de 2023 (01 de noviembre de 2023): Por la cual se impone una sanción y se imparten órdenes administrativas*. Ministerio de Comercio, Industria y Turismo. <https://sedeelectronica.sic.gov.co/sites/default/files/normativa/RE68753-2023.pdf>
- Vela Reyna, J., Olmedo Noguera, C., e Ibarra-Cisneros, M. (2024). E-commerce: experiencia, seguridad, confianza y satisfacción. *Investigación Administrativa*, 53(133), 00005. <https://doi.org/10.35426/iav53n133.05>



Capítulo 5

Aspectos legales y éticos de la Inteligencia Artificial: un enfoque en LLM y arquitecturas RAG

Daniel Betancur Vásquez

Daniel Carmona Cardona

Edwin Alexánder Moncada

Introducción

En la era contemporánea, la inteligencia artificial (IA) ha emergido como una fuerza transformadora en diversos sectores, desde la medicina hasta el entretenimiento, pasando por la educación y los negocios. A medida que esta tecnología avanza, se vuelve imperativo abordar de manera crítica los aspectos legales y éticos que surgen en su implementación y desarrollo. La rápida evolución de los Modelos de Lenguaje Grande (LLM, por sus siglas en inglés) y las arquitecturas de Recuperación de Información y Generación de Respuestas (RAG, por sus siglas en inglés) plantea desafíos significativos en el ámbito legal y ético, en términos de protección de datos, transparencia, rendición de cuentas y no discriminación, que se deben atender con seriedad y rigor.

Uno de los aspectos más cruciales en el debate sobre la IA es la protección de datos. La capacidad de los LLM para manejar y analizar grandes volúmenes de información personal, plantea interrogantes sobre cómo se garantiza la privacidad y la seguridad de los datos. Las regulaciones emergentes, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, buscan establecer un marco que asegure que el manejo de datos personales se realice de manera ética y conforme a los derechos de los individuos.

En paralelo, la transparencia en el funcionamiento de la IA se erige como un principio fundamental. La opacidad en los mecanismos de los LLM y las arquitecturas RAG puede llevar a una falta de claridad sobre cómo se toman las decisiones automatizadas, la cual puede minar la confianza en la tecnología y en sus aplicaciones. Por tanto, es esencial que los sistemas de IA sean diseñados y operados de manera que sus procesos sean comprensibles y sus decisiones explicables.



La rendición de cuentas en el contexto de la IA implica establecer responsabilidades claras tanto para los desarrolladores como para los usuarios. La capacidad de los sistemas de IA para influir en decisiones críticas requiere mecanismos de supervisión que aseguren que sus acciones sean justificables y estén alineadas con estándares éticos y legales. Sin una adecuada rendición de cuentas, los sistemas de IA podrían generar consecuencias no deseadas y daños y erosionar la confianza pública en estas tecnologías.

Finalmente, los LLM y los sistemas RAG deben ser evaluados y ajustados para minimizar el riesgo de sesgos y garantizar que su funcionamiento sea justo y equitativo para todos los grupos demográficos. La no discriminación es un principio esencial para prevenir que los sesgos presentes en los datos utilizados para entrenar los modelos perpetúen injusticias y desigualdades.

La Inteligencia Artificial es una herramienta que cada día se afianza más en las diferentes aplicaciones donde se usa, y es importante presentar la interacción con el componente jurídico, y cómo en Colombia y el mundo se viene legislando para una mejor utilización.

Protección de datos y privacidad: reflexiones normativas

El primer antecedente legal sobre la privacidad proviene de Estados Unidos, con el juez Cooley quien, en su obra *The Elements of Torts*, definió la privacidad como el “derecho a estar solo”, concepto que sintetiza la idea de la privacidad como la soledad y tranquilidad a la que tienen derecho los individuos en un estado (Rebollo y Saltor, 2013). Años después, Warren y Brandeis desarrollaron el concepto de intimidad en un artículo que surgió como respuesta a la invasión de la prensa en la vida privada de Warren, lo cual abrió el camino a la creación de un nuevo derecho de protección a la intimidad, que eventualmente fue aplicado por el tribunal de Nueva York, y se consolidó como el “derecho al disfrute de la vida” (Prosser, 1960). Sin embargo, su fijación como norma tomó cerca de un siglo, y se destacaron casos como *Carliss & Walke Company* y *Robinson & Rochester Folding Box Company*, en los que aún no se reconocía plenamente el derecho a la intimidad; sin embargo, el segundo caso fue clave para el reconocimiento de los derechos de imagen en la legislación de Nueva York (Rebollo y Saltor, 2013).

Cronológicamente, otro antecedente relevante es la sentencia de la Corte Suprema de Georgia en el caso *Pavesick & New England Life Insurance*, donde se reconoció que la libertad personal abarcaba tanto el derecho a la vida pública como a la intimidad (Rebollo y Saltor, 2013). Posteriormente, en 1935, se aprobó en Estados Unidos la *Social Security Act*, que estableció la recopilación de información de



trabajadores, aunque, por su magnitud, se buscó hacerla viable mediante nuevos mecanismos (Rebollo, 2018). Durante la Segunda Guerra Mundial, proyectos como Colossus y ENIAC introdujeron la computación para manejar grandes volúmenes de datos. En la década de 1960, el procesamiento de datos cobró importancia, y en 1968 IBM introdujo el primer sistema de gestión de bases de datos, lo que generó preocupación por el posible uso abusivo de la información (Rebollo y Serrano, 2008).

En Europa, las primeras normativas de protección de datos fueron la alemana *Datenschutz* y la sueca *Data Lag* de 1970 y 1973, respectivamente, ambas fueron precedidas por la Resolución 509 de 1968 del Consejo de Europa, que advertía sobre los riesgos de las nuevas tecnologías para los derechos humanos, y por resoluciones del Comité de Ministros que recomendaban precauciones para evitar el uso indebido de datos personales en bancos de datos (Rebollo, 2018). Posteriormente, se promulgaron la *Privacy Act* en Estados Unidos y la ley de protección de datos en Francia en 1978, que se convirtieron en normas de referencia en la materia (Rebollo y Serrano, 2008).

Estos antecedentes y normativas se establecieron antes de la revolución de las comunicaciones, cuando aún no se contemplaba el poder masivo de Internet para gestionar datos. Con la popularización de Internet, surgieron nuevas preocupaciones y, con ellas, la necesidad de involucrar al Estado en la regulación para evitar la vulneración de derechos (Rebollo, 2018). Finalmente, entre los antecedentes más próximos a la normativa de la Unión Europea, se encuentran el Convenio de 1981 del Consejo de Europa y el Acuerdo Schengen de 1985, así como el fallo de 1983 del tribunal alemán, que declaró inconstitucionales partes de la ley de censo de 1982 y estableció el derecho a la autodeterminación informativa (Rebollo y Saltor, 2013). Esta evolución obligó a Estados Unidos a modificar su *Privacy Act*.

La protección de los datos personales nace como resultado de la extensión del derecho a la intimidad. Primero, se vio como el límite al Estado para que no extralimitara sus funciones relacionadas con la recolección de datos con el propósito de cumplir sus fines como Estado. Luego, con los avances tecnológicos y la masificación de las telecomunicaciones, se ha visto como una barrera de contención a quienes tienen la capacidad de gestión de grandes cantidades de información que, de facto, les brinda la posibilidad de irrumpir en la intimidad de los propietarios primarios de los datos.

De igual forma, es importante tener en cuenta que la gestión de datos, con los últimos avances de la tecnología, ha tenido que volcarse a cambios que le permitan acercarse a regular las situaciones que se presentan con las nuevas tecnologías y, en especial, con las plataformas de gestión de internet.



Reglamento europeo de protección de datos

Para hablar sobre este reglamento de protección de datos, es necesario abordar algunas cuestiones que se encuentran por fuera de la norma y han sido determinantes para consolidar esta regulación en la Unión Europea.

Se ha destacado que el principal inconveniente que contenía la legislación anterior (Directiva 95/46/CE) se presentaba con respecto a la posibilidad de poder enviar datos personales a terceros países bajo ciertas circunstancias. El mejor ejemplo de la materialización de este supuesto normativo puede verse con el denominado acuerdo de “puerto seguro” o *Safe Harbour*, que fue aprobado en el año 2000 y que, en palabras del comisario de Mercado Interior, Frits Bolkestein, “ayudaría a explotar el enorme potencial de la revolución de la información al ofrecer seguridad jurídica a los operadores y protección de la vida privada de los consumidores” (Comisión Europea, 2000).

Tratados Safe Harbour y Privacy Shield

El tratado de Safe Harbour, establecido entre la Unión Europea y el Gobierno de los Estados Unidos, permitía la transferencia de datos desde la UE a los EE. UU., a pesar de las diferencias legislativas en la protección de datos, amparada en los artículos 25 y 26 de la Directiva 95/46/CE (Ortega, 2014). En Europa, la Directiva 95/46/CE impone requisitos estrictos para el tratamiento de datos personales, reconocidos como un derecho fundamental en la Carta de Derechos Fundamentales de la UE (Unión Europea, 2016). En contraste, la legislación estadounidense, basada en la Privacy Act, combina regulación sectorial, autorregulación y legislación, aplicables solo a ciudadanos y residentes permanentes de EE. UU., lo que permite un nivel de protección menor y una vigilancia extensiva bajo la ley FISA 702 (Noyb, 2020; Ortega, 2014). Esta disparidad llevó a que, a pesar del acuerdo Safe Harbour, las plataformas tecnológicas enfrentaran dificultades para cumplir con las normativas europeas debido a la obligación de proporcionar datos a autoridades estadounidenses, como reveló Edward Snowden en 2013 (Noyb, 2020). La demanda de Maximillian Schrems contra Facebook condujo a la invalidación de Safe Harbour y al desarrollo de un nuevo marco normativo, el Reglamento UE 2016/679, que buscaba una mejor adecuación a las condiciones de protección de datos.

La transición hacia el Privacy Shield, implantado tras la sentencia del CJEU del 6 de octubre de 2015, buscó superar las deficiencias de Safe Harbour. Aunque el Privacy Shield mantenía similitudes con su predecesor, introdujo medidas adicionales como la notificación a titulares de datos, la opción de exclusión, la limitación del acceso y la creación de un defensor del pueblo independiente en EE. UU. (Unión



Europea, 2016; Agencia de los Derechos Fundamentales de la Unión Europea, 2018). Sin embargo, estas medidas no resolvieron los problemas fundamentales de acceso a datos por parte del gobierno estadounidense, lo que llevó a invalidar el Privacy Shield en 2020 mediante el caso C-311/18, conocido como Schrems II (Noyb, 2020). Ambos acuerdos demostraron ser más una herramienta comercial que una solución efectiva a las diferencias en la protección de datos, y subestimaron las implicaciones de la recolección y el tratamiento de datos personales.

Análisis del Reglamento UE 2016/679

Luego de exponer las situaciones que antecedieron y acompañaron la promulgación del reglamento UE 2016/679, corresponde ahora hablar en estricto sentido sobre este. En mayo de 2016, fue publicado en el diario oficial de la Unión Europea el vigente reglamento de protección de datos de las personas físicas, mediante el cual se derogó la Directiva 95/46/CE. El proceso para llegar a esta nueva normativa no fue corto y tuvo varios años de desarrollo antes de poder ver la luz.

El interés por modificar la Directiva 95/46/CE comenzó entrada la segunda década del siglo XXI, el 4 de noviembre de 2010, con una comunicación⁴³ del Parlamento Europeo sobre la importancia de adoptar un enfoque global de protección de datos personales en la Unión Europea (Hernández López, 2018). Hablar sobre el enfoque global implicaba un viraje en la estrategia de protección de datos hacia su actualización, con respecto a la expansión de Internet y de las plataformas que lo usan como medio de difusión. En esta comunicación se expone, por primera vez, la intención de actualizar una norma que había sido redactada para una época anterior a Internet y que era anterior a la Carta de los Derechos Fundamentales de la UE y, por consiguiente, a los derechos que consagra en materia de protección de datos. Se necesitaba una normativa capaz de desarrollar la Carta y atender los avances tecnológicos de la sociedad de la información (López Aguilar, 2019). Luego de este comunicado, en enero de 2011, se publicó un dictamen⁴⁴ del Supervisor Europeo de Protección de datos donde se soporta la comunicación del Parlamento y se resaltan algunos temas destacables que deberían ser incluidos dentro de la perspectiva del nuevo proyecto legal. Estos temas se ven condensados en la ampliación del marco de protección para los usuarios, la aplicación de una perspectiva global del derecho aplicable, la protección de la privacidad desde el propio diseño de las herramientas de gestión de datos, entre otros.

En el año 2012, por iniciativa de la Comisión Europea, se dio trámite a la propuesta de reglamento del Parlamento Europeo relativo a la protección de datos

⁴³ El documento se encuentra disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52010DC0609>

⁴⁴ El texto del dictamen se encuentra disponible en: https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf



personales. Desde ese momento, se comenzó a trabajar de manera activa en la redacción de una norma que reemplazara la Directiva 95/46/CE (Hernández López, 2018). La iniciativa sobre la nueva normativa de protección de datos se vio inmersa en la legislatura europea 2009-2014, siendo esta la primera legislatura del Parlamento Europeo tras la vigencia del tratado de Lisboa. Así lo describe, para esas fechas, el eurodiputado López Aguilar (2019):

[...] los proyectos de Reglamento de Protección de Datos 2016/679, que pasó a ser denominado RGPD (o GDPR, por sus siglas en inglés), y la nueva Directiva para la Protección de Datos en la Investigación de Delitos 2016/680 (conocida como “*Police Directive*”, por tener como destinatarios a las *Law Enforcement Agencies*) pasaron a ser objeto de una discusión tan prolongada como tensa y exhaustiva durante todo el mandato, con la perspectiva ambiciosa de dar un salto adelante en la protección de la privacidad y la confidencialidad de los datos personales de la ciudadanía europea. (p. 32)

En los debates para la construcción de la norma, uno de los primeros puntos de interés que se marcó fue la necesidad de que esta normativa no se viera disgregada en un montón de pequeñas normas que formaran parte de un marco jurídico. Más bien se esperaba que fuera un texto completo y autónomo que tuviera la robustez necesaria para poder llevar a buen camino sus perspectivas regulatorias. Otro de los puntos importantes tiene que ver con el cambio de paradigma que se pretendía introducir: no se buscaba una norma para permitir o, simplemente, regular la libre circulación de datos, sino que se pretendía un cambio de paradigma con respecto a la interpretación de lo que significa el tratamiento de datos personales; se buscaba la concesión de la autodeterminación informativa. Es decir, se introduce la idea de que los datos constituyen un aspecto relevante de nuestra identidad y se obliga, a quienes los gestionen, a tener una responsabilidad proactiva sobre ellos. Esta situación se ve expresada en el fortalecimiento de derechos de acceso, rectificación y cancelación (López, 2019, p. 32) y en conceptos como el de privacidad por defecto y desde el diseño. Otro de los aspectos esenciales en los que se concentró la nueva normativa tendría que ver con hacerles frente a las llamadas *big tech*, que participaron activamente en el proceso a través de los mecanismos de participación propios de quienes son directamente afectados por una norma y del uso de sus influencias (*lobby*).

El proyecto normativo no sería aprobado durante la legislatura 2009-2014, pasaría a serlo en la siguiente. Luego de que la Comisión Europea lo pasara, en 2012, a los diferentes grupos de trabajo, fue aprobado en 2014, mediante resolución legislativa del Parlamento Europeo, el *Data Protection Package* (López, 2015). En 2015 se llegó a un acuerdo sobre el enfoque general del reglamento (Hernández, 2018), en 2016 se aprobó la norma, que fue publicada en el Diario Oficial de la Unión Europea, y 20 días después de su publicación entró en vigor y comenzó a tener efectos jurídicos desde el 18 de mayo de 2018.



Como ya se ha expresado, el RGPD introdujo una reforma sustancial a la perspectiva general sobre el tratamiento de datos. Se cambia el paradigma de libre circulación por el paradigma de gestión responsable de datos. Esta situación se evidencia en las definiciones que se dan dentro de la propia normativa. Por ejemplo, la definición de dato de carácter personal es, sustancialmente, diferente con respecto a la anterior normativa. Así, la nueva definición nos dice que dato personal no solo es el dato como tal, sino la información resultante del dato. Se entendería, entonces, que un dato personal es cualquier dato que, incluso sin estar directamente relacionado con una persona, sí permita directa o indirectamente llegar a ella (Davara, 2017). También se introduce la definición de dato biométrico, se modifica la definición de consentimiento y se inserta el concepto de *Data Protection Officer* (DPO). Frente a los datos biométricos, dice que son los datos personales obtenidos a través de tratamientos técnicos específicos, entre los cuales se incluyen las características físicas, fisiológicas o de conducta de una persona que permitan su identificación inequívoca, y prohíbe que estos sean utilizados para tal fin (claro está, por fuera de las labores policiales sobre las que el Estado detenta su monopolio). Además, se crean unas excepciones, como expresar el consentimiento inequívoco para ese fin, para proteger los intereses vitales del interesado y por razones de interés público.

Frente al consentimiento, en el texto del RGPD se dice que es toda manifestación de voluntad libre, específica, informada e inequívoca mediante la cual el interesado acepta la gestión de sus datos; se elimina la posibilidad del consentimiento tácito (Davara, 2017). Conviene reflexionar sobre el consentimiento desde una perspectiva material, pues, materialmente, el consentimiento se puede expresar de muchas formas, pero para hacerlo de una manera inequívoca debe tenerse pleno conocimiento de lo que sucederá con el hecho consentido. Esto constituye un problema no menor, porque en la práctica descartamos el hecho de atender las recomendaciones y avisos previos que se nos presentan antes de darnos de alta en, por ejemplo, las aplicaciones de gestión de opinión. Nos vemos coaccionados a aceptar las cláusulas tipo de estas plataformas, porque de lo contrario no podríamos acceder a sus productos. En juicio de compensación, siempre terminará teniendo más valor el acceso a estas plataformas porque tienen valor y relevancia social. Además, por motivos de la propia confidencialidad de la propiedad intelectual que estas empresas tienen sobre sus productos, nunca podremos saber, ciento por ciento, qué destino tendrá la información que les brindemos. Desde esta perspectiva, nuestro consentimiento no podrá ser libre, plenamente informado y capaz, por sí mismo, a la hora de proteger nuestra privacidad, sino que tendrá que ser asistido por la coacción de un tercero regulador que vigile las condiciones exógenas que permitan su cumplimiento. En todo caso, en su aspecto más material, resulta utópico que todo consentimiento expresado sea plenamente libre e informado.



Otra figura que es una novedad en el RGPD es la del delegado de protección de datos (DPO), quien es la persona encargada de velar por el cumplimiento de la protección y de garantizar que se realice una gestión de datos acorde con el reglamento (Davara, 2017). En determinadas circunstancias, será elegido por la entidad responsable del fichero, pero, en general, se podrá elegir entre los empleados del responsable del fichero o mediante una empresa que preste estos servicios. Es obligación del responsable del fichero compartir los datos de contacto del DPO. Básicamente, es una figura que funge el papel de un tercero mediador entre el integrado y el responsable del fichero, es decir, quien realiza la gestión de los datos. Es una forma expedita en que los interesados pueden ejercer sus derechos con respecto a los datos. En síntesis, es un tercero que funge como mediador y agente de cumplimiento entre las diferentes partes involucradas: autoridades, responsables e interesados.

En el propio paradigma que introdujo el RGPD, es importante destacar que se trazaron unas obligaciones para los encargados de la gestión de datos. La estructura del Reglamento contempla la existencia de obligaciones y de derechos. Las obligaciones se encuentran detalladas en los principios que debe cumplir el responsable del fichero. Los derechos, por su parte, son los que tienen los interesados con respecto al tratamiento de sus datos (Davara, 2017). Entre las obligaciones que tiene el responsable, se encuentran:

- La transparencia y licitud del tratamiento.
- Privacidad por defecto y desde el diseño.
- Evaluación del impacto.
- Protección frente a las violaciones de seguridad.
- Accountability.

Grosso modo, la transparencia y licitud del tratamiento se refieren a que sus responsables brinden mayor información a los usuarios sobre el tratamiento que les realizan a sus datos. Se entiende que el tratamiento es lícito cuando se ha tenido consentimiento previo (Agencia Europea de Derechos Fundamentales, 2018). Por ejemplo, frente a los menores se especifica que debe hacerse en un lenguaje que estos puedan comprender. El principio más novedoso e interesante que se introduce a través del RGPD es el de privacidad por defecto y desde el diseño. Este principio es el que, materialmente, tiene mayor capacidad de cambiar la protección de datos personales. A través de él se pretende que las herramientas sean creadas de modo que no sean demasiado invasivas y que su diseño se realice de forma que la privacidad sea su punto central (Piñar, 2016). La privacidad desde el diseño tiene una doble funcionalidad: por un lado, crea las condiciones idóneas para que los datos se encuentren protegidos, por otro, les limita el recaudo de datos y de información a los responsables del tratamiento. En la práctica, la privacidad por defecto se hace evi-



dente cuando el usuario no tiene que configurar sus preferencias de privacidad para tener mayor grado de protección. El principal inconveniente será la verificación de su cumplimiento por parte de los encargados de gestionar los datos (Duaso, 2016).

En cuanto a la seguridad, nos encontramos con la misma definición que en el reglamento anterior, pero con algunos cambios respecto de las consideraciones sobre la seguridad de los sistemas y la no intromisión de terceros. Otro de los principios novedosos que introdujo el RGPD ha sido el de “contabilidad” (*accountability*), o registro de los tratamientos de datos realizados. Las organizaciones no solo están obligadas a adherirse al cumplimiento de los principios en Protección de Datos, sino que deben demostrar este cumplimiento y documentar los tratamientos (Davara, 2017, p. 192).

Otro grupo de novedades que entró a formar parte del RGPD, son los derechos inherentes a la protección de datos. Entre estos podemos encontrar el derecho al olvido digital, el derecho a la información y el derecho a la portabilidad de datos. Este último, por ser el más novedoso, merece especial cuidado. El derecho a la portabilidad de los datos se refiere a que el titular de los datos, que haya facilitado a un responsable del tratamiento, tendrá derecho a recibir los datos personales que le incumban en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado (Davara, 2017, p. 196).

Nos corresponde, ahora, hablar sobre uno de los puntos más controversiales en relación con el tratamiento de datos: el envío de datos a terceros países para su tratamiento. Con los antecedentes de lo que sucedió con este apartado normativo, se presentaron algunos cambios con respecto a las condiciones para considerar que un tercero cumple con condiciones análogas de protección de datos. En consecuencia, se expresa, por un lado, el convencimiento de que las transferencias internacionales no solo son una realidad, sino una necesidad y, por otro, la preocupación por ofrecer un nivel de protección de datos adecuado con relación a esta situación (Piñar, 2016, p. 429). Lo primero que se debe considerar es que el nivel de protección de datos ha sufrido un cambio sustancial y ahora se aprecia como mayor. Por lo tanto, para considerar un nivel de protección como análogo deberá tener características similares al actual. Esta situación es complicada porque la normativa europea es una de las más avanzadas en este sentido. Por este motivo, toman relevancia las condiciones materiales que se establecen para ser consideradas análogas o que, sin serlo, se permita el tránsito de datos. De acuerdo con el capítulo quinto del Reglamento, que no difiere semánticamente de su respectivo análogo en la Directiva 95/46/CE, las condiciones para que se puedan transferir datos son (Comisión Europea, 2017):

- Mediante una decisión de adecuación de la Unión Europea que declare que un Estado no perteneciente a la UE presenta un nivel adecuado de protección. Esta



decisión permite que se puedan transferir datos sin que su exportador deba ofrecer más garantías o esté sujeto a condiciones adicionales. Estas transferencias son asimiladas como transferencias entre Estados miembros.

- Si no existe una decisión de adecuación, la transferencia se podrá hacer mediante el establecimiento de garantías adecuadas y con la condición de que se puedan tener acciones para validar los derechos de los interesados en gestión de datos. Las garantías exigidas se ven expresadas en:
 - **Normas corporativas vinculantes.** Son las que se presentan en los casos de los grupos empresariales y de las empresas que tienen una actividad económica común.
 - **Acuerdos contractuales con el destinatario de los datos personales.** Estos se utilizan, mayormente, a través de las cláusulas tipo aprobadas por la UE.
 - **La circunscripción de estas compañías a un código de conducta.** Un mecanismo de certificación junto con compromisos vinculantes y exigibles frente a la protección de datos que se les debe brindar a los interesados.

En caso de no concurrir alguna de las situaciones anteriores, se podrá realizar la transferencia mediante el consentimiento explícito e informado por parte de los interesados.

Uno de los aspectos positivos de esta situación ha sido que, para equipararse al nivel de protección ofrecido por la ley europea, la mayor parte de estas compañías han adaptado, progresivamente, su autorregulación para poder cumplir con los estándares que solicita la ley (Ustarán y García, 2019). En este aspecto, el RGPD ha tenido un rol fundamental, al ser moldeador de las políticas de datos públicas y privadas alrededor del mundo. Aunque esta situación es en parte excepcional, no describe la realidad del panorama de gestión de datos con terceros países (Rebollo, 2018). La manera más efectiva y usada sigue siendo mediante la adherencia a tratados como el *Privacy Shield*.

Con respecto al *Privacy Shield*, es importante destacar que se promulgó durante la vigencia del RGPD. Sin embargo, debido a que este último solo tendría efectos a partir de 2018, su vigencia se circunscribió a la Directiva 95/46/CE. Esta situación es importante porque, luego de la entrada en vigencia del RGPD, no tendría que revocarse el acuerdo, ya que, en la propia normativa, el artículo 45.9 nos señala que los acuerdos firmados durante la vigencia de la normativa anterior seguirían siendo efectivos hasta que fueran modificados por una nueva decisión. Aunque el acuerdo (actualmente invalidado por la sentencia C-311/2018) hubiera sido modificado por una decisión de la autoridad europea, no ofrecería un nivel de protección adecuado,



porque no solucionaría la situación de fondo: el tratamiento ilícito de datos europeos por parte de las autoridades de los Estados Unidos.

Los esfuerzos de la ley se ven desbordados por la magnitud de la cuestión que se debe regular y por la forma como se expresan sus efectos prácticos. Si bien se ha intentado la aplicación práctica de nuevas figuras que aumenten la robustez de las medidas frente al tránsito de datos con terceros países, como la introducción de la adherencia a códigos de conducta, la realidad del RGPD es que da continuidad al *status quo* implementado por la Directiva 95/46/CE (Ustarán y García, 2019). Al continuar preservando las condiciones de la anterior norma, la directiva no cuenta con la capacidad de poner freno a las acciones que llevaron a la invalidación del acuerdo *Safe Harbour*. Sus únicas herramientas reales frente a la protección de datos se ven expresadas en no certificar a otros países, porque no cuentan con condiciones análogas como, por ejemplo, la privacidad por defecto o desde el diseño.

En consideración a lo anterior, se evidencia que la normativa, pese a su esfuerzo y ambición de robustez, no tiene efectos capaces de solucionar los inconvenientes propios de la disyuntiva que presentan los asuntos de *Safe Harbour* y *Privacy Shield*. Aunque se prohíba la posibilidad de realizar transferencias de datos, esto no ocurrirá. Vale la pena, entonces, preguntarse por qué si Estados Unidos no cumple los estándares de protección europeos, no se ha detenido el flujo de datos que existe con compañías estadounidenses. La respuesta a esta pregunta tiene dos vertientes. La primera se expresa en la consideración 101 del RGPD: “porque no puede detenerse la expansión del comercio”. La segunda es mucho más práctica: por la existencia de otros mecanismos que estas empresas pueden pactar con la Unión o con los propios usuarios interesados en la gestión de datos, con el fin de que puedan seguir ejerciendo sus actividades con normalidad. Un caso serían las cláusulas SSC (CCE), que analizaremos más adelante. El principal problema de esta segunda respuesta es que no soluciona sino que, por el contrario, legitima el hecho de que un país tercero pueda acceder a datos personales —potencialmente formadores de opinión— de los ciudadanos europeos. Por este motivo, pese al fallo de la sentencia C-311/2018 mediante la cual se invalidó el acuerdo del *Privacy Shield*, estas compañías siguen realizando transferencias de datos, entre sus filiales europeas y sus matrices norteamericanas, con total normalidad.

Protección de datos en Colombia

El derecho fundamental al *habeas data* está consagrado constitucionalmente por medio del artículo 15 de la Constitución Política de 1991 y el desarrollo jurisprudencial de la Corte Constitucional a partir del año 1992, con relación a los derechos de los ciudadanos a tener conocimiento de la composición, actualización y rectificación



de las informaciones que se hubieren acumulado “sobre ellos en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales” (Escobar y Pajarito, 2014, p. 8). La información es parte fundamental en el mundo actual de las telecomunicaciones. Por esa razón, el 17 de octubre de 2012, el Gobierno Nacional promulgó la Ley Estatutaria 1581 de 2012, se dice que es ley estatutaria porque se entiende que está instituida principalmente para regular y proteger los derechos de los titulares. Dicha ley propende por la protección de los datos personales registrados en bases de datos y en archivos, lo cual tiene que ver con el tratamiento de datos que hacen las entidades tanto públicas como privadas, que pueden realizar acciones como recolección, almacenamiento, uso, circulación o eliminación de datos.

La jurisprudencia constitucional ha tratado desde el principio el derecho al *habeas data* como una garantía del derecho a la intimidad. Conforme a esta idea, se habla de la salvaguarda de los datos que sean del dominio de la vida privada y familiar, comprendida como el entorno individual impenetrable donde las personas pueden realizar su proyecto de vida y donde ni el Estado u otros actores particulares pueden intervenir (Colombia Digital y Certicámara, 2014). La intimidad envuelve la posibilidad de reclamar respeto por parte de los demás en relación con el ámbito que le interesa solo al individuo, y que se refleja en la protección de las posesiones privadas, los gustos particulares y las actitudes personalísimas (Sentencia T-552, 1997).

En Colombia, el *habeas data* es una garantía y un derecho fundamental dado que “pretende la protección de situaciones y condiciones indispensables para que las personas puedan desarrollar sus proyectos vitales sin obstáculos y con decoro en el contexto de la sociedad de la información” (Escobar y Pajarito, 2014, p. 10). Es claro que ahora el *habeas data* es esencialmente un derecho autónomo, que está conformado por la independencia informática y la libertad económica. Este derecho necesita para su autonomía de la protección real de una serie de elementos que lo aseguren, los cuales no pueden depender solo de la actividad de los jueces, sino que también deben estar encuadrados en una institucionalidad administrativa que, además de ejercer control y vigilancia a los sujetos de derecho tanto público como privado ratifique el cumplimiento efectivo de la protección de datos. Entre los alcances mínimos que emanan del derecho de *habeas data*, está el derecho de las personas a tener acceso a la información que sobre ellas está contenida en bases de datos, lo que implica poder conocer los datos contenidos en ellas, adicionalmente, el derecho a introducir nuevos datos con el fin de que se provea una imagen completa del interesado y el derecho de poder actualizar la información, es decir, que la información que se encuentre en bancos de datos sea rectificada o corregida, de manera que se ajuste a la realidad, o la posibilidad de eliminar información de un banco de datos, ya sea porque se hizo un uso indebido de ella, o por voluntad del interesado, exceptuando lo previsto en las normas.



El tratamiento y flujo de los datos personales debe garantizar la protección de los derechos fundamentales de sus titulares ante los posibles atropellos que sean objeto por acción de los administradores de bases de datos o archivos, teniendo acceso a información falsa, inexacta, incompleta o sin autorización por parte del titular. En respuesta a esta preocupación, fueron promulgadas las leyes 1266 de 2008 y 1581 de 2012, la primera se ocupa del tratamiento de la información que se encuentra en bases de datos personales de carácter financiera, crediticia, comercial, de servicios y la proveniente de terceros países. La segunda hace referencia a mandatos generales para la protección de datos personales (Escobar y Pajarito, 2014, p. 8). Con el tiempo y el desarrollo jurisprudencial

se ha establecido un marco normativo para una protección real de los titulares de la información, manejada por los usuarios, operadores o fuentes de información. La Corte Constitucional y las normas antes mencionadas se han manifestado continuamente con el fin de salvaguardar los derechos del titular de la información, [...] que los datos personales deben ser manejados con autorización previa y expresa del ciudadano, y que no puede administrarse información desactualizada, errada y no autorizada (Escobar y Pajarito, 2014, p. 8).

Es importante resaltar que se trata de una clara manifestación del compromiso que adquirió el país en la protección de este derecho, con el fin de eliminar las barreras en la transferencia de datos personales a Colombia, ya que antes de la entrada en vigencia de la Ley 1581 de 2012, la Unión Europea consideraba a Colombia como un país no seguro en protección de datos, pero con esta ley se buscó que el país fuera un mercado más atractivo en la región en lo que tiene que ver con tercerización de servicios, para lograr un impulso importante en el sector empresarial. Conforme a lo anterior, hoy en día, uno de los límites más característicos en el mundo empresarial y comercial es el derecho fundamental del *habeas data*, que fue consagrado en Colombia con la promulgación de la Constitución Política de 1991, pero solo se estableció dentro del sistema jurídico a partir del año 2013, cuando entró en vigencia la Ley 1581 de 2012 y su decreto reglamentario 1377 de 2013.

Entre sus fundamentos, la norma incluye varios principios. En primer lugar, el principio de acceso y circulación restringidos, por medio del cual se busca establecer que la administración de los datos personales se sujete a los límites que se derivan de su naturaleza, de la norma estatutaria y de los criterios que le son aplicables a esta actividad, en especial los de temporalidad de la información y finalidad del banco de datos. Asimismo, en virtud de este principio, no se podrá acceder a los datos personales —salvo la información pública— por internet o por otros medios de divulgación o comunicación masiva, a menos que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o a los usuarios autorizados para ello, en los términos de la disposición estatutaria.



En segundo lugar, el principio de seguridad. De acuerdo con este principio, en la información personal contenida en bases de datos y la resultante de las consultas que realicen los usuarios, se deben incorporar las medidas técnicas necesarias para garantizar la seguridad de los registros, a fin de evitar su adulteración, pérdida, consulta o uso no autorizados.

Por otro lado, con el principio de confidencialidad, todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, incluso después de finalizada su relación con alguna de las labores que comprende el tratamiento, y solo pueden suministrar o comunicar datos personales cuando ello corresponda con el desarrollo de las actividades autorizadas en la ley.

De igual forma, la ley establece mecanismos de vigilancia y sanción. La violación al derecho de *habeas data* ocurre cuando la información contenida en el archivo o base de datos se recoge de manera ilegal sin el consentimiento del titular del dato, es errónea o recae sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente. Con la promulgación de la Ley 1581, se creó la Autoridad de Protección de Datos Personales de la Superintendencia de Industria y Comercio, con el fin de que dicha entidad ejerza la vigilancia para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

Aunque la normativa colombiana sobre *habeas data* representa un gran avance en la protección de los datos personales, todavía no alcanza los estándares establecidos por el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Un ejemplo claro es la implementación de la privacidad por defecto, que en Colombia aún no ha sido incorporada y no se desarrolla con la misma rigurosidad que en el marco europeo. Esta diferencia subraya la necesidad de seguir fortaleciendo el marco jurídico colombiano para garantizar una protección efectiva y proactiva de los derechos de los titulares de datos, sobre todo en los albores de la aplicación de tecnologías de inteligencia artificial, como los LLM y las arquitecturas tipo RAG.

Transparencia y explicabilidad con el uso de la IA

El uso de modelos de lenguaje grande (LLM, por sus siglas en inglés) en el ámbito legal y jurídico plantea una serie de consecuencias significativas cuando se evalúa desde la perspectiva de métricas filosóficas de medición de eficiencias. Estas métricas filosóficas consideran, más allá de las métricas técnicas tradicionales, aspectos como la justicia, la equidad, la responsabilidad y la transparencia. En términos de justicia y equidad, los LLM pueden perpetuar y amplificar los sesgos presentes en los datos



con los que fueron entrenados, lo que podría resultar en decisiones legales injustas (Cheong et al., 2024). Al reflejar sesgos inherentes a los datos de entrenamiento, los modelos de lenguaje pueden exacerbar desigualdades, lo cual es particularmente problemático en contextos legales donde la imparcialidad es fundamental.

La responsabilidad es otro aspecto crítico. La opacidad de los LLM dificulta la atribución de responsabilidad cuando ocurren errores o se toman decisiones injustas. En el contexto legal, esto plantea serias preguntas sobre quién es responsable cuando un modelo sugiere una interpretación errónea de la ley. Naik et al. (2022) señalan que la falta de transparencia en los sistemas de inteligencia artificial puede erosionar la confianza en las decisiones que toman estos sistemas, especialmente en contextos sensibles como el legal. La explicabilidad es también un desafío significativo. La dificultad para interpretar los LLM complica la justificación de las decisiones legales basadas en sus recomendaciones, lo que puede socavar la confianza pública en el sistema legal. Se argumenta que la explicabilidad es esencial para garantizar que las decisiones de la inteligencia artificial sean comprensibles y aceptables, especialmente en contextos jurídicos.

En términos de eficiencia y costo, aunque los LLM pueden acelerar la resolución de casos legales y reducir costos, existe el riesgo de que esto se logre a expensas de la precisión y la justicia, se manifiesta que la eficiencia técnica no debe obtenerse a costa de valores fundamentales como la equidad y la justicia en la aplicación de la ley.

Desde una perspectiva filosófica más amplia, la integración de LLM en el ámbito jurídico cuestiona la naturaleza de la ley y su interpretación. La pregunta central es si la ley es simplemente un conjunto de reglas a seguir o si es un campo dinámico que requiere interpretación humana basada en principios morales y éticos. Floridi (2019) sostiene que la filosofía de la inteligencia artificial debe considerar cómo estas tecnologías afectan la capacidad humana para tomar decisiones éticas y responsables, particularmente en áreas críticas como la ley. Por eso las políticas y regulaciones deben guiar el desarrollo de estas tecnologías para asegurar que su aplicación sea coherente con los valores fundamentales del sistema legal.

Entre los temas primordiales para tener en cuenta, está la comparación cognitiva entre el LLM y un humano, considerando el contexto de razonamiento artificial y natural. Pensar en una herramienta de medición de razonamiento del LLM es un reto filosófico. Se podría pensar en situaciones similares a la medición de IQ y otros métodos tradicionales en el contexto humano. Existen métricas de evaluación de la respuesta de un LLM, a saber:



1. **BLEU (Bilingual Evaluation Understudy):** Mide la precisión de N-grams, comparando la respuesta generada con la referencia. Calcula la similitud usando la media geométrica ponderada por N-grams.
2. **ROUGE (Recall-Oriented Understudy for Gisting Evaluation):** Mide la superposición de N-grams, cadenas de palabras y subsecuencias entre la respuesta generada y la de referencia.
3. **METEOR (Metric for Evaluation of Translation with Explicit ORDERing):** Combina precisión y *recall unigrama*, utilizando *stemming* y coincidencia de sinónimos. Busca correlación con el juicio humano en el nivel de oración.
4. **Perplejidad:** Se calcula a partir de la pérdida de log-verosimilitud del modelo, midiendo la probabilidad de predecir una secuencia de palabras.
5. **CIDEr (Consensus-based Image Description Evaluation) (multimodal):** Evalúa descripciones generadas para imágenes, ponderando N-grams raros mediante TF-IDF y utilizando la similitud de coseno.
6. **SPICE (Semantic Propositional Image Caption Evaluation) (multimodal):** Evalúa la estructura semántica del contenido, comparando gráficos de escena generados con los de referencia.
7. **BERScore:** Evalúa la similitud semántica entre la salida generada y las referencias utilizando *embeddings* de BERT, lo que la hace robusta a variaciones léxicas y sinónimos.

Métricas para sistemas de preguntas y respuestas:

8. **SaCC:** Mide la exactitud estricta comparando respuestas generadas con referencias, útil en tareas que requieren respuestas específicas y exactas.
9. **LaCC:** Mide la precisión permitiendo variaciones en las respuestas generadas utilizando similitud semántica, como la de coseno entre *embeddings*.
10. **MRR (Mean Reciprocal Rank):** Evalúa la posición de la primera respuesta relevante en una lista de resultados ordenados.

Mediciones LLM-to-LLM:

11. **G-Eval:** *Framework* que utiliza LLM con técnicas de razonamiento en cadena (CoT) para evaluar salidas según criterios personalizados.
12. **Max Pseudo Entropy:** Mide la diversidad y la incertidumbre en las salidas generadas por un modelo, evaluando la distribución de probabilidades de las respuestas.

Modelos LUNA y Galileo Chainingpoll: *Frameworks* de medición de respuesta de LLM y arquitecturas RAG, como RAGAS, tecnologías de vanguardia en la detección de alucinaciones en modelos de lenguaje.



Al considerar las consecuencias del uso de modelos de lenguaje grande (LLM) en el ámbito legal, es crucial integrar hallazgos recientes que abordan tanto el razonamiento moral y legal de estos modelos como el impacto en la práctica jurídica. El uso de LLM en asesoría legal se debe regular cuidadosamente, lo que sugiere que estos modelos han de enfocarse en ayudar a los usuarios a formular preguntas y obtener información relevante, en lugar de emitir juicios legales definitivos. Este enfoque se deriva de la preocupación de que los LLM, aunque poderosos, aún no pueden reemplazar la interpretación legal humana a causa de la complejidad y la responsabilidad que conlleva el asesoramiento legal. Los expertos legales consultados en el estudio subrayan la necesidad de que los LLM operen dentro de un marco ético que evite la práctica no autorizada de la ley, mantenga la confidencialidad y asegure que los usuarios comprendan que la IA no puede reemplazar la asesoría legal profesional (Cheong et al., 2024).

Por otro lado, el estudio que investiga cómo los LLM, como GPT-4 y otros modelos actuales, se alinean con el razonamiento humano en temas morales y legales, revela que, aunque estos modelos muestran una correlación significativa con las respuestas humanas, existen diferencias sistemáticas que se deben abordar. GPT-4, en particular, demostró la mayor alineación, pero los LLM en general tienden a exagerar ciertos efectos presentes en los humanos, lo que sugiere una necesidad de precaución al considerar estos modelos como reemplazos para participantes humanos en investigaciones psicológicas o legales.

Estos dos estudios subrayan la importancia de un enfoque multidisciplinario en la implementación de LLM en el ámbito legal. Es evidente que los LLM ofrecen un potencial significativo para mejorar el acceso a la información legal y apoyar la toma de decisiones, sin embargo, su uso debe estar cuidadosamente enmarcado dentro de políticas y regulaciones que consideren no solo la precisión técnica, sino también las implicaciones éticas, la equidad y la transparencia. Las diferencias observadas en cómo estos modelos manejan el razonamiento moral y legal en comparación con los humanos subrayan la necesidad de un escrutinio continuo y una mejora constante en su diseño y aplicación. Además, estos hallazgos sugieren que los LLM, si no se abordan adecuadamente, podrían no solo replicar, sino también distorsionar ciertos aspectos del juicio humano, lo cual tendría consecuencias significativas en el ámbito jurídico.

En conclusión, la integración de LLM en el ámbito legal requiere una evaluación cuidadosa que combine conocimientos técnicos con consideraciones éticas y legales profundas. La colaboración entre expertos en IA, psicólogos y profesionales del derecho será fundamental para garantizar que el uso de LLM en contextos legales avance de manera responsable, alineada con los valores fundamentales de la justicia y la equidad.



Responsabilidad y rendición de cuentas

Establecer la responsabilidad y la rendición de cuentas es un desafío significativo en el ámbito de la inteligencia artificial (IA). Cuando un sistema de IA falla o causa daño, se debe determinar quién es responsable. Los marcos legales deben definir claramente la responsabilidad y asegurar que las entidades desarrolladoras y operadoras de IA puedan rendir cuentas por sus acciones. La responsabilidad legal en el ámbito de la IA es un tema multifacético y en constante evolución que abarca diversas áreas del derecho, como la protección de datos, la propiedad intelectual, la responsabilidad civil y la regulación específica de esta tecnología.

En cuanto a la *responsabilidad civil y penal*, uno de los aspectos más críticos es determinar quién es responsable si un sistema de IA causa daños a personas o propiedades. La responsabilidad puede recaer sobre el desarrollador del software, el proveedor del hardware o el usuario final, dependiendo de factores como el diseño del sistema, la previsibilidad de los daños y el nivel de control ejercido sobre la IA. Además, la negligencia en la supervisión, el desarrollo o la aplicación práctica de la IA puede dar lugar a responsabilidades legales, especialmente si no se tomaron las precauciones adecuadas para prevenir daños.

En el **área de protección de datos y privacidad**, la IA debe cumplir con regulaciones como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que impone estrictos requisitos sobre el procesamiento de datos personales. Los sistemas de IA deben adherirse a principios de minimización de datos, transparencia y obtención de consentimiento explícito. La capacidad de explicar las decisiones tomadas por la IA es crucial para garantizar que no se vulneren los derechos de los individuos, especialmente en situaciones sensibles como la contratación o la concesión de crédito.

Con respecto a la *propiedad intelectual*, la creación de obras por IA plantea desafíos legales sobre la titularidad de los derechos de autor y la posibilidad de patentar invenciones generadas mediante esta tecnología. Actualmente, las leyes tienden a reconocer los derechos a los creadores humanos, lo que deja un vacío legal en los casos donde la IA cumple un papel predominante en la creación.

En cuanto a la *regulación específica de la IA*, la Unión Europea está desarrollando un marco regulador que podría incluir la categorización de riesgos para diferentes aplicaciones de IA, desde aquellas de bajo riesgo, como los *chatbots*, hasta las de alto riesgo, como los sistemas de IA utilizados en medicina. Además, países como Estados Unidos y China están formulando sus propias normativas, que abarcan la seguridad, la ética y la transparencia en el uso de la IA.



En el ámbito de la **ética y las normas internacionales**, organizaciones como la UNESCO han elaborado directrices éticas que promueven prácticas responsables en el desarrollo y uso de la IA. Aunque estas directrices no son legalmente vinculantes, influyen significativamente en la legislación y las políticas corporativas. La responsabilidad algorítmica es un tema de debate creciente, sobre todo en cuanto a si las empresas deben ser responsables por los sesgos en sus algoritmos, que pueden afectar de manera desproporcionada a grupos vulnerables.

Los desafíos éticos y legales en torno a la IA son amplios y complejos, e involucran cuestiones como la transparencia algorítmica, las vulnerabilidades en ciberseguridad, el sesgo, la discriminación y la falta de mecanismos para impugnar decisiones automatizadas. Estos problemas plantean serias preocupaciones sobre cómo la IA puede afectar el bienestar humano y subrayan la necesidad de un enfoque más sólido para proteger los derechos humanos en la era digital (Díaz-Rodríguez et al., 2023).

Además, la creciente desconfianza hacia la IA, especialmente en sectores como los servicios financieros, evidencia la importancia de adoptar estrategias que gestionen los impactos sociales, económicos y éticos de esta tecnología. La responsabilidad digital corporativa emerge como una propuesta para promover una sociedad digital más equitativa, y enfatiza la necesidad de transparencia, ética y supervisión humana en el desarrollo e implementación de sistemas de IA (Elliott et al., 2021).

La creación de una IA confiable requiere un enfoque que integre legalidad, ética y robustez a lo largo de todo el ciclo de vida de los sistemas. Este enfoque holístico debe considerar tanto los aspectos técnicos como los sociales, y se sugiere la implementación de mecanismos regulatorios, como las “cajas de arena regulatorias”, para probar y validar los sistemas de IA de manera segura y responsable. En resumen, es fundamental abordar estos desafíos desde múltiples frentes para asegurar que la IA se desarrolle y utilice de manera que beneficie a la sociedad en su conjunto (Rodrigues, 2020).

No discriminación y equidad

La *no discriminación y equidad* en la IA es un aspecto fundamental por el potencial de sus sistemas para perpetuar o amplificar sesgos y desigualdades sociales existentes. Estos problemas surgen principalmente a causa de los datos utilizados para entrenar los modelos de IA y las decisiones algorítmicas que puedan reflejar prejuicios humanos. Es esencial garantizar que los sistemas de IA no discriminen por razones de raza, género, edad, religión, orientación sexual u otras características protegidas. Cuando los datos de entrenamiento reflejan desigualdades históricas, existe



un riesgo real de que la IA reproduzca esas desigualdades, lo que puede llevar a resultados discriminatorios en áreas como selección de personal, decisiones crediticias y justicia penal.

Para mitigar estos problemas, se están desarrollando marcos legales y éticos que obligan a las empresas y desarrolladores a poner en práctica medidas para detectar, corregir y mitigar sesgos en sus sistemas de IA. En la Unión Europea, por ejemplo, el Acta de IA propone requisitos para realizar evaluaciones de impacto sobre derechos fundamentales y asegurar la transparencia en los algoritmos. Esto es crucial para garantizar que las decisiones algorítmicas sean explicables y justificables, en aras de proteger a los grupos vulnerables.

Las prácticas de desarrollo ético son igualmente importantes, e incluyen la diversidad en los equipos de desarrollo de IA, lo que permite identificar y mitigar sesgos desde las etapas iniciales del desarrollo. Además, la auditoría continua de los sistemas de IA es esencial para mantener su equidad a lo largo del tiempo, especialmente en contextos dinámicos. Promover la equidad implica diseñar políticas y prácticas que aseguren un acceso igualitario a las tecnologías de IA, y así evitar que estas exacerben las desigualdades sociales o económicas.

La responsabilidad y la rendición de cuentas son fundamentales en la promoción de la no discriminación y la equidad en la IA. Las organizaciones deben ser transparentes respecto del funcionamiento de sus algoritmos, estar preparadas para rendir cuentas si sus sistemas causan daños discriminatorios, y establecer mecanismos claros para la reparación de daños y la rectificación de sesgos cuando se identifican. Este enfoque es esencial para construir sistemas de IA justos y beneficiosos para toda la sociedad.

Protección jurídica en Colombia frente a la Inteligencia Artificial: comparación con Europa y Estados Unidos

En Colombia, la regulación de la IA está en una fase de desarrollo emergente y fragmentado. Aunque el país ha iniciado pasos hacia la regulación de esta tecnología, aún no dispone de una legislación específica que aborde de manera integral los desafíos, riesgos y oportunidades únicos que plantea la IA.

La Ley 1581 de 2012, que regula la protección de datos personales, sigue siendo una de las principales normativas en Colombia. La importancia de esta ley radica en que la IA a menudo maneja grandes volúmenes de datos personales (González, 2020). Sin embargo, la Ley 1581 no aborda directamente las especificidades de la IA, como la transparencia algorítmica y la responsabilidad por los daños derivados de decisiones automatizadas (Serrano, 2021).



En 2021, el Gobierno colombiano lanzó la Política Nacional de Inteligencia Artificial, con el objetivo de promover el desarrollo y la adopción de la IA en el país (Mintic, 2021). Sin embargo, esta política aún no se ha materializado en un marco regulatorio detallado. Las iniciativas sectoriales, como las leyes relacionadas con la ciberseguridad y el comercio electrónico, están en discusión, pero no abordan de manera integral la IA (Wu, W. & Liu, S. 2023).

En contraste, la regulación de la IA en Europa está considerablemente más avanzada. En 2021, la Unión Europea propuso el Reglamento de Inteligencia Artificial, que implanta un marco legal basado en el riesgo. Este reglamento clasifica las aplicaciones de IA en categorías según el nivel de riesgo, establece requisitos específicos para cada categoría y exige a los sistemas de alto riesgo que sean explicables y auditables para promover la confianza pública y la rendición de cuentas (Comisión Europea, 2021; Mokander et al., 2021). En 2023, el reglamento fue revisado para incluir directrices más estrictas sobre la evaluación y certificación de los sistemas de IA, subrayando la importancia de la seguridad y la equidad (Parlamento Europeo, 2024).

Por otro lado, en Estados Unidos, la regulación de la IA sigue un enfoque fragmentado y sectorial. Las leyes y regulaciones aplicables a la IA varían según el sector, como lo ejemplifica la Ley de Privacidad del Consumidor de California (CCPA), que aborda la privacidad de datos, pero no específicamente con la utilización de la IA (Weaver, 2020). La Comisión Federal de Comercio (FTC) ha emitido directrices y alertas sobre prácticas desleales o engañosas en el uso de sistemas de IA, aunque aún no existe una legislación federal integral que regule todas las dimensiones de esta tecnología (DiResta, 2025).

Tendencias y proyecciones en la Inteligencia Artificial: perspectivas de Gartner y McKinsey

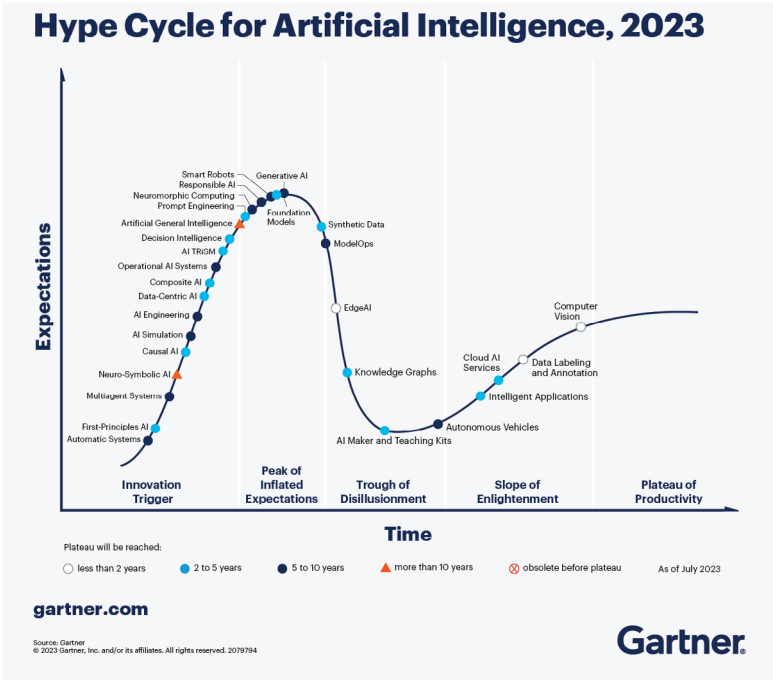
Son muchas las firmas consultoras, web académicas, ONG, tendencias y estudios de mercado, etc., que presentan estudios respecto al pasado, estado actual, y crecimiento y futuro de las diferentes tecnologías emergentes, entre las cuales se encuentra la inteligencia artificial. Algunas de estas firmas son las siguientes: Gartner Hype Cycle, McKinsey & Company, Forrester Research, Statista, International Data Corporation (IDC), World Economic Forum (WEF), Organización para la Cooperación y el Desarrollo Económico (OECD), ResearchGate y ArXiv.

Por ser Gartner Hype Cycle y McKinsey & Company las firmas más consultadas en el ámbito internacional para vislumbrar los avances de la IA, se muestra brevemente lo que estas firmas han comunicado al respecto.



Gartner Hype Cycle: se puede inferir de la gráfica de Gartner (Figura 1), que se proyecta una evolución significativa en el crecimiento de la IA impulsada por avances continuos en tecnologías como la IA generativa y la automatización. A medida que estas tecnologías alcanzan el “Ascenso hacia la madurez” en el *Hype Cycle*, se espera que la IA se integre de manera más profunda y efectiva en diversas industrias, mejore la eficiencia operativa y habilite nuevas capacidades. Sin embargo, el progreso vendrá acompañado de desafíos relacionados con la transparencia, la ética y la regulación, que se deberán abordar para garantizar una adopción responsable. Las expectativas infladas iniciales darán paso a una fase de desilusión, en la que la industria ajustará sus enfoques basados en resultados tangibles y realistas, para establecer finalmente una madurez que permita una integración sólida y segura de la IA en la vida cotidiana y en los procesos empresariales.

Figura 1. Gráfica de Tendencias de Gartner para 2022



Nota tomado de Gartner Hype Cycle (2023).

McKinsey & Company: comentaba que antes de 2023, la adopción de la IA había mostrado un crecimiento notable desde 2017, cuando solo el 20 % de las organizaciones la utilizaban en algún área de negocio. Para 2022, este porcentaje había aumentado aproximadamente al 50 %, aunque había alcanzado su punto máximo en 2019 con un 58 %. Durante este periodo, el número promedio de capacidades de IA



implementadas en las organizaciones se había incrementado de 1,9 a 3,8, y se destacaban como las aplicaciones más comunes la automatización robótica de procesos y la visión por computadora. Las inversiones en IA también se habían incrementado, y representaban más del 5 % de los presupuestos digitales de muchas empresas, con un enfoque predominante en la optimización de operaciones de servicio.

Desde 2023, la IA generativa (IAG) ha emergido como un área de crecimiento explosivo. Un tercio de las organizaciones encuestadas reportan el uso regular de IAG en al menos una función empresarial. Los líderes empresariales están adoptando estas herramientas de manera más decidida, y la IAG se ha convertido en una prioridad en las agendas de los consejos de administración. Sin embargo, la gestión de los riesgos asociados con la IAG, como la imprecisión, sigue siendo un desafío. Se prevé que para 2024, al menos un tercio de las empresas utilizará IA, y será el máquetin una de las industrias más activas en su adopción. La IAG continuará siendo un área clave de inversión, lo que refleja los avances significativos y la creciente importancia de la IA en el panorama empresarial.

Contexto actual y futuro de la inteligencia artificial en Colombia: iniciativas y perspectivas en 2024

Colombia enfrenta desafíos significativos en términos de protección jurídica frente a la IA, principalmente por la falta de una regulación específica y un enfoque integral. En comparación con Europa, que avanza hacia un marco regulatorio robusto, y con Estados Unidos, que mantiene un enfoque más fragmentado y sectorial, Colombia aún tiene un camino por recorrer para desarrollar una legislación que asegure una protección adecuada de derechos y promueva una adopción ética y segura de la IA (González, 2020; Parlamento Europeo, 2024; Serrano, 2021; Smith, 2021).

En 2024, Colombia está en una fase crucial de desarrollo en relación con la IA. El país se encuentra en un proceso de construcción de una política nacional que equilibre la promoción de la innovación con la protección de los derechos y el abordaje de los desafíos éticos. Este esfuerzo surge como una respuesta a la necesidad de establecer un marco normativo robusto y adaptado a las realidades locales, que posicione a Colombia como un actor relevante en el panorama global de la IA, y pueda utilizarla en los diferentes aspectos sociales, económicos, productivos, etc., a fin de lograr un crecimiento económico, pero con una regulación acorde con las implicaciones de su uso.

El contexto actual revela una creciente preocupación por los impactos de la IA en sectores clave como la economía, la seguridad y los derechos individuales. Según el Departamento Nacional de Planeación de Colombia (DNP, 2024), se han llevado



a cabo numerosas consultas y foros con actores clave para desarrollar una política de IA que promueva tanto el desarrollo tecnológico como una protección adecuada para los ciudadanos. Estos foros han abordado temas críticos como la transparencia en los algoritmos, la privacidad de los datos, la responsabilidad por errores de IA, y la promoción de la equidad y la no discriminación.

Estas iniciativas de consulta pública y académica son fundamentales para asegurar que la política de IA refleje una comprensión amplia de los desafíos y oportunidades que presenta esta tecnología. En comparación con la Unión Europea, En comparación con la Unión Europea, que ha avanzado significativamente con su Reglamento de Inteligencia Artificial (Comisión Europea, 2021), y con Estados Unidos, que mantiene un enfoque más fragmentado y sectorial (Mokander, Axente, Casolari, & Floridi, 2021), Colombia busca desarrollar un marco normativo adaptado a su contexto local y sus propias necesidades.

El enfoque colombiano en la creación de su política de IA destaca la importancia de una gobernanza participativa que incluya a diversos sectores de la sociedad. Este enfoque busca evitar problemas similares a los que enfrentan otros países que han aplicado marcos regulatorios menos inclusivos o flexibles (Martínez y Pérez, 2023). Al involucrar a actores de distintos ámbitos, Colombia pretende construir un entorno regulatorio que facilite la adopción de la IA mientras asegura su uso ético y responsable, lo que refleja un compromiso con la protección de derechos y la promoción de una tecnología que beneficie equitativamente a toda la sociedad.

Conclusiones

1. La convergencia de la inteligencia artificial y el derecho es un campo dinámico y en constante evolución. Los desarrolladores de IA deben trabajar en estrecha colaboración con expertos legales para asegurar que sus tecnologías sean tanto innovadoras como éticas y conformes a las leyes vigentes. La anticipación y mitigación de riesgos legales y éticos son fundamentales para el desarrollo sostenible y responsable de la IA.
2. En Colombia, la ausencia de una legislación específica para la IA representa un desafío significativo para garantizar la protección adecuada de los derechos de los ciudadanos y promover un uso ético de la tecnología. Aunque la Ley 1581 de 2012 y la reciente Ley de Protección de Datos Personales establecen importantes fundamentos en materia de privacidad, aún es necesario desarrollar un marco regulatorio integral que afronte las particularidades y riesgos asociados con la IA, como la transparencia algorítmica y la rendición de cuentas. Las iniciativas actuales, como la Política Nacional de Inteligencia Artificial, representan un



paso positivo, pero deben concretarse en una regulación detallada que cubra de manera efectiva estos aspectos críticos.

3. Colombia ha adoptado un enfoque inclusivo y participativo en la elaboración de la política nacional de IA para desarrollar un marco normativo que refleje las realidades locales y los intereses de todos los sectores de la sociedad. Al involucrar a investigadores, profesionales y el público en general, Colombia busca construir un entorno regulatorio que no solo facilite la adopción de la IA, sino que también garantice que su implementación sea ética y responsable. Este enfoque puede ayudar a evitar problemas —comunes en otros países— y asegurar que la política de IA sea relevante y efectiva en el contexto colombiano.
4. La Unión Europea ha tomado la delantera en la regulación de la IA con la propuesta del Reglamento de Inteligencia Artificial, que introduce un enfoque basado en el riesgo y requisitos estrictos para las aplicaciones de alto riesgo. Este marco avanzado busca promover la transparencia, la explicabilidad y la rendición de cuentas, y establecer un modelo que otros países podrían considerar al desarrollar sus propias regulaciones. Sin embargo, la implementación efectiva de este reglamento y la adaptación continua a los rápidos avances tecnológicos seguirán siendo desafíos clave para garantizar que la regulación cumpla con sus objetivos de protección y confianza pública.
5. En Estados Unidos, la regulación de la IA sigue un enfoque fragmentado y sectorial que puede limitar la cohesión y la protección integral de los derechos de los ciudadanos. Aunque las leyes, como la CCPA, y las directrices de la FTC tratan ciertos aspectos de la IA, la falta de una legislación federal unificada y de un enfoque integral puede resultar en vacíos en la protección y en la capacidad de adaptación a los rápidos cambios en la tecnología. Este enfoque permite flexibilidad e innovación, pero también plantea riesgos de inconsistencias y brechas en la protección, lo que destaca la necesidad de una regulación más coherente y consolidada en el ámbito de la IA.
6. La implementación del Reglamento General de Protección de Datos (RGPD) en la Unión Europea marcó un cambio de paradigma en la gestión de datos personales, al introducir un enfoque centrado en la responsabilidad proactiva de quienes manejan la información y fortalecer derechos como el acceso, la rectificación y la privacidad desde el diseño, lo cual ha sido clave para afrontar los desafíos planteados por las tecnologías emergentes y la globalización de la información. No obstante, la implementación del Reglamento parece no ser concomitante con la arquitectura de los diferentes desarrollos que se han llevado a cabo en el marco del avance de las tecnologías de IA. La IA necesita un volumen de gestión de datos que es incompatible con las determinaciones de los diferentes reglamentos de datos.



Referencias

- Agencia de Derechos Fundamentales de la Unión Europea (FRA). (2019). *Manual de legislación Europea en materia de protección de datos*. Luxemburgo. fra.europa.eu. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf
- Cheong, I., Xia, K., Feng, K. J. K., Chen, Q. Z., & Zhang, A. X. (2024). (A) I Am Not a Lawyer, But...: Engaging Legal Experts towards Responsible LLM Policies for Legal Advice. *FACCT 2024: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, 2454-2469. <https://doi.org/10.1145/3630106.3659048>
- Colombia Digital, y Certicámara. (2014). Virtualización y seguridad de la información. Casos de uso en la experiencia de Certicámara S. A. https://web.certicamara.com/sites/default/files/2024-01/virtualizacion_y_seguridad_de_la_informacion.pdf
- Comisión Europea. (30 de marzo, 2000). “La Comisión aprueba el acuerdo de ‘puerto seguro’”. CORDIS - Resultados de investigaciones de la UE. *Cordis.europa.eu*. <https://cordis.europa.eu/article/id/14577-commission-endorses-safe-harbour-agreement/es>.
- Comisión Europea. (2017). What rules apply if my organisation transfers data outside the EU? https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_es
- Comisión Europea. (2021). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión. Documento 52021PC0206. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0206>
- Congreso de la República de Colombia. Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Corte Constitucional de Colombia. (1997). *Sentencia T-552/97*. <https://www.corteconstitucional.gov.co/relatoria/1997/t-552-97.htm>
- Davara Fernández, E. (2017). El reglamento Europeo de Protección de datos. En V. Cazorro Barahona (dir.), A. Fayos Gardó y M. C. Lorente López (coords.), *Derecho Digital: perspectiva interdisciplinar* (pp. 175-201). J. M. Bosch.
- Departamento Nacional de Planeación (DNP). (2024). *Nace una nueva política Nacional de Inteligencia Artificial (IA)*. https://www.dnp.gov.co/Prensa_/Noticias/Paginas/nace-una-nueva-politica-nacional-de-inteligencia-artificial-ia.aspx
- Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., y Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, 99, 101896. <https://doi.org/10.1016/j.inffus.2023.101896>



- DiResta, A. E. (2025, 11 de junio). *FTC evaluando reclamos engañosos de inteligencia artificial*. Holland & Knight Alert.
- Duaso Calés, R. (2016). Los principios de protección de datos desde el diseño y protección de datos por defecto. En J. Piñar Mañas (dir.), M. Álvarez Caro y M. Recio Gayo (coords.), *Reglamento General de Protección de datos*. (pp. 295-320). REUS.
- Elliott, K., Price, R., Shaw, P., Spiliotopoulos, T., Ng, M., Coopamootoo, K., y Van Moorsel, A. (2021). Towards an equitable digital society: artificial intelligence (AI) and corporate digital responsibility (CDR). *Society*, 58(3), 179-188. <https://link.springer.com/article/10.1007/s12115-021-00594-8>
- Escobar Peñalver, A. F., y Pajarito Contreras, M. P. (2014). Alcance e implicaciones del derecho al habeas data en el comercio colombiano [Trabajo de grado]. Pontificia Universidad Javeriana. [http://repository.javeriana.edu.co/bitstream/10554/14895/1/EscobarPenalverAndresFelipe 2014.pdf](http://repository.javeriana.edu.co/bitstream/10554/14895/1/EscobarPenalverAndresFelipe%202014.pdf)
- Fazlioglu, M. (Julio de 2017). Decrypting Information Sensitivity: Risk, Privacy, and Data Protection Law in the United States and the European Union. Unites Estates: Indiana University. Retrieved 11 de Octubre de 2021. <https://www.proquest.com/docview/1951780375/6E054AA900054E8APQ/16?accountid=14744#>
- Floridi, L. (2019). *La ética de la inteligencia artificial*. Oxford University Press.
- Fondo Nacional de Garantías (FNG). (2014). *Manual Habeas Data* <https://www.fng.gov.co/ES/Documentos%20%20Proteccion%20de%20Datos%20Personales/Manual%20Habeas%20Data.pdf>
- Hernández López, J. M. (2018). *Reglamento General de Protección de datos*. Tirant lo Blanch.
- López A., J. F. (2015). Data Protection Package y Parlamento Europeo. En A. Rallo Lombarte y R. Garcia Mahamut (eds.), *Hacia un nuevo derecho europeo de proteccion de datos* (pp. 29-84). Tirant lo Blanch.
- López A., J. F. (2019). La protección de datos en la UE: El punto de vista del Parlamento Europeo. En R. García Mahamut y B. Tomás Mallén (eds.), *El Reglamento general de protección de datos* (pp. 31-48). Tirant lo Blanch.
- Ministerio de Tecnologías de la Información y Comunicaciones de Colombia (MinTic). (2021). *Política Nacional de Inteligencia Artificial*.
- Naik, N., Hameed, B. M. Z., Shetty, D. K., Swain, D., Shah, M., Paul, R., Aggarwal, K., Brahim, S., Patil, V., Smriti, K., Shetty, S., Rai, B. P., Chlost, P., & Somani, B. K. (2022). Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility? *Frontiers in Surgery*, 9(March), 1-6. <https://doi.org/10.3389/fsurg.2022.862322>
- Noyb. (16 de julio, 2020). Data Transfers. *Noyb.eu*. <https://noyb.eu/es/proyecto/transferencias%20de%20eeuu-us>
- Mokander, J., Axente, M., Casolari, F., & Floridi, L. (2021). *Conformity assessments and postmarket monitoring: A guide to the role of auditing in the proposed European AI Regulation* [Preprint]. arXiv. <https://doi.org/10.48550/arXiv.2111.05071>



- Ortega Giménez, A. (mayo de 2014). El acuerdo de puerto seguro. *Revista Telos*, (97). <https://telos.fundaciontelefonica.com/archivo/numero097/el-acuerdo-de-puerto-seguro/>
- Parlamento Europeo. (2024). *Reglamento de Inteligencia Artificial*. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf
- Piñar Mañas, J. (2016). Transferencias de datos personales a terceros países u organizaciones internacionales. En J. Piñar Mañas (dir.), M. Álvarez Caro y M. Recio Gayo (coords.), *Reglamento General de Protección de Datos* (427-460). Madrid: REUS.
- Prosser, W. (1960). Privacy. *California Law Review*, 48(3), 383-423. <https://doi.org/10.2307/3478805>
- Rebollo Delgado, L., y Saltor, C. (2013). *El derecho a la protección de datos en España y Argentina. Orígenes y regulación vigente*. Madrid: Dykinson.
- Rebollo Delgado, L., y Serrano Perez, M. (2008). *Introducción a la protección de datos*. Madrid: Dykinson.
- Rebollo Delgado, L. (2018). *Protección de datos en Europa. Origen, evolución y regulación actual*. Madrid: Dykinson.
- Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, 4, 100005. <https://doi.org/10.1016/j.jrt.2020.100005>
- Unión Europea. (12 de julio de 2016). Decisión de Ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. *Diario Oficial de la Unión Europea*. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016D1250>
- Ustarán, E., y García, P. (2019). Transferencias Internacionales de datos. En R. García Mahamut y B. Tomás Mallen, *El reglamento general de protección de datos*. (pp. 459-491). Valencia: Tirant Lo Blanch.
- Weaver, J. F. (2020). *Everything is not Terminator: AI issues raised by the California Consumer Privacy Act*. *RAIL: The Journal of Robotics, Artificial Intelligence & Law*, 3(1), 1–7
- Wu, W., & Liu, S. (2023). *A comprehensive review and systematic analysis of artificial intelligence regulation policies* [Preprint]. arXiv. <https://arxiv.org/abs/2307.12218>



Capítulo 6

Algor-ética: un concepto en construcción necesario para materializar la tutela judicial efectiva en una administración de justicia asistida por la inteligencia artificial⁴⁵

Débora Guerra Moreno

Darwin Clavijo Cáceres

Introducción

Distintos documentos académicos coinciden en afirmar que el primer antecedente sobre la existencia de un algoritmo computacional data del año 1842, gracias al trabajo de Ada Lovelace, quien es considerada como la primera programadora de la historia. A esta científica se le atribuye la idea de producir una serie de instrucciones codificadas que podían ser ejecutadas repetidamente o en “bucle” por una máquina, en este caso, una máquina analítica creada por Charles Babbage.

Si bien esta máquina no logró terminarse y, en consecuencia, los algoritmos ideados por Ada Lovelace no fueron aplicados para su operación, el trabajo de esta investigadora marcó un hito para que en las décadas posteriores otros investigadores realizaran avances importantes en el ámbito de la programación computacional que desembocaron en el surgimiento de la denominada inteligencia artificial (IA) en el siglo siguiente. Este concepto fue utilizado por primera vez por John McCarthy en una conferencia dictada en Dartmouth en 1956, quien lo concibió como un conjunto de algoritmos que permitían operar máquinas inteligentes que lograban replicar procesos que anteriormente se concebían como propios de la inteligencia humana.

En ese momento de la historia, las funciones en que intervenía la inteligencia artificial se podían considerar como básicas, en comparación con la inmensa gama de utilidades que ofrece en la actualidad, para facilitar las distintas labores que

⁴⁵ Artículo inédito. El presente artículo de investigación e innovación hace parte del proyecto de investigación “El sistema procesal en Colombia: integración de disposiciones procesales desde los ámbitos especiales de aplicación al ámbito residual. Crisis del carácter dinámico del derecho sustancial y procesal”, vinculado al Grupo de Investigación en Derecho Público de la Universidad Libre Seccional Cúcuta, Colombia.



desarrollan los seres humanos. En efecto, todo un siglo de avances tecnológicos ha servido para que en el presente se pueda desarrollar cualquier tipo de algoritmo con la capacidad de incorporar razonamientos y operaciones en las máquinas, retener información, aprender de los datos recolectados y utilizarlos en la toma de decisiones, de manera similar a como lo haría un ser humano.

En concreto, se puede destacar que, en la actualidad, gracias a la IA, es posible contar, en las computadoras o *smartphones*, con softwares que cumplen, entre otras, las siguientes funciones: reconocimiento de voz y procesamiento de lenguaje natural; generación de imágenes; asistencia de voz como Siri o Alexa; producción de textos desde cero, como si fueran redactados por una persona, o el suministro de respuestas a una pregunta determinada sobre cualquier área del conocimiento. Todas estas utilidades han logrado optimizar y efectivizar el trabajo humano en distintos ámbitos, al reducir los tiempos requeridos para cumplir con una determinada tarea y realizarla con una calidad mejorada.

La labor de administrar justicia no ha sido ajena a la inmersión de las funcionalidades que ofrece la IA, pues se ha hecho común que jueces y magistrados recurran a aplicaciones como *ChatGPT* para auxiliar la redacción de providencias y el análisis de los fundamentos jurídicos que servirán de base para estas, aspecto sobre el cual ya se pronunció la Corte Constitucional mediante la Sentencia T-323 de 2024. El Consejo Superior de la Judicatura ha manifestado en diferentes escenarios su compromiso con la expedición de lineamientos que regulen el uso de la inteligencia artificial en la Rama Judicial, que tienen como objetivo garantizar que la tecnología aporte valor a la administración de justicia, sin sustituir el juicio crítico del operador judicial, sino como un recurso de apoyo en la toma de decisiones, de ello es ejemplo el Acuerdo de 16 de diciembre de 2024 mediante el cual se adoptan lineamientos para el uso y aprovechamiento respetuoso, responsable, seguro y ético de la inteligencia artificial en la Rama Judicial.

Ahora bien, la aplicación de la IA en el ámbito del derecho representa interesantes ventajas: logra aligerar el trabajo de los operadores jurídicos, acelera las tareas asignadas y aumenta la exactitud de los resultados. Sin embargo, genera serias dudas con respecto a la “deshumanización” de la labor que desempeña el jurista por dos factores principales: el alejamiento de valoraciones de equidad en cada caso concreto, y la eventual multiplicación de sesgos considerablemente discutibles (Bujosa, 2022)

En efecto, con la introducción de la IA en el proceso judicial, se pueden generar importantes dilemas éticos en la solución de los litigios. Recurrir a una plataforma de IA para resolver un problema jurídico planteado dentro de un caso determinado, podría aumentar la expectativa de objetividad e imparcialidad en el respectivo fallo. Sin embargo, debe advertirse que los datos que procesan estos sistemas, en últi-



mas, son producto del pensamiento humano, previamente procesado en una base de datos; del mismo modo, los distintos algoritmos son diseñados también por seres humanos, por lo que, de acuerdo con Kelleher y Tierney (2018), los datos recogidos por la IA “siempre son parciales y sesgados” y los algoritmos que operan a partir de dicha información no funcionan de forma “objetiva”.

Dicho esto, es claro que la aplicación de IA en los procesos judiciales conlleva unas implicaciones éticas serias, máxime si se considera que los algoritmos utilizados como mecanismo para la producción de la sentencia provienen de empresas privadas, las cuales pueden terminar imponiendo sus ideologías o preferencias en la providencia por medio de la información que sistematizan sus algoritmos. Como este, surgen otros dilemas en la práctica judicial, tanto en las distintas etapas procesales como en la producción de la misma sentencia, que, en últimas, pueden afectar el derecho fundamental a la tutela judicial efectiva de los usuarios de la administración de justicia, que contiene en sus componentes esenciales el respeto por el debido proceso y la garantía de una sentencia motivada, razonable, congruente y fundada en derecho. Analizar de qué manera la aplicación de la IA en el proceso judicial puede afectar estos componentes, constituye el objetivo central del presente documento, para lo cual, de paso, se aportan algunos fundamentos éticos como solución a tal problemática.

La aplicación de la inteligencia artificial en el proceso judicial y su impacto en el derecho fundamental a la tutela judicial efectiva

La posibilidad de acudir ante un tercero investido de funciones jurisdiccionales para el reconocimiento de los derechos establecidos en las normas jurídicas se configura como uno de los elementos trascendentales para la convivencia pacífica entre los miembros de la sociedad, para el mantenimiento del orden público, y para lograr los fines del Estado. En tal sentido, Hannah Arendt afirmaba que

el acceso a la justicia es el derecho de toda persona a tener derechos. Si alguien es titular de un derecho, pero carece de la posibilidad de reclamarlo ante una autoridad imparcial e independiente, en realidad carece del derecho que le ha sido teóricamente reconocido. (La Rota *et al.*, 2014, p. 13)

La Corte Constitucional de Colombia resalta la importancia del acceso a la administración de justicia como una necesidad esencial para los individuos. Sin este acceso, tanto las personas como la sociedad no podrían desarrollarse adecuadamente, ya que carecerían de una herramienta fundamental para garantizar la convivencia armoniosa: la correcta y adecuada aplicación de las normas que rigen



la vida en sociedad. La Corte advierte que, si no se garantiza este derecho, se correría el riesgo de que los intereses particulares prevalezcan sobre los generales, lo que iría en contra de los principios básicos del modelo jurídico y político establecido por la Constitución de 1991. Por lo tanto, el acceso a la justicia es reconocido como un derecho fundamental que goza de una protección especial por parte del Estado, y su respeto es esencial para el equilibrio y la armonía social (Corte Constitucional, Sentencia T-476 de 1996).

Así, en el marco de un Estado social de derecho, como se constituyó Colombia en su Constitución, el acceso a la administración de justicia se erige como un elemento indispensable para materializar los derechos, ya que es la instancia en donde las personas pueden ventilar sus controversias con la finalidad de que un tercero imparcial proteja y haga efectivos sus derechos. Sin embargo, la simple posibilidad de acudir ante un operador judicial no es suficiente para lograr la efectividad de los derechos consagrados en la Carta Política, pues es necesario que el trámite que se surta ante dicha autoridad esté acorde con las exigencias del debido proceso, y la decisión que ponga fin a la reclamación debe resolver de fondo el asunto planteado y estar suficientemente motivada, razonable, y con fundamentos jurídicos.

En ese sentido, el acceso a la administración de justicia ha evolucionado en un concepto más completo: el de la tutela judicial efectiva. Sobre esta última, la misma Corte Constitucional ha precisado que se trata de un derecho fundamental reconocido a todas las personas que residen en Colombia, consistente en la posibilidad de acudir ante los jueces de la República para solicitar la protección o el restablecimiento de sus derechos, con respeto al debido proceso y a las garantías sustanciales reconocidas por el ordenamiento jurídico (Sentencia C-086, 2016).

En el ámbito doctrinal se han aportado elementos esenciales que componen este derecho fundamental, verbigracia, Ramírez Carvajal aporta los siguientes: “un acceso real del ciudadano al juez, un proceso eficiente en tiempos y utilización de recursos, y una decisión eficaz” (Ramírez, 2021. p. 68).

En similar sentido, la jurisprudencia colombiana ha indicado que la tutela judicial efectiva se materializa, principalmente, en tres elementos: la posibilidad de acceder ante la justicia; el derecho a obtener una sentencia motivada y fundada en derecho que resuelva de fondo el problema jurídico planteado, y el derecho a que tal fallo sea cumplido efectivamente (Consejo de Estado, 2012).

Estos elementos esenciales identificados por la doctrina y la jurisprudencia nacionales han encontrado en la práctica serios impedimentos para ser materializados en los distintos procesos adelantados ante la administración de justicia. Si bien la tutela judicial efectiva se ha categorizado como un derecho fundamental que garantiza a las personas la posibilidad de acudir a una instancia judicial imparcial y obtener



una decisión motivada y fundada en derecho, en la práctica, la materialización de este derecho enfrenta múltiples obstáculos en Latinoamérica y, específicamente, en Colombia. Estos obstáculos incluyen, entre otros factores, la mora judicial, la falta de recursos, la corrupción y la insuficiencia de infraestructura judicial.

Uno de los mayores impedimentos para la tutela judicial efectiva en Latinoamérica es la mora judicial. En este sentido, la Corte Constitucional ha señalado que “el desconocimiento del plazo razonable viola la garantía de acceso oportuno a la administración de justicia” (Sentencia T-099 de 2021). En Colombia los tribunales están saturados por la gran cantidad de casos acumulados y la insuficiencia de jueces y personal judicial. Esto se traduce en largos tiempos de espera para obtener una resolución judicial. Según un informe del Consejo Superior de la Judicatura (2019), los procesos judiciales en el país pueden tardar varios años en resolverse, lo que genera desconfianza en el sistema judicial y viola el derecho a un juicio rápido y efectivo. La mora judicial afecta especialmente a los sectores más vulnerables de la sociedad, que dependen de la justicia para la protección de sus derechos fundamentales. En este sentido, la mora judicial en Colombia impide la garantía de los derechos a la igualdad y a la justicia, ya que son los ciudadanos de menores recursos quienes más sufren las consecuencias de la demora en la resolución de sus conflictos (Defensoría del Pueblo de Colombia, 2019).

En muchos países latinoamericanos, el acceso a la justicia está condicionado por factores socioeconómicos. La falta de recursos económicos y la carencia de asesoría legal gratuita limitan la posibilidad de que las personas más vulnerables puedan acudir a los tribunales para defender sus derechos. En Colombia, aunque existen mecanismos como la acción de tutela para proteger los derechos fundamentales de forma expedita, la desigualdad en el acceso a la justicia sigue siendo un problema. La Comisión Económica para América Latina y el Caribe (CEPAL) ha señalado que en Latinoamérica existe una relación directa entre la pobreza y la falta de acceso a la justicia. La población de bajos ingresos enfrenta barreras económicas, geográficas y culturales para acceder al sistema judicial (Negro, 2010). Esta realidad es evidente en las zonas rurales y en las comunidades indígenas de Colombia, en las que la falta de infraestructura judicial y la ausencia de jueces agravan la situación de exclusión jurídica (Fedesarrollo. 2019).

Otro factor que obstaculiza la tutela judicial efectiva es la corrupción. En muchos países de la región, los sistemas judiciales están permeados por prácticas corruptas que van desde el soborno hasta la injerencia política en la administración de justicia. En Colombia, la corrupción judicial ha sido un problema recurrente, lo que ha generado desconfianza de los ciudadanos en el sistema judicial y ha afectado gravemente el acceso a una justicia imparcial. Transparencia por Colombia (2024) afirma que “el sector Defensa y Seguridad se destaca como el más impactado



por la corrupción, seguido por los sectores judicial, educación, vivienda y salud”. La corrupción en el poder judicial se manifiesta en prácticas como el tráfico de influencias y la manipulación de decisiones judiciales, lo que vulnera el derecho a la tutela judicial efectiva. La falta de independencia judicial también afecta la capacidad de los jueces para tomar decisiones justas y equitativas, libres de presiones políticas o económicas.

Otra limitación para la tutela judicial efectiva en Colombia y otros países latinoamericanos es la insuficiencia de infraestructura judicial. Muchas regiones carecen de tribunales, jueces y personal capacitado, especialmente en áreas rurales y zonas alejadas de los centros urbanos. La falta de recursos materiales y humanos dificulta la resolución eficiente de los casos y contribuye a la saturación del sistema judicial. El estado actual del sistema judicial colombiano muestra que la eficiencia y capacidad de respuesta dependen en buena medida de la inversión en infraestructura, tecnología y capacitación del personal judicial. El Informe al Congreso del Plan Decenal de Justicia (Ministerio de Justicia, 2022) resalta mejoras en la cobertura territorial y tiempos de atención gracias a recientes inversiones. Asimismo, un análisis del BID subraya que las tecnologías digitales sólo alcanzan su potencial cuando van acompañadas por la formación adecuada del personal judicial (Cordella y Contini. 2020)

En Latinoamérica, la percepción de injusticia y la desconfianza en las instituciones judiciales constituyen importantes barreras para la tutela judicial efectiva. La desconfianza en el sistema judicial puede estar relacionada con experiencias previas de corrupción, discriminación o ineficacia en la administración de justicia. En Colombia, esta desconfianza se ha incrementado por la falta de transparencia y la percepción de parcialidad en la toma de decisiones judiciales (Fedesarrollo, 2019). Según la Corporación Excelencia en la Justicia (CEJ, 2020), el 59,1 % de las personas consideran que el nivel de corrupción en la Rama Judicial es alto o muy alto. Además, existen barreras culturales que limitan el acceso a la justicia, especialmente para comunidades indígenas y grupos minoritarios. Según el mismo estudio, el 66,7 % de las personas encuestadas consideran que en Colombia NO se protegen y garantizan los derechos de las minorías (étnicas y sociales) (CEJ, 2020). En muchos casos, las prácticas legales y los procedimientos judiciales no se adaptan a las realidades y necesidades de estas comunidades, lo que dificulta su participación efectiva en los procesos judiciales y el reconocimiento de sus derechos. Este desajuste entre el sistema legal y las realidades socioculturales de las poblaciones marginadas refuerza la exclusión y limita la eficacia de la tutela judicial (Defensoría del Pueblo de Colombia, 2018).

Para superar los obstáculos e impedimentos a la tutela judicial efectiva, los países latinoamericanos, incluido Colombia, han impulsado diversas reformas judiciales, sin que se hayan logrado mayores cambios, pues los problemas asociados



a la deficiente prestación del servicio de justicia se mantienen. Por enunciar un ejemplo: “En 2019 Colombia tenía 11,6 jueces por cada 100.000 habitantes, sin embargo, el estándar fijado por la OCDE es de 65 jueces por cada 100.000 habitantes” (CEJ, 2020, p. 3). Estas reformas han buscado modernizar el sistema judicial, mejorar la formación de jueces y promover la transparencia.

La implementación de las reformas judiciales en Colombia ha sido parcial e insuficiente, debido a la complejidad de los problemas estructurales del sistema. Además, la falta de coordinación interinstitucional y la ausencia de una política integral de justicia han dificultado el avance hacia un sistema más eficiente y accesible (DNP y Ministerio de Justicia, 2017).

En este contexto, la IA se presenta como una herramienta potencialmente transformadora que puede contribuir a superar algunas de estas barreras y mejorar el acceso a la justicia. Por ejemplo, con relación a la mora judicial, la IA puede contribuir de forma clara a reducir esta carga, mediante la automatización de tareas repetitivas y administrativas, lo que permitiría a los jueces y abogados concentrarse en los aspectos más complejos de los casos. Estonia ha sido uno de los países pioneros en explorar el uso de inteligencia artificial en la administración de justicia. En 2019, su Ministerio de Justicia anunció un proyecto piloto para desarrollar un sistema de IA orientado a resolver disputas de menor cuantía, como reclamaciones contractuales simples. El sistema, aún en fase experimental, buscaba que un algoritmo analizara la información presentada por las partes y propusiera una decisión, que podría ser apelada ante un juez humano. Aunque no ha sido plenamente implementado, este experimento ilustra el potencial de la tecnología como herramienta de apoyo en casos de baja complejidad (Niiler, 2019). Además, el uso de la IA ha demostrado ser eficiente en términos de costos, ya que los procesos judiciales automatizados pueden ser mucho más rápidos y menos costosos que los tradicionales (Carranza *et al.*, 2023).

Este enfoque ha contribuido no solo a reducir los tiempos de resolución de casos menores, sino también a generar mayor confianza en el sistema judicial, al hacer que los procesos sean más rápidos y accesibles para los ciudadanos. Herramientas de IA como “Ross” y “CaseCruncher” han demostrado ser eficaces en la revisión y análisis de grandes volúmenes de datos legales en un tiempo mucho menor que el requerido por un ser humano. Al automatizar estas tareas, los tribunales pueden agilizar los procesos judiciales y reducir los tiempos de espera, y así contribuyen a una justicia más eficiente y oportuna.

En Argentina, la Fiscalía de la Ciudad Autónoma de Buenos Aires lanzó, desde 2017, PROMETEA, un sistema basado en IA para generar dictámenes judiciales de manera automática. Gracias a esta herramienta, la Fiscalía logró mejorar notablemente la eficiencia de sus procedimientos. Por ejemplo, el tiempo requerido



para resolver un pliego de contrataciones se redujo drásticamente, al pasar de 90 minutos a tan solo un minuto, lo que representa un 99 % de disminución. En el caso de los procesos de requerimiento a juicio, el tiempo se redujo de 167 días a 38, un 77 % menos. Asimismo, para los amparos habitacionales que implican citación de terceros, el tiempo bajó de 190 a 42 días, es decir, un 78 % menos. Esta optimización permitió que los empleados y funcionarios, que anteriormente se dedicaban a estas tareas automatizadas, pudieran enfocarse en casos más complejos que demandan un análisis más exhaustivo, lo que ha contribuido a mejorar la calidad de las decisiones en estos asuntos (Estévez, Fillottrani y Linares, 2020).

Se mencionó antes que otro de los obstáculos que impiden o dificultan el acceso a la justicia es la falta de acceso a asesoría legal, especialmente para las personas de bajos ingresos. El uso de la IA puede contribuir a mejorar la asistencia jurídica mediante el desarrollo de chatbots legales y sistemas de IA que brinden asesoramiento básico de manera rápida, eficiente e incluso gratuita o a bajo costo, para acercar a los ciudadanos a información sobre sus derechos y orientarlos sobre los pasos a seguir para presentar una demanda o defenderse en un proceso judicial.

En Colombia, el sistema PretorIA es referente obligado. Se trata de un sistema de IA diseñado para optimizar el proceso de selección de tutelas en la Corte Constitucional. La Corte recibe para su posible revisión todas las tutelas que se presentan en el país, un procedimiento que implica un esfuerzo considerable para los funcionarios encargados de seleccionar los casos que serán analizados y sobre los cuales se emitirá una sentencia.

Para comprender la magnitud de esta tarea, basta considerar que en 2019 llegaron a la Corte más de 620.000 tutelas, lo que equivale a casi 1.700 tutelas diarias. La herramienta no pretende sustituir el trabajo humano, sino facilitarlo. PretorIA realiza un análisis preliminar de las sentencias de tutela, y entrega a los encargados de la selección información más estructurada y detallada para identificar con mayor facilidad cuáles casos se deben seleccionar para su revisión. Este sistema opera a través de cuatro funciones principales:

1. **Clasificación de sentencias:** la función principal de PretorIA es clasificar automáticamente las sentencias de tutela emitidas por los jueces de instancia, organizándolas según las categorías establecidas por la Corte Constitucional. Esto permite a los funcionarios filtrar y localizar la información más relevante para el proceso de selección.
2. **Búsqueda en expedientes:** con la clasificación ya realizada, buscar en los expedientes la información de interés se torna más eficiente, y esto agiliza el proceso de selección.



3. **Resúmenes no narrativos:** PretorIA genera resúmenes no narrativos sobre las categorías detectadas en las sentencias, lo que facilita la comprensión y evaluación de los casos.
4. **Generación de información estadística:** el sistema también ofrece información estadística sobre el uso de la tutela en Colombia, lo que proporciona a la Corte datos valiosos para entender las tendencias y patrones en la presentación de tutelas a nivel nacional.

El principal aporte de PretorIA está en su capacidad para descongestionar los despachos judiciales, al agilizar y simplificar la selección de tutelas. La automatización del análisis preliminar de las sentencias contribuye a un proceso de selección más eficiente, reduce significativamente la carga de trabajo manual, lo cual permite que los funcionarios se concentren en los casos más relevantes y urgentes, lo que, a su vez, resulta en una administración de justicia más efectiva que beneficia tanto a la Corte como a los ciudadanos que buscan la protección de sus derechos.

Son muchos los aportes que ofrece la IA para mejorar el acceso a la justicia y asegurar la tutela judicial efectiva para muchas personas. Sin embargo, no se pretende enunciar con exhaustividad cada una de esas contribuciones. Ese trabajo ya lo han llevado a cabo diversos autores y expertos en la materia. Nuestro objetivo, en cambio, se centra en explorar las implicaciones éticas de la IA en el ámbito judicial, lo que denominamos *algor-ética*. Nos interesa analizar cómo se pueden diseñar y aplicar sistemas de IA que respeten los derechos fundamentales, eviten la discriminación y se utilicen de manera justa y responsable en los procesos judiciales. Es claro que la IA ya no es una ficción, con los avances tecnológicos, la incorporación de IA en la aplicación y el desarrollo del derecho y la justicia se hará necesaria, pero se deben mantener la integridad y los valores fundamentales de nuestros sistemas. La IA no va a reemplazar la labor humana, hoy por hoy constituye una herramienta valiosa que, con una adecuada y responsable reglamentación y en manos de profesionales comprometidos, puede llevar a la justicia a un nivel superior de confianza si quienes deben tomar la decisión judicial la aplican con los criterios de razonabilidad, celeridad, ética y transparencia.

Un tema urgente en el debate sobre la aplicación de la IA en el proceso judicial es la preocupación sobre si los sistemas de IA podrían reemplazar al juez humano. La justicia no es solo una cuestión de aplicar normas, sino también de interpretar y valorar circunstancias específicas de cada caso. Los jueces, en su labor, aplican principios jurídicos, pero también toman en cuenta valores éticos y sociales que son fundamentales para administrar justicia (Bench-Capon, 2017).

Los sistemas de IA, a pesar de sus capacidades avanzadas, carecen de la conciencia y la empatía humanas. Como señala Pasquale (2024), la toma de decisiones



judiciales conlleva la aplicación de valores humanos que las máquinas no pueden replicar. Por lo tanto, aunque la IA puede ser una herramienta poderosa para asistir a los jueces en su trabajo, no debe sustituir la función del juez humano. La decisión judicial requiere una evaluación compleja de los hechos, el derecho y las circunstancias particulares, lo cual no puede ser completamente automatizado sin riesgo de deshumanizar la justicia.

La evolución del concepto de *algor-ética* y su necesidad para fortalecer la función jurisdiccional

La IA, en su autoorganización compleja, crea propiedades emergentes que pueden tener efectos incontrolados y significativos en la sociedad, en los individuos y en el medio ambiente. Este fenómeno ha sido ampliamente discutido por autores como Luciano Floridi, quien señala que los sistemas de IA no son meramente herramientas neutrales, sino artefactos tecnológicos con moralidad incorporada que pueden influir en las dinámicas de poder y autoridad (Floridi, 2019). La IA y las tecnologías relacionadas, como el big data, están reconfigurando la democracia y la organización social, y plantean un nuevo ecosistema con el potencial de transformar nuestras vidas, derechos y libertades fundamentales.

La interacción entre los seres humanos y la IA, así como con otras tecnologías convergentes, está acelerando la transformación de nuestra sociedad en entornos sociotécnicos. En estos espacios, las fronteras entre las personas y la tecnología se vuelven cada vez más borrosas, lo que lleva a una especie de simbiosis en la que la inteligencia humana y la artificial (*Human-Machine-Interaction*) trabajan en conjunto. En este contexto, la IA puede ser vista como una forma de inteligencia colectiva y social que integra sistemas inteligentes compuestos por múltiples agentes (Ausín, 2021). Por esta razón, sería más acertado hablar de “inteligencias artificiales” en plural, para reflejar la diversidad y complejidad de estos sistemas.

Funtowicz y Ravetz (2000) describen este entorno como una “ciencia post-normal” caracterizada por la incertidumbre sobre los hechos, la disputa de valores, la magnitud de los desafíos y la necesidad de tomar decisiones urgentes. En este contexto, los dilemas éticos que plantea la IA no pueden ser resueltos únicamente desde una perspectiva técnica, requieren un enfoque multidisciplinario que incorpore la deliberación pública, la transparencia y la buena gobernanza. En este sentido, la Unión Europea ha formulado una estrategia general de Investigación e Innovación Responsables (RRI), que se basa en cuatro principios de gobernanza: anticipación, reflexividad, deliberación y responsabilidad. Estos principios fomentan la participación ciudadana, la igualdad de género, la educación científica, la ética en la



investigación, el acceso abierto a la información científica y la gobernanza inclusiva (*European Commission*, 2019). La RRI busca reducir la brecha entre la comunidad científica y la sociedad, incentivando que diversos actores trabajen juntos en todo el proceso de investigación e innovación y alineando los resultados con los valores y expectativas sociales.

El desarrollo y uso de la IA se deben regir por una serie de deberes éticos mínimos que protejan al individuo, a la sociedad y al medio ambiente de los daños e impactos negativos que esta tecnología puede ocasionar. Estos deberes, que se presentan como un amparo frente a la vulnerabilidad humana en relación con la IA, incluyen minimizar los daños, maximizar los beneficios, respeto y autonomía, garantizar la privacidad y la identidad personal, proteger el medio ambiente y las generaciones futuras, promover la inclusión y la justicia (UNESCO. 2021).

Junto a los deberes éticos mínimos, existen elementos novedosos que singularizan la reflexión ética sobre la IA:

Explicabilidad y auditoría: La toma de decisiones basada en IA afecta ámbitos sensibles de la vida, como la atención sanitaria y los derechos humanos. Por tanto, los algoritmos deben ser auditables y trazables, especialmente en su aplicación en la administración de justicia. Sin embargo, esto plantea un desafío técnico, y es que, con mucha frecuencia, los sistemas de aprendizaje profundo funcionan como “cajas negras”, difíciles de explicar y auditar (O’Neil, 2018).

Evitar sesgos: No es un hecho que la IA sea una solución de imparcialidad para la toma de decisiones; los algoritmos de IA pueden replicar y amplificar los prejuicios inherentes a los datos, y dar lugar a discriminaciones por género, raza o estatus económico. Como lo señala O’Neil (2018), los algoritmos son opiniones encapsuladas que pueden perpetuar los errores que intentan evitar. En la administración de justicia, esto puede traducirse en una “dictadura de datos” que refuerza estereotipos y socava los principios de equidad e imparcialidad.

Atribución de responsabilidad: A medida que la IA adquiere mayor protagonismo, surge la cuestión de la responsabilidad: ¿quién es responsable cuando un sistema de IA toma una decisión equivocada? Al considerar la naturaleza distribuida de los sistemas sociotécnicos, la ética para la IA debe abordar la definición de la autonomía de la máquina y la atribución de responsabilidades entre los diseñadores, fabricantes y usuarios (Floridi, 2019).

La *algor-ética* es un concepto relativamente nuevo que combina las palabras “algoritmo” y “ética”, y se refiere al estudio de los principios éticos que deben guiar el diseño, desarrollo y uso de algoritmos, especialmente en el contexto de la IA. Esta disciplina ha surgido como respuesta a las preocupaciones crecientes sobre el impacto de los algoritmos en la sociedad y los desafíos éticos que plantea su uso.



A lo largo de los últimos años, la algor-ética ha evolucionado desde la simple consideración de sesgos en los algoritmos hasta un enfoque más integral que involucra principios de justicia, equidad, responsabilidad y transparencia. La preocupación por los aspectos éticos de los algoritmos y la IA surge a medida que estas tecnologías empiezan a desempeñar un papel cada vez más relevante en la toma de decisiones. Desde los sistemas de reconocimiento facial hasta los algoritmos que determinan el acceso a créditos o servicios, el poder de la IA para influir en la vida de las personas ha suscitado importantes interrogantes éticos.

Floridi (2015) afirma que la inteligencia artificial no debe entenderse solo como una herramienta técnica, sino también como un nuevo espacio en el que se desarrollan las relaciones humanas. Propone una visión que subraya la importancia de diseñar estos sistemas bajo principios éticos claros, lo que llevaría a la formulación de la algor-ética como un campo autónomo. En palabras de Floridi (2019, p. 83): “El diseño ético de los sistemas de IA debe garantizar que las personas sean tratadas con justicia y que los sistemas no perpetúen o amplifiquen los sesgos presentes en los datos”.

En este sentido, los primeros debates en torno a la algor-ética se centraron en cuestiones como el sesgo algorítmico. Los algoritmos, percibidos como herramientas objetivas y neutrales, en realidad son “opiniones incrustadas en código”. Esto se debe a que los sistemas de IA aprenden de los datos en los que se entrenan, y si estos datos contienen sesgos o reflejan disparidades sociales, los algoritmos tienden a reproducir esos patrones. (O’Neil, 2018, p. 45). Cuando las tecnologías de IA no se controlan y ajustan adecuadamente, pueden contribuir de forma activa a la marginación y discriminación de ciertos grupos poblacionales y reforzar así las brechas sociales (O’Neil, 2018).

Un ejemplo claro de esta problemática se observa en los sistemas de reconocimiento facial. Estudios han demostrado que estos algoritmos presentan tasas de error significativamente más altas al identificar a personas de piel más oscura o mujeres. Buolamwini y Gebru (2018) encontraron que algunos de los sistemas más utilizados tenían una precisión mucho menor en el reconocimiento de mujeres y personas de piel más oscura, debido a la falta de diversidad en los conjuntos de datos utilizados para entrenar estos sistemas. Mientras que las tasas de error para los hombres de piel clara eran casi insignificantes, las tasas de error para las mujeres de piel oscura podían ser hasta 34 % mayores. Esta disparidad en el desempeño de los algoritmos de reconocimiento facial no solo refleja los sesgos implícitos en los datos de entrenamiento, sino que también plantea serias preocupaciones sobre la equidad y los derechos fundamentales, ya que estas tecnologías son utilizadas en contextos críticos, como la vigilancia policial y la toma de decisiones judiciales.



Además, O'Neil (2016) destaca que estos sesgos no se limitan a los sistemas de reconocimiento facial. Algoritmos utilizados en ámbitos como la educación, el empleo, el crédito y la justicia penal también han demostrado inclinarse en contra de minorías étnicas, mujeres y personas de bajos ingresos. Por ejemplo, los sistemas de evaluación de riesgos utilizados en la justicia penal para predecir la probabilidad de reincidencia han sido criticados por ser más propensos a etiquetar a personas de raza negra como de “alto riesgo” en comparación con las personas blancas, incluso cuando la primera vez que se comete un delito es de menor gravedad (Angwin *et al.*, 2016).

Los ejemplos demuestran que la IA, lejos de ser una panacea para la toma de decisiones, puede exacerbar las desigualdades sociales si no se aborda desde una perspectiva ética que priorice la equidad, la diversidad y la inclusión. Por ello, O'Neil (2018) y otros expertos enfatizan en la necesidad de implementar mecanismos de supervisión, regulación y auditoría de los algoritmos, y en la importancia de incorporar la algor-ética en el diseño y la aplicación de sistemas de IA, para garantizar que estas tecnologías sean utilizadas de manera justa y responsable.

Esta tarea la iniciaron hace varios años diferentes instituciones internacionales que comenzaron a formular principios éticos para guiar su desarrollo. Uno de los esfuerzos más importantes ha sido la Guía Ética para una IA confiable de la Comisión Europea (2019). Para la Comisión, no es suficiente desarrollar la IA dentro del marco legal para que sea fiable, pues es probable que las leyes se queden rezagadas frente a la rápida evolución de las tecnologías, además, pueden ser incoherentes con las normas éticas, por ello, “para que los sistemas de IA sean fiables, deben ser también éticos” (Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, 2019). Esto implica que es preciso garantizar que cumplan las normas éticas que establecen los principios de transparencia, equidad y responsabilidad como pilares fundamentales para la IA ética.

1. *Transparencia*: se refiere a la necesidad de que los algoritmos sean comprensibles y explicables para los seres humanos. “Los algoritmos que afectan aspectos esenciales de nuestras vidas, como la justicia o el acceso a oportunidades, deben ser auditables y abiertos al escrutinio público” (Comisión Europea, 2019. N° 50).
2. *Responsabilidad*: implica que los diseñadores y usuarios de IA deben asumir la responsabilidad por las decisiones tomadas por estos sistemas. Este principio ha sido promovido por diversos autores que sostienen que la autonomía de los sistemas no exime de responsabilidad a quienes los programan. Por ejemplo, los Principios de IA de Asilomar proponen que las entidades que aplican en la práctica la IA deben ser responsables por las acciones de los sistemas, y que



deben existir mecanismos claros para subsanar los errores que puedan surgir (Moradín, 2023)

3. *No discriminación y justicia*: la IA debe diseñarse de manera que no perpetúe las desigualdades. Esto es especialmente relevante en áreas como la justicia penal, donde ya se han documentado casos en los que los algoritmos han discriminado a minorías étnicas. Según Benjamín (2019, p. 72), “los algoritmos tienen el potencial de convertirse en armas de opresión si no se controlan sus sesgos y se hace una revisión crítica de los datos con los que se alimentan”.

A medida que el concepto de algor-ética ha evolucionado, se ha ampliado para incluir temas relacionados con la sostenibilidad y la autonomía humana. Por ejemplo, el filósofo Thomas Metzinger (citado por Castelluccio, 2020), en su trabajo sobre la IA y la ética, propone que se deben establecer límites claros para evitar que los sistemas de IA tomen decisiones que comprometan la dignidad o la autonomía de las personas (Castelluccio, 2020).

Además, en 2021 la UNESCO aprobó la Recomendación sobre la ética de la inteligencia artificial. El enfoque actual de la algor-ética también aboga por la creación de algoritmos que no solo respeten principios éticos, sino que contribuyan activamente al bienestar social. En el informe *AI for Good Global Summit* (2021), se subraya la importancia de utilizar la IA para abordar desafíos globales como la pobreza, el cambio climático y la justicia social. Uno de los desafíos más importantes es la diversidad cultural. La concepción de lo que es ético varía según el contexto cultural, lo que complica la tarea de formular principios universales. Wachter y Mittelstadt (2019) han argumentado que la creación de marcos éticos debe ser flexible y adaptable para reflejar las diversas culturas y valores que coexisten en un mundo globalizado.

Se requieren guías, manuales o lineamientos para implementar la IAG en la rama judicial

La creciente implementación de sistemas de IA en la administración de justicia ha generado grandes expectativas en cuanto a la optimización de los procesos judiciales y la mejora en la tutela judicial efectiva. Sin embargo, la utilización de la IA, especialmente de la IA generativa (IAG), también plantea desafíos éticos, legales y sociales que requieren un marco regulatorio claro y preciso. En este contexto, surge la necesidad de establecer guías, manuales o lineamientos que orienten su aplicación práctica en la rama judicial, y así garantizar que su desarrollo y uso se lleven a cabo de manera ética, justa y en consonancia con los derechos fundamentales.



Se dice que la IAG se refiere a sistemas capaces de crear contenido nuevo, como texto, imágenes o sonido, lo que plantea nuevas oportunidades para el ámbito judicial, pero también riesgos. Por un lado, es cierto que estas tecnologías pueden contribuir a descongestionar los tribunales, porque se automatizan tareas repetitivas como la redacción de documentos legales o la clasificación de casos, de modo que los jueces y funcionarios podrían enfocarse en las cuestiones más complejas, pero, por otro lado, la IAG plantea preocupaciones significativas en torno a la transparencia, la responsabilidad, la protección de datos y los posibles sesgos inherentes en los algoritmos.

Como indica la Comisión Europea (CE) en sus directrices sobre la IA, es necesario y urgente garantizar que cualquier sistema de IA, incluidos los generativos, se desarrolle y utilice de manera que sea coherente con los valores y derechos fundamentales, y ello incluye la dignidad humana, la libertad individual, la democracia y la igualdad (Comisión Europea, 2019). En el ámbito judicial, significa que la IA no debe usurpar el papel del juez, sino actuar como una herramienta de apoyo que promueva la justicia y la equidad en los procesos legales.

La CE ha señalado la necesidad de establecer una visión normativa clara en torno al desarrollo y uso de la IA, y ha subrayado el concepto de una “IA fiable” como un modelo que no solo cumple con los requisitos legales, sino que además respeta los principios éticos y los derechos fundamentales (Comisión Europea, 2019). Podríamos extender esta orientación a la aplicación práctica de la IA en la rama judicial, para lo cual se requerirían guías y manuales que aborden aspectos críticos como la transparencia, la rendición de cuentas, la privacidad y la no discriminación. En este ámbito en particular, para asegurar que la IA se emplee de manera responsable, ha de ser guiada por principios éticos, como el respeto por la autonomía humana, la prevención del daño, la equidad y la explicabilidad, que se deben incluir en cualquier guía o manual sobre la aplicación práctica de la IAG en la justicia (Comisión Europea, 2019). Tales guías deben proporcionar un marco que oriente tanto a desarrolladores y operadores como a usuarios en la toma de decisiones, con el fin de garantizar que los sistemas de IA respeten los derechos de las personas y no se tomen decisiones automatizadas que las puedan afectar negativamente.

Un aspecto fundamental para la aplicación práctica de la IA en la justicia es la creación de mecanismos de rendición de cuentas. La IA puede ser vista como una “caja negra”, lo que dificulta la comprensión de cómo se toman ciertas decisiones o se generan determinados resultados. Por esta razón, las guías y manuales deben incluir directrices claras sobre cómo garantizar la trazabilidad, auditabilidad y supervisión de los sistemas de IA. La Comisión Europea subraya la importancia de que los sistemas de IA sean capaces de explicar sus decisiones y procesos, especialmente en contextos críticos como el judicial (Comisión Europea, 2019).



Además, las guías deben establecer la necesidad de una supervisión humana significativa en la implementación de la IA en la justicia. Los jueces y operadores jurídicos deben tener la capacidad de comprender y, en caso necesario, corregir o intervenir en las decisiones automatizadas. Esto garantiza que las decisiones finales en los procesos judiciales mantengan un componente humano y se ajusten a los principios del debido proceso y la tutela judicial efectiva.

Los sistemas de IAG en la justicia se deben diseñar y aplicar de tal manera que respeten los derechos fundamentales para evitar sesgos y discriminaciones. Ya se demostró antes que si no se controlan adecuadamente, los algoritmos pueden reforzar las desigualdades existentes (O’Neil, 2018). Por lo tanto, en las guías y manuales se debe recalcar la importancia de que se utilicen datos diversos e inclusivos en el entrenamiento de los sistemas de IA, para evitar que perpetúen sesgos que puedan afectar negativamente a determinados grupos poblacionales.

Asimismo, la protección de la privacidad es un aspecto prioritario, ya que los sistemas de IA generativa pueden manejar grandes cantidades de datos personales. En las guías se deben implantar normas estrictas en relación con la recopilación, almacenamiento y uso de datos, para garantizar que la privacidad de las personas esté protegida y que se cumplan las normativas vigentes de protección de datos, al estilo del Reglamento General de Protección de Datos (RGPD) en Europa (Comisión Europea, 2016).

Bonett (2023) destaca que los límites éticos de la IA se vinculan a la teoría de las TIC, y que las garantías judiciales deben protegerse tanto desde el derecho constitucional como procesal. Asimismo, la automatización del proceso impone un fuerte enfoque en la protección de datos personales frente a decisiones algorítmicas automatizadas (Palma Ortigosa, 2022).

Algunos países han comenzado a establecer lineamientos para el uso ético de la IA en la justicia. Por ejemplo, Canadá publicó la “*Directive on Automated Decision-Making*”, que establece directrices para el uso de sistemas de toma de decisiones automatizadas en la administración pública, incluidos principios de transparencia, equidad y responsabilidad (Gobierno de Canadá, s. f.) En el ámbito judicial, esta directiva puede servir de referencia para la elaboración de guías que regulen y garanticen un uso ético y responsable de la IA.

Por su parte, en Colombia, la Corte Constitucional ha exhortado a los jueces y funcionarios judiciales a incorporar en su trabajo las herramientas y prototipos de IA, con criterios éticos de responsabilidad, transparencia, no sustitución de la racionalidad humana, igualdad y equidad. Entre tanto, el Consejo Superior de la Judicatura, máxima corte encargada del funcionamiento de la Administración de Justicia, trabaja, con la participación de diversos actores (magistrados, jueces, empleados



judiciales, ingenieros, academia y centros de investigación y pensamiento), en la elaboración de los lineamientos con los cuales se busca integrar la IA de manera ética y efectiva, procurando que la tecnología sea una herramienta de apoyo en la decisión que resuelve la situación procesada sin que se reemplace el rol humano.

Conclusiones

La inteligencia artificial se ha convertido en un aliado potencial para agilizar los procesos judiciales y reducir la mora que afecta a muchos sistemas judiciales, sobre todo en países donde la carga de casos supera la capacidad de respuesta de los tribunales. Sin embargo, la IA no debe reemplazar el papel del juez humano, cuyo criterio y sensibilidad aportan una perspectiva ética y contextual que las máquinas no pueden replicar y que es esencial para interpretar las leyes en contextos específicos. La aplicación práctica de la IA debe, por lo tanto, enfocarse en complementar la labor humana, por ejemplo, se pueden automatizar tareas administrativas o análisis de datos, pero las decisiones críticas quedan en manos de los jueces.

Para aprender y tomar decisiones, los sistemas de IA se basan en datos, lo que implica que cualquier sesgo presente en esos datos puede ser perpetuado o incluso amplificado por el algoritmo. Estudios han demostrado que los algoritmos de reconocimiento facial, por ejemplo, pueden tener tasas de error significativamente mayores para personas de piel oscura o mujeres, por la falta de diversidad en los datos utilizados para su entrenamiento. En el ámbito judicial, esta realidad se traduce en un riesgo serio de discriminación si los sistemas de IA se emplean sin mecanismos de control y auditoría que identifiquen y mitiguen dichos sesgos. Por lo tanto, la incorporación de la IA en la administración de justicia debe ir acompañada de esfuerzos proactivos para asegurar que tanto el diseño como el uso de estos sistemas sean inclusivos y justos.

La “algor-ética” surge como una necesidad para guiar el desarrollo y la aplicación de la IA en la justicia. No basta con que los sistemas de IA cumplan con los requisitos legales, se deben, además, diseñar y aplicar con una base ética sólida que incluya valores como la transparencia, la equidad, la responsabilidad y la explicabilidad. La falta de una perspectiva ética en el diseño de sistemas de IA generará decisiones automatizadas opacas, sesgadas y, en última instancia, injustas. La algor-ética proporciona un marco para que los desarrolladores y usuarios de la IA en la justicia puedan evaluar las implicaciones de las decisiones algorítmicas, con el fin de garantizar que se tomen en cuenta los derechos y la dignidad de las personas que puedan verse afectadas por estas tecnologías.



Para garantizar que la implantación de la IA en la rama judicial se realice de manera ética y responsable, es imprescindible contar con guías, manuales y lineamientos específicos, los cuales deben abordar aspectos como la protección de datos, y para ello se deben establecer directrices claras sobre el manejo y almacenamiento de información sensible. Asimismo, se debe detallar la importancia de la supervisión humana, para asegurar que sean los jueces y operadores jurídicos quienes tomen o revisen las decisiones finales, y así evitar la deshumanización del proceso judicial. Además, las guías deben incluir recomendaciones sobre cómo prevenir daños, como la perpetuación de sesgos, y determinar procedimientos para la auditoría y el control de los algoritmos. Este conjunto de lineamientos puede ofrecer un marco normativo que permita incorporar la IA en la justicia de manera alineada con los principios del Estado de derecho.

La intervención humana en los sistemas de IA es esencial para garantizar que las decisiones automatizadas sean justas y se adecuen al marco legal. La IA en la justicia no debe operar de manera autónoma sin un control significativo. Los jueces y operadores jurídicos deben poder revisar y, en su caso, intervenir en los resultados generados por la IA, lo que significa que los algoritmos deben ser auditables y comprensibles para asegurar su transparencia. Solo a través de la transparencia y la posibilidad de revisión humana se puede garantizar que las decisiones judiciales respeten los principios del debido proceso y la tutela judicial efectiva. La “caja negra” de la IA no puede ser una excusa para la opacidad en las decisiones judiciales, la supervisión humana actúa como un contrapeso necesario para mantener la equidad y la justicia.

Para que la IA sea considerada una herramienta confiable en la administración de justicia, se debe desarrollar y aplicar siguiendo un marco ético riguroso, tal como lo plantea la Comisión Europea. El desarrollo de sistemas de IA confiables implica que estos deben respetar los principios de autonomía humana, equidad y protección de los derechos fundamentales. La IA confiable se basa no solo en su precisión técnica, sino en su capacidad para ser transparente, justa y equitativa. Esto requiere el uso de mecanismos que permitan evaluar y monitorear continuamente el desempeño de los sistemas de IA, para asegurar que su impacto en la justicia sea positivo y se mantenga alineado con los valores democráticos. En última instancia, la IA debe ser un facilitador del acceso a la justicia, no una fuente de nuevas formas de exclusión o desigualdad.

Los marcos éticos y normativos para la IA deben ser lo suficientemente flexibles para adaptarse a la diversidad cultural y a las distintas realidades sociopolíticas de cada país. Lo que puede ser considerado un estándar ético en un contexto cultural específico, puede no ser aplicable de la misma manera en otro. En América Latina, por ejemplo, los sistemas judiciales enfrentan desafíos particulares relacionados con



la desigualdad, el acceso a la justicia y la protección de los derechos de comunidades indígenas y minorías. Los lineamientos para implementar la IA en la justicia deben reconocer y respetar estas diferencias culturales mediante la incorporación de enfoques inclusivos y culturalmente sensibles. Solo así se podrá garantizar que la IA se convierta en una herramienta que promueva la justicia de manera equitativa en contextos diversos.

La rápida evolución de la IA y su creciente impacto en la administración de justicia hacen urgente la implantación de regulaciones claras y efectivas. Actualmente, la falta de un marco normativo específico para la IA en muchos países deja un vacío que puede dar lugar a abusos, irresponsabilidad y decisiones opacas. La regulación debe ser el resultado de un proceso inclusivo que involucre a expertos en IA, juristas, legisladores y la sociedad civil, y ser lo suficientemente dinámica como para adaptarse a los rápidos avances tecnológicos, sin sacrificar la protección de los derechos fundamentales. La normatividad en este ámbito debe abordar los aspectos tanto técnicos como éticos de la IA, para garantizar que su uso en la administración de justicia contribuya a la equidad, la transparencia y la tutela judicial efectiva.

Referencias

- Angwin, J., Larson, J., Mattu, S., y Kirchner, L. (2016). Machine bias (Sesgo de la máquina). *ProPublica.org* [página web]. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
- Ausín, T. (2021). ¿Por qué ética para la Inteligencia Artificial? Lo viejo, lo nuevo y lo espurio. *Sociología y tecnociencia*, 11 (Extra_2), 1-16. DOI: 10.24197/st.Extra_2.2021.1-16
- Benjamín, R. (2019). *La carrera tras la tecnología: herramientas abolicionistas para el nuevo código Jim*. Polity Press.
- Bonett Ortiz, S. (2023) El proceso judicial automatizado. En: D. Guerra Moreno (Coord.), *Constitución y prototipos de IA en el proceso* (pp. 155-190). Bogotá: Grupo Editorial Ibáñez, Universidad Libre.
- Bujosa Vadell, L. (2022). Ética e inteligencia artificial. Una mirada desde el proceso jurisdiccional. En: F. Bueno de Mala (dir.), *El impacto de las tecnologías disruptivas en el derecho procesal* (pp. 43-73). Universidad de Salamanca.
- Buolamwini, J., y Gebru, T. (2018). Matices de género: disparidades de precisión interseccional en la clasificación de género comercial. *Proceedings of Machine Learning Research*, (81), 1-15. <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>
- Carranza Barona, J., Segura Torres, V., Defas Ayala, V. (2023). La inteligencia artificial en los procesos de administración pública. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, 4(6), 1485-1495. <https://doi.org/10.56712/latam.v4i6.1541>



- Castelluccio, L. (2020). El verdadero sesgo es moral – Inteligencia Artificial. Una breve respuesta y reflexión al artículo: “Antinatalismo artificial benevolente (BAAN). <https://sinapticas.com/2017/10/20/el-verdadero-sesgo-es-moral/>
- Comisión Económica para América Latina y el Caribe CEPAL. (2019). Panorama social de América Latina 2018 (LC/PUB.2019/3-P). CEPAL. <https://www.cepal.org/es/publicaciones/44598-panorama-social-america-latina-2018>
- Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías. (2019). *Directrices éticas para una IA fiable*. Oficina de Publicaciones. <https://data.europa.eu/doi/10.2759/14078>
- Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías. (2016). Reglamento General de Protección de Datos (RGPD) en Europa. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Consejo Superior de la Judicatura. (2019). *Informe sobre la Justicia en Colombia*. Imprenta Nacional.
- Cordella, A., y Contini, F. (2020). *Tecnologías digitales para mejorar los sistemas de justicia: Un conjunto de herramientas para la acción*. Posadas, A., y Vásquez Jordán, D. (Eds.). <https://doi.org/10.18235/0002297>
- Corporación Excelencia en la justicia (CEJ), (2020). *Manual Azul de la Justicia en Colombia. Estadísticas sobre el estado de la justicia en Colombia*. <https://cej.org.co/wp-content/uploads/2020/11/MANUAL-AZUL-DE-LA-JUSTICIA-DE-LA-CEJ.pdf>
- Corte Constitucional de Colombia. Sala Segunda de Revisión. Sentencia T-323 de 2024. M.S. Juan Carlos Cortés González.
- Corte Constitucional de Colombia. Sentencia T-476 de 1996. M.P. Fabio Morón Díaz.
- Corte Constitucional de Colombia. Sala Octava de Revisión. Sentencia T-099 de 2021. M.S. José Fernando Reyes Cuartas.
- Corte Constitucional de Colombia. Sala Plena de la Corte Constitucional. Sentencia C-086 de 2016. M.P. Jorge Iván Palacio Palacio.
- Defensoría del Pueblo de Colombia (2019). *Informe Anual: Acceso a la Justicia y Derechos Humanos en Colombia*. <https://www.defensoria.gov.co/es/public/informes>
- Defensoría del Pueblo de Colombia. (2018). *Acceso a la justicia para las personas en condición de vulnerabilidad en Colombia*. <https://www.defensoria.gov.co/es/public/informes>
- Departamento Nacional de Planeación & Ministerio de Justicia y del Derecho. (2017). *Plan Decenal del Sistema de Justicia 2017–2027*. Bogotá: DNP. Recuperado de <https://colaboracion.dnp.gov.co/CDT/Justicia%20Seguridad%20y%20Gobierno/Documento%20Plan%20Decenal.pdf>
- Estévez, E., Fillottrani, P., y Linares, S. (2020). PROMETEA: Transformando la administración de justicia con herramientas de inteligencia artificial. Banco Interamericano de Desarrollo (BID). <http://dx.doi.org/10.18235/0002378>



- Fedesarrollo. (2019). La eficiencia en el sector justicia colombiano, Énfasis en la jurisdicción ordinaria. https://www.repository.fedesarrollo.org.co/bitstream/handle/11445/3793/Repor_Mayo_2019_Camacho_et_al_final.pdf?sequence=5&isAllowed=y
- Floridi, L. (2015). *La Cuarta Revolución: Cómo la infosfera está transformando el mundo*. Madrid: Paidós Ibéricos.
- Floridi, L. (2019). *La ética de la inteligencia artificial*. Oxford University Press.
- Funtowicz, S. O., & Ravetz, J. R. (1993). *Science for the postnormal age*. *Futures*, 25(7). [https://doi.org/10.1016/0016-3287\(93\)90022-L](https://doi.org/10.1016/0016-3287(93)90022-L) 739755.
- Gobierno de Canadá. (s. f.). Responsible use of artificial intelligence in government. <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html>
- Kelleher, J. D., & Tierney, B. (2018). *Data Science*. MIT Press.
- La Rota, M. E., Lalinde, S., Santa, S., y Uprimny, R. (2014). *Ante la justicia. Necesidades jurídicas y acceso a la justicia en Colombia*. Bogotá: Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia.
- Ministerio de Justicia y del Derecho. (2022). Informe al Congreso: Plan Decenal de Justicia 2022–2023. Bogotá: Ministerio de Justicia y del Derecho. Recuperado de <https://www.minjusticia.gov.co/Sala-de-prensa/Documents/INFORME%20AL%20CONGRESO%20PDSJ%202022%202023.pdf>
- Negro, D. (2010). *Pobreza, desigualdad, sectores vulnerables y acceso a la justicia*. En *Desigualdad e inclusión social en las Américas* (pp. 98–107). OEA y CEPAL
- Niiler, E. (2019, 25 de marzo). *Can AI Be a Fair Judge in Court? Estonia Thinks So*. WIRED. Recuperado de <https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/>
- Moradín, F. (2023). *Principios normativos para una ética de la inteligencia artificial*. México. <https://philarchive.org/archive/MORDDM-2v1>
- O'Neil, C. (2018). *Armas de Destrucción Matemática. Cómo el Big Data aumenta la desigualdad y amenaza la democracia*. Madrid: Capitán Swing. O'Neil, C.
- Palma Ortigosa, A. (2022). *Decisiones automatizadas y protección de datos: Especial atención a los sistemas de inteligencia artificial*. Madrid: Dykinson. <https://doi.org/10.2307/j.ctv2zp4t7t>
- Pasquale, F. (2024). *Las nuevas leyes de la robótica*. Barcelona: Galaxia Gutenberg.
- Ramírez, D. (2017) El rol del juez en la construcción de la tutela judicial efectiva. *IPSO JURE* (Núm. 38). *Revista del Poder Judicial del Perú*. P.60-71. Recuperado de <https://www.pj.gob.pe/wps/wcm/connect/c6456d804353a9c2972db7875b9b83f6/IPSO+JURE+38..pdf?MOD=AJPERES&CACHEID=c6456d804353a9c2972db7875b9b83f6>
- Transparencia por Colombia (2024). Más de \$21 billones de pesos perdidos y 15 millones de personas afectadas por la corrupción en Colombia revela la Radiografía de la



Corrupción 2016 – 2022. Comunicado 11 2024. <https://transparenciacolombia.org.co/comunicado-radiografia-2016-2022/>

UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. París: UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000380455>

Wachter, S., y Mittelstadt, B. (2019). Un derecho a inferencias razonables: repensar la legislación sobre protección de datos en la era del big data y la inteligencia artificial. *Columbia Business Law Review*, 2. <https://ssrn.com/abstract=3248829>



Capítulo 7

El “abogado programador” como alternativa para abordar la IA en el derecho procesal Perspectivas a partir de la Sentencia T-323/24

Omar Alfonso Cárdenas Caycedo

Introducción

En este capítulo se aborda una visión distinta sobre la relación entre el derecho procesal y la inteligencia artificial (IA), una visión, si se quiere, atrevida y por ello arriesgada. Se pretende repensar la forma como los abogados interactúan con la IA puesto que, hasta ahora, acuden a ella en busca de soluciones o respuestas jurídicas, de hecho, son innumerables las conferencias y textos que retratan los riesgos asociados a esta práctica. Una segunda propuesta, otro camino posible, es el de un abogado que se acerca a la IA en busca de respuestas no jurídicas, sino tecnológicas, como, por ejemplo, la creación de código fuente con posibles aplicaciones en lo jurídico.

Para presentar esta idea, en la primera parte se desarrolla el problema que conlleva el fenómeno de la “IA embebida”, esto es, cómo las aplicaciones más comunes se unen con la IA y generan, sí o sí, un impacto en las comunidades que usan una aplicación base que ahora tiene, quieran o no, a la IA como una opción del día a día. La IA se vuelve inevitable.

En segundo lugar, se hace un breve recorrido sobre algunos aspectos expuestos por la Sentencia T-323/24 de la Corte Constitucional de Colombia, sentencia que se mueve en un contexto de IA embebida en cada vez más aplicaciones y programas. Esta providencia propone algunos usos autorizados en el derecho, pero, en lo tecnológico, no desarrolla cómo deben realizarse.

Para echar a andar estos usos permitidos de la IA en el Derecho, se propone aquí la figura del “abogado programador”: un jurista que se atreve a “programar” o al menos acercarse a este concepto, para lo cual se vale de la IA (ChatGPT-4.0 para



ser exactos) con el fin de encontrar soluciones verdaderamente tecnológicas a problemas cotidianos.

El texto presenta los resultados de la investigación que, al respecto, se ha adelantado en la Universidad de Nariño, en los cuales se evidencian los primeros pasos que debe seguir un abogado que decide asumir este enfoque, se exponen los *prompts*⁴⁶ utilizados, las respuestas de la IA y las posibles aplicaciones prácticas de la programación personalizadas y de fácil acceso con ayuda de la IA generativa.

Finalmente, se presentan los posibles usos de este nuevo enfoque, que van mucho más allá de las pruebas realizadas, para luego advertir los riesgos implícitos en esta forma de acercarse a la IA.

El fenómeno de la “IA embebida”

En 2011, Marc Andreessen, cofundador de Netscape, escribió un artículo en *The Wall Street Journal* con un título llamativo: “Por qué el software se está comiendo el mundo”. Años después, en 2017, el CEO de NVIDIA, Jensen Huang, retomó esa reflexión y la reformuló en una entrevista para la prestigiosa *MIT Technology Review*: “El software se está comiendo el mundo, pero la IA se va a comer al software” (Simone, 2017).

Las dos frases, y con ellas los dos momentos históricos que reflejan, con apenas seis años de diferencia, ponen en evidencia los profundos cambios que la sociedad humana está viviendo en lo que va corrido del siglo XXI. Estos cambios pueden describirse por etapas: (i) en la primera etapa, lo tecnológico fue haciendo parte de las diferentes interrelaciones sociales (desde comunicarse hasta enamorarse) y generó que prácticamente todos los estadios de la vida estuviesen mediados, o se pudieran mediar, por Internet, softwares y computadores (Sadin, 2018). Esta primera etapa, claramente, ya ocurrió, y es a la que se refería Andreessen en 2011. (ii) Luego, llegó

⁴⁶ Sobre la definición de *prompt* se ha dicho: “Recibimos la expresión *prompt* desde el idioma inglés, aunque su origen es bastante más remoto. [...] Según el ‘Oxford Advanced Learner’s Dictionary of Current English’, [...] como adjetivo *prompt* significa ‘acting, done, sent, given, without delay’. Es decir, hace referencia a una cualidad vinculada con actuar sin demoras, velocidad de respuesta. El mismo diccionario, al hacer referencia al verbo *to prompt*, en su primera acepción indica que se refiere a ‘be the reason causing (sb to do sth)’, lo que implica ser la causa de una acción, por ejemplo, hacer que alguien haga algo. En la segunda acepción del verbo encontramos un significado bien específico, dice que significa ‘follow the text of a play and give (an actor) his cue’, relacionando la expresión con una instrucción, un texto al cual alguien tiene que seguir. Siguiendo esta acepción se define al ‘prompter’ como ‘a person who prompts actors’, es decir, es quien va proporcionando el texto o lineamientos a una persona que debe seguirlo o cumplirlo.

“En el diccionario inglés-español ‘Collins Pocket’, se establecen los mismos lineamientos de traducción: tratándose del adjetivo, *prompt* significa rápido, mientras que como verbo en general se trata de mover, incitar o instar, [y] en el mundo del teatro se traduce ‘prompt’ como apuntar. También se destaca *prompt* como expresión que se añade a una hora determinada y, por lo tanto, significa ‘puntualmente’ o ‘en punto’, como si se dice ‘five o’clock prompt’.

“Desde el punto de vista etimológico, *prompt* viene del latín ‘promptus’ que es el participio pasado del verbo ‘promere’, que significa originalmente prontitud, o —como verbo de movimiento— que va para adelante, ir de atrás hacia adelante. Efectivamente, consultando la raíz en idioma latín de la expresión ‘promptus’ significa ‘pronto, presto, expedito, fácil’, así como ‘salida pronta o prontitud’, según el Diccionario Latino Español Valbuena Reformado” (Bugallo, 2023, pp. 126-127).



la segunda etapa, en la cual, una vez la sociedad humana dependía mayoritariamente de las TIC para trabajar, interrelacionarse, comunicarse, e incluso formar su opinión política, se dio una correlación muy íntima entre lo tecnológico y lo humano, que implica que todo cambio que se produzca en el escenario tecnológico, como la llegada de una nueva tecnología, conlleva, necesaria e insoslayablemente, un cambio o impacto en lo social. Ese estado se alcanzó entre 2011 y 2020, y fue acentuado por la pandemia. (iii) En la tercera etapa, la tecnología sufre un cambio muy fuerte con el advenimiento de la IA, lo que representa un avance muy grande que hace que todo el escenario tecnológico se transforme y con ello se transforme también, como una consecuencia de las dos etapas anteriores, la sociedad humana en su conjunto (Sadin, 2020); a esto se refería Jensen Huang en 2017.

Esa tercera etapa, que va más o menos desde 2015 hasta la actualidad, tiene un componente particular: la inteligencia artificial (IA). La IA está transformando sustancialmente todo el contexto tecnológico, esto quiere decir que las empresas y desarrolladores de software y hardware en todo el mundo están compitiendo por incorporar, en mayor o menor medida, IA a sus aplicaciones y softwares. Si ese mundo tecnológico cambia gracias a la IA, necesariamente la sociedad humana, muy vinculada ya con ese mundo tecnológico, cambia también y termina relacionándose de forma íntima con la IA. Un ejemplo sencillo lo demuestra: hoy, es absolutamente normal y cotidiano utilizar procesadores de texto (como Word de Microsoft) para laborar o estudiar, si Microsoft incluye la IA en su procesador de texto, es inevitable que todos los usuarios que utilizan el programa queden, automáticamente, inmersos en el mundo de la IA y su uso para las tareas cotidianas. De hecho, Microsoft ya ha anunciado el proyecto Copilot, que consiste básicamente en generar IA embebida en la suite de Office, y hacer que todos los usuarios de los populares Word, Excel o Power Point, trabajen con apoyo de la IA (Microsoft Centro de Noticias, 2024).

Un segundo ejemplo, muy claro y reciente es de Meta Inc, propietaria de las aplicaciones Facebook, Instagram y WhatsApp, la cual venía desarrollando una IA del tipo LLM (gran modelo de lenguaje) denominada Llama⁴⁷ (llama.meta.com). La primera fase se dio cuando los ciudadanos del mundo empezaron a descargar masivamente la aplicación WhatsApp, muy popular en América Latina, como proveedor de mensajería instantánea; una vez gran parte de la sociedad la había incorporado en su cotidianidad laboral, personal, familiar e incluso sentimental, Meta puso a disposición en la aplicación, a principios de 2024, el sistema LLaMa, para que todos sus usuarios puedan, desde la aplicación, dialogar con la IA (CNN en español, 2024). Si la sociedad está conectada a través de un software, y este es alimentado con una IA, necesariamente la IA impacta en esa sociedad.

⁴⁷ El modelo de LLaMa es la apuesta de la gran corporación Meta Inc. (antes Facebook Inc.): un modelo de código abierto que se puede implementar en diferentes aplicaciones, el actual es LLaMa 3.1 y cuenta con versiones en 8B, 70B y 405B. Sobre este modelo véase: Córdón García (2023), Misseri (2023), Maya Gualtieri (2023) y Radanliev (2024).



Este fenómeno, que aquí llamamos “IA embebida”, consiste en que las aplicaciones cotidianas, poco a poco, terminan con un grado mayor o menor de IA incorporada, de tal suerte que al usuario no le queda de otra que interactuar con la IA para seguir disfrutando de la aplicación tradicional.

La IA embebida también es un fenómeno que ocurre en el derecho. Por ejemplo, hoy el sistema judicial y la asesoría legal están, necesariamente, mediadas por programas informáticos: los juzgados usan la suite de Microsoft como Word o Excel para generar documentos y cálculos (piénsese en las liquidaciones de créditos en procesos ejecutivos), Outlook de Microsoft para el correo electrónico, y utilizan diversos programas para llevar a cabo las audiencias por medios virtuales (Teams, Jitsi, Polycom, Lifesize, etc.); estos programas, poco a poco, van incorporando IA (decisión que les corresponde a sus fabricantes y propietarios en materia de derechos de autor), por lo que, sin duda, la actividad judicial también empezará, tarde que temprano, a aplicar las facilidades que esa IA embebida en el programa puede brindar al usuario. Si la IA embebida ayuda al usuario, por ejemplo, a redactar un párrafo, a liquidar más fácil, a transcribir una audiencia o a contestar un correo, será solo cuestión de tiempo para que ese usuario la use, al principio con timidez y polémica, pero después con mayor normalidad y cotidianidad.

En consecuencia, el impacto de la IA en el derecho no pasa por la discusión de si se va a dar o no, pues es un hecho que las aplicaciones que utilizan los abogados tendrán —o ya tienen— IA embebida, sino, más bien, de cómo se dará esa incursión, en qué medida, con cuáles límites y en cuánto tiempo. La discusión no es, se itera, en el qué, sino en el cómo se interrelacionará la IA con el derecho. En otras palabras, la IA inevitablemente tendrá que ver con el trabajo de jueces y abogados en el corto plazo.

La IA embebida y la Sentencia T-323/24

La Corte Constitucional de Colombia profirió una de las decisiones más interesantes, y quizá polémicas, sobre el uso de IA, específicamente de ChatGPT, por parte de jueces y magistrados. La decisión, consagrada en la Sentencia T-323 de 2024, surgió de un caso relativamente sencillo en términos jurídicos, pero en cuyo fallo un juez decidió utilizar ChatGPT para redactar algunos párrafos de la parte considerativa, todo dentro del trámite de acción de tutela (Corte Constitucional de Colombia, Sentencia T-323, 2024).

La sentencia trata in extenso el problema de la IA y su uso por parte de autoridades judiciales, sin embargo, analizar a profundidad cada una de sus aristas desborda el objetivo de este trabajo, de modo que nos detenemos en ciertas cuestiones fundamentales que son de relevancia frente a, por un lado, el fenómeno de la IA embebida y, por otro lado, a la propuesta del abogado programador.



Una nueva visión del debido proceso.

Varios sectores de la academia —incluido el autor de este escrito— habían advertido que el advenimiento de la IA hacía necesario reformular el compendio de garantías que forman parte del debido proceso, a fin de incluir unas nuevas prerrogativas que protejan al individuo de la actual comunión entre IA y derecho; estas garantías deben emerger de los instrumentos de *soft law* ya existentes en la materia (Cárdenas Caycedo, 2023; Nieva Fenoll, 2018; Pulido, 2020).

La Corte Constitucional desarrolla esta tesis bajo el concepto de “sistema de garantías tecnológico”, por cuanto observa que el advenimiento de la IA puede implicar agresiones a las garantías de juez natural, la motivación de las decisiones judiciales y el debido proceso probatorio (Corte Constitucional de Colombia, Sentencia T-323, 2024). La Corte lo expresa en los siguientes términos:

En conclusión, pese a la inexistencia de un marco regulatorio sobre la IA en el Estado colombiano, la Constitución Política de 1991, la ley sobre tecnologías de la información, las leyes sobre manejo de datos e instrumentos del ejecutivo contienen todo un sistema de garantías que, en palabras actualizadas de Ferrajoli, constituiría un sistema de garantías tecnológico (Corte Constitucional de Colombia, Sentencia T-323, 2024, p. 2)

La Corte comprende los problemas de la IA desde una perspectiva de garantías que incluye el debido proceso, el *habeas data*, entre otros derechos inmersos. Se trata de una propuesta que obliga a repensar la necesidad de adecuar las garantías y derechos constitucionales contenidos en la Constitución Política de 1991, en la cual lo tecnológico no se encontraba en la agenda principal de los constituyentes.

En dicha sentencia, la Corte sintetizó algunas garantías que deben mediar en el uso de IA en la decisión judicial: transparencia, responsabilidad, privacidad, no sustitución de la racionalidad humana, seriedad y verificación, prevención de riesgos, igualdad y equidad, control humano, regulación ética, adecuación a buenas prácticas y estándares colectivos, seguimiento continuo, adaptación e idoneidad. (Corte Constitucional de Colombia, Sentencia T-323, 2024). Estas garantías coinciden, en líneas generales, con instrumentos internacionales sobre la materia como, por ejemplo, el Reglamento (UE) 2024/1689 (IA Act), o la Guía de Principios del ELI para la toma de decisiones automatizadas, entre otros.

Usos autorizados y no autorizados de la IA en el derecho procesal.

La Corte Constitucional reseña algunos usos autorizados o legítimos de la IA en escenarios judiciales, porque no afectan derechos o garantías de los usuarios del sector justicia. La Corte lo refiere de la siguiente manera:



En efecto, tratándose del servicio de justicia, estas tecnologías eventualmente podrían utilizarse con fines de (i) gestión administrativa y documental (p. ej. reparto, agenda para la programación de diligencias, digitalización y clasificación de expedientes, sistemas de relatoría y motores de búsqueda de jurisprudencia); (ii) apoyo a la función judicial, en actividades que no suponen una labor de creación de contenido ni interpretación de hechos o textos, ni solución de casos, como en el caso de la herramienta Pretoria aplicado por esta Corte Constitucional en materia de seguimiento a procesos por acción de tutela (p. ej. referenciación de jurisprudencia, seguimiento de líneas jurisprudenciales, análisis de datos estadísticos, identificación de temas repetitivos, interacción con usuarios del Poder Judicial, contestando dudas de los usuarios mediante un banco de preguntas frecuentes preestablecidas); y (iii) corrección y síntesis de textos, siempre y cuando, estos sean supervisados posteriormente por el operador jurídico para determinar su precisión, coherencia y correcta aplicación. El uso de la IA para los anteriores fines tiene el potencial de mejorar el bienestar de los funcionarios públicos de la Rama Judicial y de los ciudadanos que hacen uso de este servicio, pues permite que la prestación del servicio judicial sea más eficiente y eficaz. Sin duda, progresivamente la justicia sin perder su majestad e independencia, habrá de caber en un terminal de comunicación personal, dentro de una red tecnológica que le sirva de sustento, a tiempo con el avance de una sociedad cada vez con mayor digitalización. (Corte Constitucional de Colombia, Sentencia T-323, 2024)

Después de un extenso análisis, la Corte encontró también que, por el contrario, existen ciertos usos de la IA en entornos judiciales que conllevan un alto nivel de riesgo para los derechos y garantías fundamentales. En tal sentido, la Corte concluyó que no debe usarse IA en aspectos como: (i) evaluación de las pruebas —licitud, legalidad, pertinencia, conducencia y utilidad— y su valoración; (ii) manejo de datos sensibles o personales; (iii) cuando se usa la IA como sustituto del raciocinio humano que es indelegable; (iv) cuando no se informa el uso de la IA; (v) cuando no se verifica el resultado o no se hace supervisión o control humano; (vi) cuando no se adoptan medidas para evitar la lesión a derechos fundamentales (Corte Constitucional de Colombia, Sentencia T-323, 2024).

La Corte aclaró que estas subreglas son temporales y pueden cambiar conforme varíen los adelantos tecnológicos y las condiciones. Este tipo de admoniciones deja entrever que la Corte es consciente del cambio vertiginoso de la tecnología y su inevitable impacto en la labor de los jueces, lo que puede implicar a futuro cambios de postura hacia otras más o menos rígidas.

El “abogado programador”: una alternativa a la relación IA y derecho

La Sentencia T-323/24 puso de presente una cuestión muy novedosa en el derecho procesal colombiano: la posibilidad de que un juez o un magistrado apliquen la IA en labores como la gestión administrativa y documental, el apoyo a la función judicial o



la corrección y síntesis de textos (Corte Constitucional de Colombia, Sentencia T-323, 2024). En este escrito no se aborda una crítica a los postulados de la Corte, más bien, se trata de responder a una pregunta sobre la posibilidad real de que un juez o un magistrado sigan a pie juntillas la posición de la Corte. Dicho de otra manera, se pretende dar respuesta a los siguientes interrogantes: ¿cómo podría un juez usar la IA en los tres ejemplos que la Corte dio de usos autorizados?, ¿cómo aplicar la IA para la gestión administrativa y documental, el apoyo a la función judicial o la corrección y síntesis de textos?

Normalmente, cuando los abogados se acercan a la IA se piensa en ella teniendo como epicentro el derecho, se espera que la IA haga análisis como los hacen los abogados, que redacte documentos, etc.; en síntesis, se maravillan al pensar que la IA pueda, o no, desempeñar sus tareas cotidianas. Esto conduce a que los intentos siempre tengan el mismo esquema: llevar la IA a lo jurídico. Ejemplos pululan, el caso mismo que analizó la Sentencia T-323/24, esto es, la decisión del juez de Cartagena que usó ChatGPT es uno emblemático. El abogado se acerca a la IA para realizar preguntas de corte o contenido jurídico, tal vez por eso las respuestas no son las más afortunadas o los ejercicios están llenos de controversias y críticas.

¿Es posible un ejercicio contrario? ¿Y si en lugar de traer la IA al mundo jurídico, los abogados se acercan a la IA? O mejor, en vez de pedirle a la IA que responda como abogado, ¿no se debería intentar que el abogado comprenda el lenguaje de la IA? Se pasa a explicar este planteamiento.

ChatGPT es un gran modelo de lenguaje, un LLM (por sus siglas en inglés) cuyo objetivo no fue, en principio, configurarse como una IA para abogados litigantes y jueces; este fue, si se quiere, un uso que surgió en el camino y en la explosión de popularidad de esta herramienta cuando, el 30 de noviembre de 2022, OpenAI la lanzó al mundo. Un LLM no es una herramienta *ad hoc* diseñada de manera personalizada para el mundo jurídico, ni mucho menos dirigida exclusivamente al ordenamiento jurídico de un país concreto. Si esto fuera así, tal vez este abordaje del aplicativo puede no ser el mejor. Se trata de una herramienta más general a la que muchos le dan un uso particular, de una ciencia o disciplina altamente especializada y compleja, como puede ser el ejercicio del derecho en un determinado país. Ello podría explicar los sesgos, alucinaciones e inconsistencias que se encuentran en las respuestas y que diversos autores han referenciado (Ramírez, 2023).

Por el contrario, podría ser un ejercicio más productivo —aunque más difícil— que el abogado se acerque al aplicativo para indagar en él lo que mejor sabe hacer, o que busque en este las tareas que más fácilmente desarrolla, para luego, en un ejercicio dialéctico, tratar de incorporar esas ejecutorias en su labor. En esta forma de abordar el problema, el abogado o juez no interactúa con la IA para pedir de ella respuestas que debería encontrar con su propia formación jurídica, sino, mejor, para



analizar la IA, descubrir usos probados y luego incorporarlos en su actividad; pedirle a la IA respuestas tecnológicas, más que respuestas jurídicas.

Este tipo de aproximación es mucho más complejo, pues requiere que el abogado deje de pensar en clave exclusivamente jurídica, o en lenguaje de su saber, para atreverse a pensar en clave tecnológica o de otro saber. Es como intentar ponerse a hablar en otro idioma sin mayores bases. La propuesta que aquí se hace es que el abogado dialogue realmente con la ingeniería de sistemas, la programación y con la IA misma, pero para entender sus dialécticas y luego incorporarlas a su quehacer. Esta aproximación puede resultar menos espectacular que la redacción de una sentencia por ChatGPT, pero el resultado, por discreto, sería más seguro, fijo y absolutamente confiable.

A continuación, se presenta un uso que ha desarrollado el Grupo de Investigación Centro de Estudios Jurídicos Avanzados de la Universidad de Nariño.

El “abogado programador”.

La tecnología busca solucionar problemas cotidianos concretos. En Colombia, el abogado y el juez actuales se enfrentan a uno: ¿cómo pueden usar la IA para mejorar la gestión documental, el apoyo a la gestión documental o la corrección de textos? ¿Qué significan esas categorías?

La respuesta dependerá de cada despacho, en cada juzgado o tribunal se encuentran problemas de gestión y administrativos muy concretos que difieren unos de otros; no hay uniformidad. Del otro lado de la baranda, los litigantes también tendrán, cada uno, un problema distinto por resolver. A guisa de ejemplo, en un despacho podría ser útil un aplicativo que liquide intereses, en otro, uno que haga liquidaciones de indemnizaciones laborales, en otro, uno que calcule daño emergente o lucro cesante, en otro podría ser útil la revisión de sentencias, en otro, la carga administrativa de cada funcionario, y así sucesivamente.

¿Podría la IA resolver estos problemas? Seguramente, si se le pregunta de entrada a ChatGPT, la respuesta puede ser desalentadora. ¿Cómo es posible lograr esas funcionalidades en un diálogo con la IA? ¿Realmente las puede ejecutar con eficacia?

Es aquí donde al abogado puede lanzarse a “aguas desconocidas” y tratar de resolver estos problemas cotidianos a través de la IA, pero aprovechando una de sus capacidades más alabadas: la de programar y generar código fuente. La idea sería que el abogado pueda usar la IA para diseñar sus propias aplicaciones que se ajusten a sus necesidades, usarla para que responda con código fuente, en lugar de buscar en ella respuestas jurídicas.

Es una propuesta atrevida, pues la formación de los abogados no incluye los contenidos básicos para programar, así que la tarea no parece nada fácil. ¿Resultaría



útil? La respuesta es que un abogado que utilice la IA para programar aplicativos simples que le ayuden a resolver tareas concretas del mundo jurídico, sería mucho más competitivo que uno que espere que la IA otorgue las respuestas como si de un oráculo se tratara.

Elementos claves que debe conocer un “abogado programador”

El abogado que se atreva a acercarse a la IA de esta manera, debe empezar por conocer unas herramientas básicas. Lo primero es familiarizarse con un lenguaje de programación. En las pruebas que se realizaron en la Universidad de Nariño se empleó el lenguaje Python por su facilidad y popularidad, además por haber sido utilizado en aplicaciones jurídicas en Colombia, tal como lo refiere León García (2023). Entonces, se le insertó a ChatGPT-4o el siguiente prompt:

Prompt: Debes asumir el rol de un profesor de programación, en mi caso mi rol será de un abogado que no tiene ningún conocimiento de programación. Quiero que me expliques cómo instalar Python en mi computador para que me puedas enseñar a programar, utilizo Windows, así que todas las explicaciones deben concentrarse en este sistema. Debes hacerlo explicando paso a paso, dándome los links de acceso que requiero.

Parte de la respuesta fue la siguiente:

Figura 1. Parte inicial de la respuesta de ChatGPT-4o al prompt propuesto.



Memoria actualizada

¡Perfecto! Como mencionas que usas **Windows** y no tienes ningún conocimiento previo de programación, te guiaré paso a paso en cómo instalar Python en tu computador de la manera más sencilla posible.

Paso 1: Descargar Python

1. Ve a la página oficial de Python:

- Link: <https://www.python.org/downloads/>

Al ingresar a la página, verás un botón grande que dice “**Download Python [versión]**”. Haz clic en ese botón. La página detectará automáticamente tu sistema operativo (Windows) y te proporcionará la versión más reciente compatible.

Paso 2: Ejecutar el instalador

1. Busca el archivo descargado. Dependien  le la configuración de tu navegador, el archivo



La respuesta en su totalidad fue estructurada y acorde con lo requerido, una persona con mínimos conocimientos de computación puede seguir el paso a paso y lograr la instalación de Python en su computador personal.

El segundo paso es usar un editor de código, uno de los más comunes es Visual Studio Code, se le puede pedir a ChatGPT orientación para instalarlo. El prompt utilizado fue el siguiente:

Prompt: Debes asumir el rol de un profesor de programación, en mi caso mi rol será de un abogado que no tiene ningún conocimiento de programación. Quiero que me expliques cómo instalar Visual Studio Core en mi computador para que me puedas enseñar a programar, utilizo Windows, así que todas las explicaciones deben concentrarse en este sistema. Debes hacerlo explicando paso a paso, dándome los links de acceso que requiero. Explícame el funcionamiento básico de esta herramienta.

La respuesta de ChatGPT-4o fue acorde con lo deseado, y siguiendo las instrucciones de la IA el usuario puede fácilmente instalar el programa Visual Studio Core.

El tercer paso consiste en comprender que no todo programa puede crearse en el computador local, cuya capacidad normalmente es muy limitada para la tarea de programar, por eso se recomienda apoyarse en una herramienta en línea que permita al abogado programar fácilmente sin necesidad de adquirir hardware especializado. Esto se puede lograr a través de aplicativos como Google Colab, un sistema que permite escribir y ejecutar código Python en línea, usando los recursos disponibles por Google Inc. Básicamente, es como si se tomaran prestados los potentes servidores de Google para programar, en lugar de hacerlo en el computador de oficina o casa. El prompt utilizado fue el siguiente:

Prompt. Ahora quiero que me guíes paso a paso en la suscripción de una cuenta en Google Colab, quiero que me expliques sus principales funciones. Recuerda que no tengo conocimientos en programación, soy un abogado.

En la respuesta, el sistema explicó el paso a paso para abrir una cuenta en Google Colab.

Por su extensión, no se transcriben todas las respuestas, pero se concluye que ChatGPT-4o responde de manera muy eficaz al problema de instalar Python y Visual Studio Code en un computador local, así como para abrir un Google Colab. Como se puede ver, la explicación es sencilla y fácil de seguir por alguien sin conocimientos previos en programación y con conocimientos básicos en computación.



El abogado intenta programar con ayuda de ChatGPT.

Hasta el momento, el abogado programador tiene listas tres herramientas que ahora debe usar para programar. Existe una famosa prueba entre programadores denominada “¡Hola Mundo!”, que consiste en una sencilla línea de código de fuente que, una vez ejecutada, devuelve como respuesta la frase “¡Hola mundo!”. La idea es construir un prompt que permita que ChatGPT-4o explique al abogado programador cómo puede superar la prueba mencionada.

Prompt: Asume el rol de un profesor o maestro en programación, debes partir de la base que soy abogado y no tengo conocimientos en programación. Ya tengo una cuenta en Google Colab, debes explicarme paso a paso cómo podría programar la famosa prueba “¡Hola Mundo!”, señala el paso a paso. En caso de requerir código fuente, debes entregarme las líneas listas para copiar y pegar.

Figura 2. Parte de la respuesta de ChatGPT-4o al Prompt mencionado

Paso 2: Crear un nuevo cuaderno

1. Una vez en la página principal de Google Colab, busca y haz clic en el botón “Nuevo cuaderno” o “New Notebook”. Este botón suele estar en la esquina inferior derecha o en el menú principal.
2. Se abrirá una nueva pestaña con un cuaderno en blanco. Aquí es donde escribirás y ejecutarás tu código.

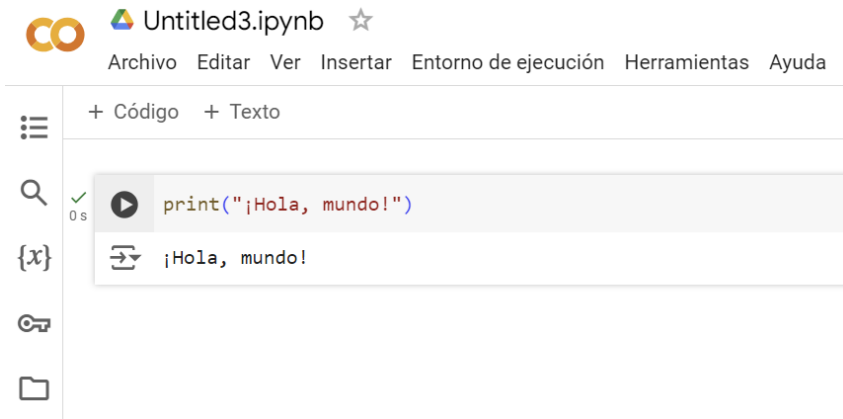
Paso 3: Escribir el código “¡Hola, mundo!”

1. Verás una **celda de código** vacía que tiene un símbolo `[ ]` al lado.
2. Haz clic dentro de esta celda para comenzar a escribir código.
3. Escribe el siguiente código exactamente como aparece:

A screenshot of a code cell in Google Colab. The cell has a dark background. At the top left, the word "python" is written in a light gray font. At the top right, there is a copy icon and the text "Copiar código". In the center, the Python code `print("¡Hola, mundo!")` is displayed in a light green font.

En este caso, ChatGPT-4o señaló los pasos, uno a uno, que debe seguir el abogado programador para superar la prueba ¡Hola Mundo!. En la investigación, y sin auxilio de ningún ingeniero, se procedió a seguir los pasos en la plataforma Google Colab. El resultado fue el siguiente:



Figura 3. Prueba ¡Hola Mundo! en Google Colab orientada por ChatGPT

El siguiente paso es realizar la misma prueba, pero en el entorno local del computador personal, es decir, utilizando Visual Code Studio y Python instalados en el sistema. Para ello se le pidió a ChatGPT con el siguiente prompt:

Prompt: Asume el rol de un profesor o maestro en programación, debes partir de la base que soy abogado y no tengo conocimientos en programación. Ya tengo instalado en mi PC, con Windows, Python y visual Studio Code. Debes explicarme paso a paso cómo podría programar la famosa prueba “¡Hola Mundo!”. En caso de requerir código fuente, debes entregarme las líneas listas para copiar y pegar.

En la respuesta, ChatGPT-4o orientó perfectamente y paso a paso cómo utilizar Visual Studio Code, arrojó la línea de código fuente requerida y explicó la forma de ejecutarla. Aquí es muy importante conocer que, para ejecutar la prueba, se debe abrir la terminal del sistema o símbolo de sistema, buscar la carpeta donde se guardó el archivo `.py` creado con Visual Studio Code y, en esa carpeta, ejecutar las instrucciones que ChatGPT proporciona. La IA explica cómo se puede navegar en la terminal del sistema (comandos `dir`, `cd`, `cd.`).

El resultado, en la terminal del sistema, fue el siguiente:

Figura 4. Terminal del sistema ejecutando Python

```
PS C:\Users\Udenar\downloads> python holamundo.py
¡Hola, mundo!
PS C:\Users\Udenar\downloads> |
```



Hora de dar un paso hacia adelante. ¿Qué hacer si algo sale mal?

Una vez se ha conseguido llevar a cabo estas pruebas sencillas, es posible que el abogado programador intente construir prompts con el objetivo de que ChatGPT le ayude a programar una solución concreta para un problema determinado de su despacho o bufete. Sin embargo, la IA, como toda ejecutoria humana, no es perfecta, y en ocasiones el código escrito por esta no se ejecuta bien o, en otras, el usuario, por su inexperiencia en un campo tan complejo, no ejecuta bien las instrucciones; en ambos eventos el resultado es el mismo, un error o algo que no funciona. ¿Qué hacer?

Una de las funcionalidades más interesantes de ChatGPT-4o es su capacidad de “ver”, el usuario puede cargar una imagen en formato JPG o similares y ChatGPT-4o la puede analizar y dar cuenta de su contenido, puede describirla con facilidad y realizar un prompt sobre ese contenido. Esta funcionalidad es muy útil, porque permite la interacción imagen-texto e, incluso, con la conexión que ChatGPT-4o tiene con Dall-e, interacción imagen-imagen.

El abogado que intenta programar con auxilio de la IA se enfrenta a un problema mayúsculo: su formación no incluye conocimientos especializados en computación y construcción de software, los cuales, sin duda, se requieren para resolver problemas que se presentan al intentar programar desde cero. Ante un error, como una línea de código que no funciona, no cuenta con mayores herramientas para resolver la situación por sí solo.

Una posible solución es tomar captura de pantalla del error y luego suministrar la imagen a ChatGPT-4o. La IA toma la imagen, analiza el contenido y procede a proponer una posible corrección o solución al problema.

Figura 5. Interacción con ChatGPT-4o para la solución de un error

ChatGPT 4o ▾



¡Claro! Pasa el error que estás recibiendo para que pueda ayudarte a resolverlo. Con el mensaje de error podré identificar mejor lo que está sucediendo y guiarte en la solución.

```
PS C:\Users\Udenar\downloads> pyinstaller --console --window prueba1.py
666 INFO: PyInstaller: 6.10.0, contrib: none, 2024.0
666 INFO: Python: 3.12.4
636 INFO: Platform: Windows-11-10.0.22H2-1506
636 INFO: Python architecture: C:\Users\Udenar\AppData\Local\Programs\Python\Python312
Script file 'prueba1.py' does not exist
PS C:\Users\Udenar\downloads>
```



El error que estás viendo dice "Script file 'prueba1.py' does not exist", lo que significa que PyInstaller no pudo encontrar el archivo `prueba1.py` en la ubicación desde la que ejecutaste el comando.

Posibles soluciones:

1. Verifica la ubicación del archivo:

- Asegúrate de que el archivo `prueba1.py` esté realmente en el directorio `C:\Users\Udenar\downloads` donde ejecutaste el comando. Si no es así, navega hasta el directorio correcto usando el comando `cd` en PowerShell.
↓
- Por ejemplo, si el archivo está en `C:\Users\Udenar\documents`, entonces deberías ejecutar:



En la Figura 5, se le puso de presente un error a ChatGPT-4o a través de una imagen, una captura de pantalla de la terminal o símbolo de sistema en el cual se pretendía ejecutar unas instrucciones dadas por el mismo ChatGPT. La IA analiza el contenido de la imagen, identifica el error y suministra pasos a seguir para solucionarlo.

Debe aclararse que la IA no es perfecta, en ocasiones las soluciones que propone no funcionan o el error persiste. Un buen ejercicio es presentar el error a otras IA como Claude o Gemini, la combinación de IA puede generar la respuesta al error presentado.

Resultados: aplicativo simple diseñado con auxilio de ChatGPT-4o.

En el grupo de investigación se avanzó utilizando ChatGPT-4o siempre bajo la premisa de que interactuaban usuarios con formación y conocimientos jurídicos, pero sin experiencia previa en programación. El reto que se propuso fue construir una calculadora básica a través de ChatGPT, pedirle que generara el código fuente y orientara en el paso a paso. El aplicativo no solo orientó en la construcción del código fuente y la creación del archivo Python (un archivo con extensión `.py`), sino que, además, brindó el camino para convertir el archivo `.py` en un ejecutable (`.exe`), de tal modo que, al dar doble clic sobre el mismo, se abrió una calculadora totalmente funcional.

Prompt: Asume el rol de un profesor de programación básica, yo soy abogado y no conozco nada de programación. Tengo instalado Python y Visual Studio Code, también utilizo Google Colab, mi PC funciona con Windows. Deseo programar una calculadora totalmente funcional en Python y luego convertirla a un ejecutable `.exe`, quiero que me des el paso a paso de cómo hacerlo. La calculadora debe tener las siguientes condiciones: 1. En la parte superior tendrá una franja negra con números blancos, en esta parte se podrán ver las operaciones y los resultados. 2. En la segunda parte habrá botones con números del 0 al 9, el punto (`.`), las operaciones básicas (sumar, multiplicar, restar y dividir) y el botón C que resetea la calculadora. 3. En la parte inferior tendrá una barra que indique “Calculadora desarrollada por el Grupo CEJA – Udenar”. 4. La calculadora se debe poder operar con el mouse y con el teclado.

En este caso, ChatGPT-4o suministró el paso a paso de cómo realizar el trabajo planteado: (i) primero, solicitó que se instalaran ciertos componentes adicionales en la PC, y señaló la forma de hacerlo; (ii) luego, escribió el código fuente de la calculadora con los requerimientos solicitados; (iii) ese código fuente se copió y pegó en Visual Studio Code y se generó el archivo con la extensión `.py`; (iv) luego, ChatGPT suministró los pasos para convertir el archivo `.py` a un ejecutable `.exe`. El resultado fue el siguiente:



Figura 6. Calculadora programada con ayuda de ChatGPT



Una vez obtenido el resultado que se puede observar en la ilustración 6, se procedió a realizar las pruebas para testear que la calculadora efectivamente funcionara. Las pruebas fueron totalmente satisfactorias y los resultados, correctos.

Figura 7. Ejemplo de funcionamiento de la calculadora programa con ayuda de ChatGPT



Expectativas. Una calculadora no es suficiente

A estas alturas, el lector seguramente se preguntará: hasta el momento se ha demostrado la capacidad de una IA generativa, específicamente de ChatGPT-4o, para guiar a una persona o grupo de personas neófitas en el tema de programación, con la finalidad de desarrollar simples pruebas o pequeños programas. Al final, una calculadora es algo que se puede lograr más fácilmente ingresando a Google o al celular. ¿Cuál puede ser la utilidad de esto para el derecho?

La respuesta es fascinante, y es ahí donde radica la importancia de la idea del “abogado programador”. Si los abogados experimentaran más con la IA con la finalidad de programar, podrían, poco a poco, desarrollar aplicaciones mucho más complejas que resuelvan problemas específicos de la labor jurídica, programas que no están disponibles en el mercado y cuya producción podría resultar costosa. Las universidades y los investigadores podrían potenciar soluciones técnicas a menor coste para abogados y jueces.

Esto implica, necesariamente, que el abogado se aproxime a conocimientos más profundos de programación como, por ejemplo, vincular un Python con ChatGPT directamente, lo cual se puede lograr a través de la función API que ofrece OpenAI. El mismo ChatGPT puede guiar al usuario para conseguirlo, sin acudir a expertos en programación. La información la recoge el programa creado, pero la procesa ChatGPT que devuelve la respuesta al programa.

En cuanto a la Sentencia T-323/24 y los usos autorizados de la IA, a saber: gestión documental, apoyo a la función judicial y corrección de textos, son actividades que podrían desarrollarse por medio de la programación, con el auxilio de ChatGPT, de pequeños programas. Sería una forma ética y, en principio, sin mayores problemas de cara a derechos fundamentales o garantías básicas.

A continuación, se enumeran algunos posibles usos de esta forma de aplicar la IA en el derecho. Se trata, por supuesto, de un listado enunciativo, porque las posibilidades son infinitas:

- Construcción de programas que resuelvan tareas del derecho donde se vean aplicadas las matemáticas, como liquidaciones de crédito, tasaciones de perjuicios, indexación de sumas, etc.
- Sistemas de control de casos de una oficina o de un despacho, absolutamente personalizados con las variables que el abogado o juez específicamente requieran, y con la posibilidad de escalarlos en el futuro para incorporar más funciones.
- Sistemas de reparto interno de expedientes o tareas dentro de un despacho. Un programa con Python puede desarrollar fácilmente esta tarea y luego dejar en



claro, por ejemplo, quién tenía a su cargo un expediente y la fecha en que se hizo el reparto.

- Tareas de gestión documental y organización de documentos.
- Generación de documentos básicos en proforma. El usuario suministra la información básica y el programa devuelve el documento en borrador.
- Sistemas de conteo de horas de trabajo y facturación por cada uno de los integrantes del bufete.

Los riesgos

El abogado programador, finalmente, es mucho más abogado y mucho menos programador. Esta es una realidad de a puño que no se puede ni se debe desconocer. El neófito en programación, por ejemplo, debe ser consciente de que los programas desarrollados con auxilio de ChatGPT pueden tener vulnerabilidades que no ha contemplado. En este punto, el peligro es alimentar dichos programas con información sensible. Por eso se consideran varios riesgos que se deben tener en cuenta. A continuación, se desarrollan algunos.

- Riesgo de vulneración o hackeo: el uso de programas propios alimentados con información sensible puede generar un riesgo gigante en materia de seguridad informática. Al no ser programas diseñados por expertos, pueden ser fácilmente objeto de ataques y la información que ellos guarden quedaría expuesta. Para mitigar este riesgo, se recomienda ejecutar estos programas solo a nivel local, o en entornos de nube con acceso limitado, no deben abrirse a la web, puesto que esto permitiría ataques.
- Riesgo de pérdida de información: el programa podría fallar y la información suministrada podría borrarse, es importante tener en cuenta que son programas “hechos en casa” y que son susceptibles a fallos. Por ello, es altamente recomendable realizar copias o *back ups* de la información.
- Riesgo de bloqueo del programa: al no tener un fabricante conocido, algunos antivirus o los sistemas de protección podrían bloquear el programa, lo que haría difícil operarlo.
- Riesgo de falla: el programa podría funcionar bien por un tiempo, pero tras recibir grandes cantidades de información podría bloquearse o dejar de funcionar.
- Riesgo de sesgos implícitos o programación oculta: es posible que ChatGPT escriba el código fuente con alguna clase de sesgo o falla que el usuario, al no tener conocimientos profundos en programación, solo detecte cuando se ponga en marcha. Un buen ejemplo sería un programa que reparta el trabajo de una



oficina o despacho y que el código fuente de manera predeterminada sobrecargue a cierta persona frente a las demás.

Estos riesgos pueden mitigarse en mayor medida si el abogado puede, con el tiempo, ir accediendo a conocimientos más especializados en materia de programación. No sería raro que, en un futuro no muy lejano, este tipo de habilidades o competencias se empiecen a desarrollar desde muy temprano en la formación académica.

Conclusiones

En este capítulo se exploró, en primer lugar, el problema y los retos de la IA embebida, y se concluye que, ante una sociedad hipertecnológica, los cambios en el mundo tecnológico —como el advenimiento de la IA en las diferentes aplicaciones— sin duda afectan el entorno social que se sirve de las TIC. El derecho no escaparía a este fenómeno.

En segundo lugar, se exploró la histórica sentencia T-323/24 de la Corte Constitucional de Colombia, de la cual se rescataron los usos permitidos y no permitidos de la IA, específicamente de la IA generativa en la modalidad de grandes modelos de lenguaje (LLM).

En tercer lugar, partiendo de los usos autorizados por la T-323/24, se plantea que existen dos formas en las cuales el abogado se puede acercar a la IA: una, la tradicional, que consiste en que el jurista utiliza la IA para que esta desarrolle una función jurídica; en la segunda, propuesta en el documento, el abogado trata de ubicar los usos más específicos de la IA para darles una visión jurídica, es decir que el abogado sale del confort de dialogar con la IA en términos jurídicos, para proceder a tratar de interactuar con la IA en lenguaje informático. A esta segunda forma de aproximación se le otorgó el nombre de “abogado programador”.

El abogado programador se lanza a explorar terrenos que no conoce y se atreve a interactuar con la IA para que ella realice aquello para lo que sí está bien entrenada, como es la generación de código fuente, a diferencia de la construcción de textos legales para un ordenamiento jurídico específico. El abogado entonces acude a la IA para que desarrolle código fuente con el objetivo de generar aplicaciones que puedan solucionar problemas concretos de su cotidianidad profesional. Es una aproximación diferente, radical y mucho más compleja que la primera.

A través de ChatGPT-4o, con prompts y pruebas reales, se presentaron los pasos para que un abogado neófito en temas de programación pueda indagarle y pedirle a la IA que lo guíe por este complejo universo. El abogado se atreve a dialogar francamente con otros saberes, en este caso la programación, y se aproxima a ella a través de la IA.



Se demostró que la IA puede orientar la realización de sencillas pruebas de programación utilizando el lenguaje Python, editores de código, como Visual Studio Code, y herramientas en línea como Google Colab. Sin descartar otras versiones de IA, se observa que ChatGPT-4o puede guiar efectivamente a un usuario sin conocimientos en programación y desarrollar las primeras líneas de código fuente.

Se presentaron algunos posibles usos de esta nueva perspectiva, en la que el abogado se acerca a la IA no para que le brinde soluciones propias del saber jurídico, sino para que otorgue soluciones a partir de la programación y la creación de código fuente. De este modo, el usuario puede ser creativo y diseñar sus propios aplicativos personalizados, sencillos pero útiles, y que ayuden a automatizar problemas propios de la cotidianidad del abogado.

La principal conclusión es que el enfoque del “abogado programador” que accede a la IA en busca de soluciones tecnológicas aplicadas, en lugar de buscar soluciones jurídicas, puede ser un enfoque prometedor en la relación IA y derecho. En este campo, como en toda programación, los límites son la imaginación humana y su capacidad de utilizar la IA para guiar la construcción de soluciones tecnológicas específicas.

Si la IA se va a comer al software —como empezó este escrito— vale la pena que el abogado comprenda las razones de dicha afirmación y se inserte en las nuevas realidades que permiten, en un futuro no muy lejano, que cada persona diseñe sus propios aplicativos a la medida.

Referencias

- Bugallo Montaña, B. (2023). Prompts de la Inteligencia Artificial Generativa y su posible protección por la propiedad intelectual. *Revista Rede de Direito Digital, Intelectual & Sociedade*, 3(6), 125-163. https://gedai.ufpr.br/wp-content/uploads/2024/04/Revista-RRDDIS_vol-3-n-6_2023-1.pdf#page=125
- Cárdenas Caycedo, O. (2023). Las nuevas tecnologías y decisión judicial en Colombia: entre el mensaje de datos y la Inteligencia Artificial. En I. C. de Derecho Procesal, *Sostenibilidad y proceso XLIV Congreso Colombiano de Derecho Procesal* (pp. 827-861). Bogotá: Instituto Colombiano de Derecho Procesal - Universidad Libre.
- CNN en español. (24 de julio de 2024). Qué es Meta AI en WhatsApp cómo usarla y cómo desactivarla. *CNN*. <https://cnnespanol.cnn.com/2024/07/24/que-es-meta-ai-whatsapp-como-usarlo-como-desactivarla-orix/>
- Cordón García, O. (2023). Inteligencia artificial en educación superior: oportunidades y riesgos. *RiiTE Revista interuniversitaria de investigación en Tecnología Educativa*, (15), 16-27. doi: <https://doi.org/10.6018/riite.591581>
- Corte Constitucional de Colombia, Sentencia T-323. (2 de agosto de 2024).



- León García, N. M. (septiembre de 2023). *Pasantía en la corte constitucional: contribución al análisis de datos y depuración de accionados en python*. Informe de pasantía. <http://hdl.handle.net/11349/39423>
- Maya Gualtieri, M. R. (2023). Los sistemas de chat basado en IA. *Cuadernos UCAB*, (21), 6-29. <https://revistasenlinea.saber.ucab.edu.ve/index.php/cuadernosucab/article/view/6361>
- Microsoft Centro de Noticias. (15 de marzo de 2024). *Microsoft expande Copilot a todo el mundo*. <https://news.microsoft.com/es-es/2024/03/15/microsoft-expande-copilot-a-todo-el-mundo/>
- Misseri, L. (2023). Autoría e inteligencia artificial generativa: presupuestos filosóficos de la función del autor. *Isonomía - Revista de Teoría y Filosofía del Derecho*, (59), 229-255. doi: <https://doi.org/10.5347/isonomia.59/2023.692>
- Nieva Fenoll, J. (2018). *Inteligencia Artificial y proceso judicial*. Madrid: Marcial Pons.
- Pulido, M. d. (2020). La incidencia de las nuevas tecnologías en el debido proceso. *Ius et scientia*, 6(2), 186-199. <https://doi.org/10.12795/IETSCIENTIA.2020.i02.12>
- Radanliev, P. (2024). Artificial intelligence: reflecting on the past and looking towards the next paradigm shift. *Journal of Experimental & Theoretical Artificial Intelligenc*, 1-18. doi: <https://doi.org/10.1080/0952813X.2024.2323042>
- Ramírez Autrán, R. (2023). Sesgos y discriminaciones sociales de los algoritmos en Inteligencia Artificial. *Entretextos*, 15(39). <https://dialnet.unirioja.es/servlet/articulo?codigo=9380872>
- Sadin, E. (2018). *La silicolonización del mundo. La irresistible expansión del liberalismo digital*. Buenos Aires: Caja negra editores.
- Sadin, E. (2020). *La inteligencia artificial o el desafío del siglo. Anatomía de un antihumanismo radical*. Buenos Aires: Caja negra editores.
- Simonite, T. (12 de mayo de 2017). Nvidia CEO: Software Is Eating the World, but AI Is Going to Eat Software. *MIT Technology Review*. <https://www.technologyreview.com/2017/05/12/151722/nvidia-ceo-software-is-eating-the-world-but-ai-is-going-to-eat-software/>



Acerca de los autores

Federico M. Álvarez Larrondo (Argentina). Doctor en Derecho, tesis cum laude. Coordinador del “Grupo de Expertos sobre Inteligencia Artificial” de la Universidad Nacional de Mar del Plata. Profesor titular regular de “Inteligencia Artificial, Tecnología y Derecho”, materia obligatoria para los y las estudiantes de Derecho de la Universidad Nacional de Mar del Plata (UNMDP). Profesor titular del curso “Derecho Artificial”, materia obligatoria para los y las estudiantes de Derecho de la Universidad Atlántida Argentina. Profesor adjunto de la cátedra “Sociedades, Seguros y Bancos” (UNMDP). Expresidente y árbitro permanente del Tribunal Arbitral del Colegio de Abogados de Mar del Plata. Autor de la obra “Entendiendo al bitcoin y sus desafíos jurídicos y sociales” (Ed. La Ley, 2022) y “IA ¿amenaza o solución? (Ed. El Ateneo, 2025). ORCID <https://orcid.org/0009-0002-0998-6155> Correo: federicoalarrondo@gmail.com

Juan Fernando Gil Osorio (Colombia). Candidato a doctor en Derecho, Universidad Externado de Colombia. Magíster en Derechos Humanos y Democratización, Universidad Externado de Colombia y Universidad Carlos III de Madrid. Abogado, Universidad de Medellín. Investigador Junior reconocido y categorizado por Minciencias. Par académico del Consejo Nacional de Acreditación (CNA). Miembro de la Academia Colombiana de Derecho Internacional. Contacto: juanfgo1102@gmail.com – Código ORCID: <https://orcid.org/0000-0002-6605-6846>

Jonnathan Jiménez Reina (Colombia). Candidato a doctor en Seguridad Internacional, Universidad Nacional de Educación a Distancia. Magíster en Seguridad y Defensa Nacionales y magíster en Derechos Humanos y Derecho Internacional de los Conflictos Armados, Escuela Superior de Guerra General Rafael Reyes Prieto. Profesional en Política y Relaciones Internacionales, Universidad Sergio Arboleda. Investigador asociado reconocido y categorizado en MinCiencias. Contacto: jonnathan.jimenez008@gmail.com – Código ORCID: <https://orcid.org/0000-0001-9042-834X>

Camilo Alberto Vargas Cano (Colombia). Magíster en Gerencia Estratégica del Talento Humano, Universidad Sergio Arboleda. Magíster en Contratación Estatal, Universidad de Medellín. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra. Máster en Alta Dirección Empresarial, Universidad Francisco de Vitoria. Abogado, Universidad Antonio Nariño. Administrador de Empresas, Universidad Politécnico Gran Colombiano. Profesional en Ciencias Militares, Escuela Militar



de Cadetes General José María Córdova. Contacto: camivar12@yahoo.com – Código ORCID: <https://orcid.org/0000-0001-9037-6455>

Sebastián Heredia Querro (Argentina). Abogado Universidad Católica de Córdoba (UCC). Magíster en Derecho Empresario, Universidad Austral. Magíster en Finanzas, ESADE. Certificado Program for Management Development - ESADE Business & Law School (España). Especialista en Corporate Finance & Law, de Magíster en Finanzas con orientación Fintech. Egresado de la primera cohorte de la Blockchain Summer School en la Universidad de Utrecht, Holanda. Director de la Sala de Derecho y Tecnología del Colegio de Abogados de Córdoba. Es emprendedor tecnológico, co-fundador y Co-CEO de Wootic, una compañía de servicios LegalFinTech y de desarrollo de software enfocada en DLTs & Machine Learning. Es Co-Coordinador del Grupo de Trabajo Legal (GTL) Argentina de LACChain, la red híbrida de blockchain de BIDLab. Contacto: sebastianherediaquerro@gmail.com

Juan Esteban Aguirre Espinosa (Colombia). Abogado de la Universidad de San Buenaventura Seccional Medellín, especialista en Derecho Tributario Internacional en la Universidad Externado de Colombia, magíster en Ciencias Políticas y magíster en Derecho de la Universidad Católica Luis Amigó. Doctorando en Derecho Procesal Contemporáneo de la Universidad de Medellín. Decano de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Luis Amigó. Ponente y conferencista Internacional. Investigador adscrito al Grupo de Investigaciones Jurídicas y Sociales, reconocido en A por Minciencias. Google académico: <https://scholar.google.com.co/citations?user=9QD3rjkAAAAJ&hl=es>; ORCID: <https://orcid.org/0000-0001-9012-9585> Contacto: aguirreepinosaesteban@gmail.com

Dany Steven Gómez Agudelo (Colombia). Abogado y magíster en Derecho de la Universidad Católica Luis Amigó. Especialista en Derecho Administrativo de la Universidad de Antioquia. Especialista en Contratación Estatal de la Universidad Autónoma Latinoamericana. Conjuez del Tribunal Administrativo de Antioquia, Colombia. Docente de Derecho Administrativo General, Derecho Procesal Administrativo, Derecho Informático y nuevas tecnologías, y docente del semillero de investigación en Ciencia y Derecho de la Universidad Católica Luis Amigó. Líder del Grupo de Investigaciones Jurídicas y Sociales, reconocido en A por Minciencias. Google Académico: <https://scholar.google.com/citations?user=YaysRIIAAAAAJ&hl=es>; ORCID: <https://orcid.org/0000-0003-2687-0146>. Contacto: dany.gomezag@amigo.edu.co // dany-gomezagudelo@hotmail.com

Sebastián Díaz Bolívar (Colombia). Abogado, magíster en Derecho Procesal Contemporáneo y doctorando en Derecho Procesal Contemporáneo de la



Universidad de Medellín. Coordinador del área de derecho privado civil II del Programa de Derecho de la Universidad Católica Luis Amigó. Miembro del Grupo de Investigaciones Jurídicas y Sociales, categoría A en Minciencias, de la Universidad Católica Luis Amigó, Medellín, Colombia. Google Académico: <https://scholar.google.es/citations?user=UqM-KlcAAAAJ&hl=es>; ORCID: <https://orcid.org/0000-0001-7314-6412>. Contacto: sebastian.diazbo@amigo.edu.co

Daniel Betancur Vásquez (Colombia). Docente tiempo completo ocasional Institución Universitaria de Envigado. Ingeniero Mecatrónico, Maestría en Automatización y Control Industrial con énfasis en Inteligencia Artificial. Google Académico: <https://scholar.google.com/citations?user=cAlPiKYAAAAJ&hl=es> Correo: dbetancurv@correo.iue.edu.co

Daniel Carmona Cardona (Colombia). Abogado Institución Universitaria de Envigado. Master en Derecho Constitucional y Doctor en Filosofía Universidad de Sevilla. Correo: dcarmonaca@correo.iue.edu.co

Edwin Alexander Moncada (Colombia). Docente tiempo completo ocasional Institución Universitaria de Envigado. Tecnólogo Químico, Ingeniero de Alimentos, MBA Inteligencia de Negocios y Big Data (c), Doctor en Química con énfasis en polímeros y nanomateriales. Google Académico: <https://scholar.google.es/citations?user=Nm-V7AiWAAAAJ&hl=es> Correo: eamoncadaa@correo.iue.edu.co

Débora Guerra Moreno (Colombia). Doctora en Derecho Procesal Contemporáneo de la Universidad de Medellín, doctora en Administración, Hacienda y Justicia en el Estado Social de la Universidad de Salamanca, magíster en Responsabilidad contractual y extracontractual civil y del Estado de la Universidad Externado de Colombia y magíster en Administración de la Universidad Argentina de la Empresa. Integrante del Grupo de Investigación en Derecho Público de la Universidad Libre de Cúcuta. Contacto: deboraguerramoreno@hotmail.com, ORCID ID: <https://orcid.org/0000-0003-1087-1945>

Darwin Clavijo Cáceres (Colombia). Doctor en Administración, Hacienda y Justicia en el Estado Social, magíster en Educación y Especialista en Docencia Universitaria y en Derecho Administrativo. Miembro del Grupo de Investigación en Derecho Público de la Universidad Libre. Contacto: darwing.clavijoc@unilibrecucuta.edu.co. ORCID ID: <https://orcid.org/0000-0001-9914-1265>

Omar Alfonso Cárdenas Caycedo (Colombia). Abogado de la Universidad de Nariño. Doctor en Derecho Cum Laude de la Universidad Carlos III de Madrid, magíster en Derecho Comercial y especialista en Derecho Procesal Civil de la Universidad Exter-



nado de Colombia. Profesor de la Universidad de Nariño, investigador asociado ante Minciencias y líder del grupo de investigación CEJA Categoría B de la Universidad de Nariño. Miembro del Instituto Colombiano de Derecho Procesal. Profesor invitado a posgrados y cursos de la Universidad Nacional de Colombia, Universidad Libre de Cúcuta, Universidad de Medellín, Universidad Autónoma de Bucaramanga y Universidad de Catamarca (Argentina). ORCID <https://orcid.org/0000-0002-7987-8785> Google Académico: <https://scholar.google.com/citations?user=sdS5-8gAAAAJ&hl=es> Contacto: omarcardenas@udenar.edu.co

Reseña Coordinadoras Académicas del Libro

Adriana de Pilar Henao Ochoa. Docente tiempo completo ocasional de la Institución Universitaria de Envigado. Miembro de la Red para el Estudio del Proceso y la Justicia. Abogada, Magíster en Derecho procesal (Universidad de Medellín), Especialista en Derecho Comercial (Universidad Pontificia Bolivariana) Master en Derecho de Familia (Universidad Autónoma de Barcelona). Conciliadora. ORCID ID: <https://orcid.org/0000-0003-1529-7364> Correo electrónico: a.henao.ochoa@gmail.com / aphenao@correo.iue.edu.co

Diana María Ramírez Carvajal. Coordinadora de la Red para el Estudio del Proceso y la Justicia. Magíster en Derecho Procesal de la Universidad de Medellín y Doctora en Derecho de la Universidad Externado de Colombia. Miembro de la Asociación Internacional de Derecho Procesal y del Instituto Iberoamericano de Derecho Procesal. ORCID ID: <https://orcid.org/0000-0001-7833-1393>, Correo electrónico: radiana2113@gmail.com.



Esta obra colectiva reúne una serie de capítulos que son el resultado de investigaciones académicas desarrolladas por sus autores en torno a los vínculos entre tecnología, derecho y justicia. La mayoría de los estudios adoptan un enfoque cualitativo descriptivo, mientras que otros emplean metodologías cuantitativas, lo que permite una mirada plural y enriquecedora sobre los fenómenos emergentes en esta intersección.

El texto se presenta como una invitación a repensar los paradigmas tradicionales del derecho en el contexto de la revolución digital, destacando la necesidad de enfoques interdisciplinarios y colaborativos. La articulación entre disciplinas como la ingeniería, la informática y el derecho se plantea como un camino necesario para la innovación jurídica y la transformación de los sistemas de justicia.

Bajo el título *Convergencias de la Tecnología y la Justicia*, la obra parte de la premisa de que la justicia constituye un pilar fundamental de las sociedades democráticas. En este marco, tecnologías emergentes como blockchain y la inteligencia artificial (IA) están redefiniendo los procesos judiciales y administrativos, el acceso a la justicia, la protección de los derechos fundamentales y los dilemas éticos asociados a la toma de decisiones automatizadas.