TECNOLOGÍAS EMERGENTES

QUÉ SON Y CÓMO APROVECHARLAS EN LAS INDUSTRIAS CREATIVAS Y CULTURALES

UNESCO
Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

CERLALC
Centro Regional para el Fomento del Libro en América Latina y el Caribe
Bajo los auspicios de la UNESCO

UNIVERSIDAD AUTÓNOMA DE CHILE
MÁS UNIVERSIDAD

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
Organização das Nações Unidas para a Educação, a Ciência e a Cultura

CERLALC
Centro Regional para el Fomento del Libro en América Latina y el Caribe
Bajo los auspicios de la UNESCO
Centro Regional para o Fomento do Livro na América Latina e o Caribe
Sob os auspícios da UNESCO

UNIVERSIDAD AUTONOMA DE CHILE
MÁS UNIVERSIDAD

Coeditado por el
Centro Regional para el Fomento del Libro en América Latina y el Caribe, Cerlalc
Universidad Autónoma de Chile

Coordinación editorial
Michelle Azuaje Pirela
Fredy Adolfo Forero Villa

Autores
Paula Amaya Villegas
María José Arancibia Obrador
Michelle Azuaje-Pirela
Francisco Bedecarratz Scholz
Sebastián Bozzo Hauri
Betty Martínez-Cárdenas
Roberto Navarro
Juan Carlos Salazar Camargo
Sebastián Sánchez Polanco
Felipe Osorio Umaña
Pablo Viollier Bonvin

Colaboradores
Zhiying Gao Feng
José Ignacio Nambrard Ramírez
Eduardo Salazar Ríos
Isidora Sesnic Humeres
Juan Ignacio Contardo González

Diseño de portada
Diana Carolina Martínez

Diseño y diagramación
Juan Galvis

Fotografías
Pexels

Guía

¿QUÉ SON Y CÓMO APROVECHAR LAS TECNOLOGÍAS EMERGENTES EN LAS INDUSTRIAS CREATIVAS Y CULTURALES?

UNESCO
Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

Organização das Nações Unidas para a Educação, a Ciência e a Cultura

CERLALC
Centro Regional para el Fomento del Libro en América Latina y el Caribe
Bajo los auspicios de la UNESCO

Centro Regional para o Fomento do Livro na América Latina e o Caribe
Sob os auspícios da UNESCO

DUC IN ALTUM
UA
UNIVERSIDAD AUTONOMA DE CHILE
MÁS UNIVERSIDAD

Agradecimientos

Esta guía cuenta con el apoyo de los siguientes proyectos financiados por la Agencia Nacional de Investigación y Desarrollo de Chile: i) Fondecyt de Posdoctorado N° 3210519 titulado «Transparencia algorítmica y propiedad intelectual: Propuestas para Chile»; ii) Fondecyt de Iniciación N° 11220494, titulado: "Estudio y propuesta sobre la mediación online en derecho de consumo como forma de acceso a la justicia en Chile"; y, iii) Fondecyt Regular N° 1220735, titulado: Digitalización y algoritmos en la solución de conflictos en materia de consumo en Chile. Propuestas de mejora al acceso a la Justicia de los consumidores a la luz de los sistemas comparados".

También cuenta con la colaboración del Proyecto de investigación «La responsabilidad de la inteligencia artificial: un desafío para las ciencias penales» (PID2020-112637RB-I00), financiado por el Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia, Subprograma Estatal de Generación de Conocimiento, del Ministerio de Economía y Competitividad, España.

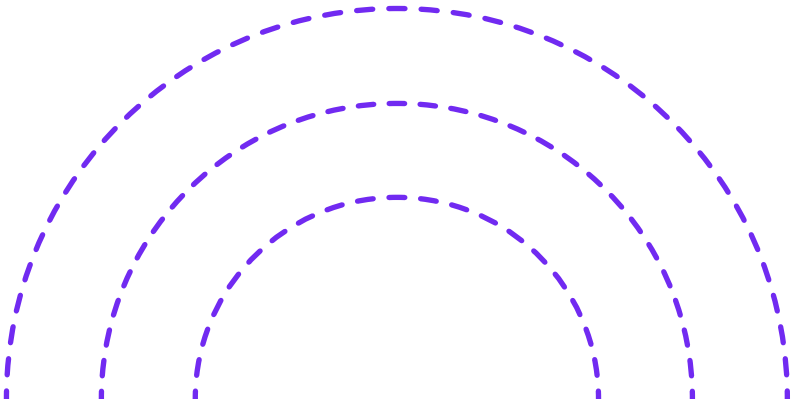
Finalmente, los autores y editores quieren agradecer expresamente a Zhiying Gao Feng, José Ignacio Nambrard Ramírez, Eduardo Salazar Ríos, Isidora Sesnic Humeres y Juan Ignacio Contardo González por su apoyo en la revisión y corrección de esta guía.

Sección 1

¿QUÉ SON LAS TECNOLOGÍAS EMERGENTES?

¿CÓMO IMPACTAN EN EL SECTOR CREATIVO Y CULTURAL?

Michelle Azuaje Pirela



Introducción

En esta sección te ofrecemos un breve panorama general del contenido de nuestra guía a partir de la explicación de lo que son las tecnologías emergentes y cuál es su impacto específico en el sector creativo y cultural. Para ello, en primer lugar, aproximaremos una definición a los términos "tecnologías emergentes", "tecnologías disruptivas" y "tecnologías digitales emergentes". En segundo lugar, explicaremos a través de ejemplos en qué consisten las tecnologías que hemos seleccionado para esta guía y cómo se relacionan con el sector creativo y cultural. Y finalizaremos con una breve explicación de algunas formas en las que dichas tecnologías pueden ayudar a generar nuevas oportunidades en el sector creativo y cultural, así como algunos riesgos asociados.

¿Qué son las tecnologías emergentes?

A principios de este siglo comenzó la que ha sido llamada la "Cuarta Revolución Industrial". Una revolución digital que se caracteriza por la cobertura de internet en los lugares más recónditos del planeta, por sensores y dispositivos cada vez más versátiles, pequeños y potentes que, a su vez, son cada vez más baratos e inteligentes, y por tecnologías cada vez más sofisticadas, integradas y extendidas que se difunden rápidamente y están transformando las sociedades y la economía mundial. Son la fusión de estas tecnologías y su interacción a través de los dominios físicos, digitales y biológicos las que hacen que se trate de una revolución fundamentalmente diferente de las anteriores (Schwab, 2016).

Para entenderlo, deténgase por un momento a pensar en cómo ha cambiado nuestra vida con la digitalización en los últimos años. Podemos deducir que, por ejemplo, hasta hace unas pocas décadas, para tener un hermoso álbum de fotografías familiares había que comprar una cámara, los respectivos "rollos" o "carretes", y luego llevar las fotos que se tomaron a un estudio fotográfico para que, al cabo de unos días, estuvieran reveladas e impresas.

Si lo anterior no le resulta familiar: ¿era usted uno de esos que esperaba impaciente la guía de programación de TV por cable para escoger y agendar los estrenos cinematográficos del mes? ¿Recuerda la guía telefónica? O ¿era de los que hacían interminables filas para comprar los boletos de un concierto?

Hoy en día, aunque de algún modo siguen existiendo dichos procesos —para muchas personas "exóticos" o "desconocidos"—, solo basta con tener un teléfono celular con cámara integrada y alguna *red social* o *plataforma* para compartir las fotos de manera digital; la programación de TV puede verla en el canal o en el sitio web de su proveedor e incluso en el catálogo digital de su servicio de *streaming* que, además, es capaz de recomendarle algunos contenidos con base a sus gustos y preferencias (Netflix, Disney+, Amazon Prime, Hulu, HBO Max, entre otros); los números de teléfono puede guardarlos en el directorio de su celular o buscarlos en *Google*, y los boletos para el concierto los puede adquirir a través de aplicaciones o páginas web de sus organizadores.

Nuestra vida ha cambiado gracias a la digitalización, el internet y la evolución de diversas tecnologías, algunas de ellas "emergentes". En la actualidad, no existe consenso para una definición única que pueda explicar lo que son las "tecnologías emergentes". No obstante, según diversos criterios, dicho término hace referencia a varios grupos de tecnologías. Algunos de ellos ponen el énfasis en tecnologías e innovaciones que provocan cambios radicales en los negocios, la industria o la sociedad. En ese sentido, no son necesariamente nuevas, pero su impacto suele ser distinto debido al nivel de avance y desarrollo que tenga cada lugar.

Otras definiciones utilizan el concepto de "*tecnologías emergentes*" para identificar a todas aquellas que se están desarrollando actualmente o se desarrollarán desde los próximos cinco a diez años, y que de una u otra forma están rodeadas de cierto grado de incertidumbre. Por tanto, una tecnología puede ser considerada emergente por su novedad, pero también por su impacto socioeconómico previsto (Rotolo, Hicks & Martin, 2015).

Lo interesante es que, tal como se expuso en los ejemplos mencionados anteriormente, estas tecnologías tienen el potencial de alterar aspectos fundamentales de la forma en que entendemos nuestra sociedad, nuestras costumbres,

cómo nos relacionamos y comunicamos, y, especialmente, la forma en que las empresas ponen a nuestra disposición una serie de productos y servicios con diversos alcances e impactos que más adelante mencionaremos. Asimismo, ese potencial que tienen para generar cambios profundos en nuestra sociedad también hace que muchas veces se les llame disruptivas, porque intentan mejorar, de forma inesperada y diferente, los productos y servicios que ya existen (Dosi, 1982; Christensen, 1995, 1997; Fernández y Valle, 2018).

En el contexto de nuestra guía nos referiremos especialmente a las "tecnologías digitales emergentes", esas que, además de tener las características antes descritas, se encuentran en el mundo digital y han llegado para cambiar varios aspectos de nuestra vida en los últimos años. Hasta la fecha, aunque no siempre queda claro cuántas y cuáles existen, podemos encontrar: la Inteligencia Artificial (IA), Internet de las cosas (*IoT*), Internet de los servicios (*IoS*), Internet de los cuerpos (*IoB*) y *Blockchain*, las cuales son vistas como algunas de las principales tecnologías en las que se basa la Cuarta Revolución Industrial, la nueva economía digital y la innovación basada en datos. No obstante, existen algunas que, aunque no consideraremos en esta guía, están estrechamente relacionadas con el sector creativo y cultural, tales como las identidades digitales, la biotecnología, robótica, la impresión 3D/4D, computación cuántica, el 5G, entre otras.

¿Cómo se relacionan las tecnologías digitales emergentes con el sector creativo?

Como veremos en las próximas secciones de nuestra guía, si bien las tecnologías digitales emergentes han impactado en muchas actividades de la vida de los seres humanos, también han incidido en el sector creativo y cultural, entre otras cosas, porque ofrecen nuevas posibilidades de interactuar, crear, difundir, comercializar y consumir lo creado. Veamos algunos ejemplos.

a) Inteligencia artificial

En términos generales, la inteligencia artificial se refiere a la ciencia y la ingeniería de fabricar máquinas inteligentes, esto es, máquinas y sistemas que imitan ciertas tareas que requerirían de inteligencia si fueran realizadas por seres humanos (McCarthy, 2007).

La IA es la tecnología encargada de que los contenidos de *streaming* puedan llegar de manera más efectiva al público interesado. Esto es posible gracias a un subcampo específico llamado *machine learning* o aprendizaje automático, que toma como base las preferencias de los usuarios para analizarlas, filtrarlas y categorizarlas, a través del software, con el fin de recomendar contenidos adaptados de manera específica a los usuarios. Pero como la IA es una tecnología de múltiple propósito, también sirve como herramienta para la producción o realización de tareas complejas en el ámbito industrial, financiero, comercial, educativo, salud, traducciones, etcétera.

Es importante destacar que, incluso en el sector creativo y cultural, también se utiliza para escribir, componer música, crear sonidos instrumentales, podcasts, códigos de software, imágenes, videos y juegos a bajo costo. Fíjese, por ejemplo, en la siguiente imagen que hemos llamado *The new Pablo Picasso* (El nuevo Pablo Picasso). Esta ha sido creada especialmente para esta guía con fines académicos, de investigación e ilustración, utilizando el software de CRAIYON.COM. Para lograr el resultado que vamos a ver, escribimos el *prompt* (solicitud o requerimiento): *The new Pablo Picasso*, digital art y, al cabo de dos minutos, obtuvimos esta imagen en la que puede verse cómo un sistema de IA es capaz de imitar el estilo y talento del gran pintor y escultor español Pablo Picasso.

Imagen generada en agosto de 2022, a través de licencia comercial gratuita de CRAIYON.COM.

Resultados impresionantes, como el anterior, hacen que hoy en día se cuestione si seremos capaces de distinguir el trabajo creativo humano de los productos generados por las máquinas. Y también que nos preguntemos ¿Qué debemos hacer con este tipo de productos? ¿Debemos protegerlos jurídicamente? ¿A quién atribuimos algún eventual derecho? ¿Debemos garantizar que existan leyes que los protejan y remuneren? ¿Cómo lo hacemos?

Para este caso, según se describe en la licencia comercial gratuita de Craiyon que hemos utilizado, las imágenes generadas pueden emplearse gratuitamente si son para uso personal o para fines académicos o de investigación, para educar o entretener en diversas plataformas de medios sociales. Sin embargo, en dicha licencia también se establece la posibilidad de utilizar las imágenes generadas con el fin de obtener ganancias financieras, siempre y cuando se cumpla con ciertas condiciones, entre las que se destacan: (1) que se pague una regalía del 20% sobre cualquier ingreso atribuible a cualquier transacción de *blockchain* (como la venta de un NFT), y (2) que pueda revocarse su derecho a utilizar el sitio o las imágenes en cualquier momento[1]. Como se ve, esta última posibilidad abre la puerta a diversos usos que permitirían, bajo ciertas condiciones, generar ingresos económicos sin que, en principio, se requiera de ningún tipo de inversión para generar las imágenes.

b) *Blockchain*, *NTs* y contratos inteligentes

De forma similar a lo que ha ocurrido con la IA, el *blockchain* tiene un gran potencial para transformar diversos campos de la sociedad actual, que va más allá de su origen: el sector financiero. En términos sencillos, la idea detrás del *blockchain* o cadena de bloques implica la existencia de una red de servidores interconectados de forma descentralizada, es decir, localizados en diferentes lugares del mundo, que cooperan simultáneamente para registrar, de forma digital, una copia exacta de la información añadida en dicha cadena (Granados, 2022, p. 20).

Como veremos en las próximas secciones de esta guía, algunas de sus características hacen que cada vez se hable

1 Para ver el detalle de la licencia y el resto de los requisitos pueden revisar los términos y condiciones de las licencias gratuitas comerciales en: https://www.craiyon.com/terms

más de sus potencialidades, especialmente por las oportunidades que ofrece para mejorar la gestión, trazabilidad y protección de los activos intangibles, y, por tanto, mejorar el sistema de propiedad intelectual en el mundo digital. En ese sentido, hay un especial interés en su potencial para cambiar el nivel de control que los artistas tienen sobre su trabajo y en el hecho de que su combinación con los contratos inteligentes y los NFTs puede facilitar la programación y recolección de los derechos de propiedad intelectual y regalías por el uso de productos digitales.

Los contratos inteligentes o *smart contract*s son programas de ordenador o acuerdos escritos en códigos computacionales, almacenados en el *blockchain*, que se ejecutan cuando se cumplen las condiciones predeterminadas. Por tanto, ofrecen nuevas alternativas para combatir los problemas del mundo digital, que son especialmente atractivas para la gestión y administración del derecho de autor. Esta tecnología es tan disruptiva que podría sustituir por completo a los sistemas tradicionales (Fink & Moscon, 2019, p. 78).

Para entenderlo, piense que los contratos inteligentes posibilitan establecer y hacer cumplir acuerdos de forma automatizada; por ejemplo: licencias o facilitar la transferencia de pagos en tiempo real a los titulares de los derechos por el uso de sus obras en el mundo digital, simplificando de este modo el comercio digital.

Además, esta tecnología puede utilizarse para evitar viejos problemas y ofrecer nuevas oportunidades y experiencias atractivas para los nativos digitales. Por ejemplo, en el sector editorial, los NFTs o tokens no fungibles (de los que hablaremos con detalle más adelante) se ofrecen como nuevas formas para ampliar las ventas de libros. Según se reseña en el sitio web de *PageDAO*, está diseñada para "ser una red descentralizada que busca: proporcionar una plataforma de publicación más racionalizada que reduzca al mínimo los costes para autores y editores"[2]. Detrás de ella está la idea de que los autores puedan autopublicarse en formato NFT. Esto permitirá no solo reducir los costos sino, además, por una parte, leer la historia y escuchar el sonido de la escena al mismo tiempo u ofrecer otras experiencias interactivas que no ofrecen los libros electrónicos tradicionales. Finalmente,

2 Al respecto, puede visitarse su sitio web: https://pagedao.org/docs/whitepaper/overview

también sirve para simplificar las licencias (Granados, 2022, pp.83-86), así como seguir la distribución de los contenidos digitales en tiempo real, verificar las autorizaciones y permitir determinados usos.

c) Realidad virtual y metaverso

Recientemente, otras tecnologías como la realidad virtual y los metaversos ofrecen nuevos medios de trabajo para los creadores. En ese sentido, el término "metaverso" se refiere a una especie de mundo virtual en el que, a través del uso de diversos dispositivos de realidad virtual y realidad aumentada, se busca una experiencia inmersiva e interactiva que dé la sensación de que estamos realmente dentro de él.

Aunque, como veremos, ni la realidad virtual ni el metaverso son conceptos estrictamente nuevos; no obstante, lo que sí resulta novedoso es la apuesta de grandes empresas tecnológicas (como Facebook-Meta-, Google, Nvidia y Microsoft) por impulsarlos. En ese sentido, la gran apuesta de Facebook es que el metaverso se convierta en un espacio en el que se generen tantas oportunidades de negocios e interacciones como en el mundo físico. Así, los metaversos ofrecen la posibilidad de generar nuevas dinámicas para, por ejemplo, asistir a conciertos, exhibir obras, realizar compras, entre otras oportunidades de recreación, inversión e interacciones que conviene analizar. Por ejemplo, Sonidos Inmersivos[3] es una startup chilena que, a través de *Otherland Music*, acerca el metaverso a la industria de la música para disfrutar conciertos en directo desde el computador.

¿Cómo pueden ayudar estas tecnologías a generar nuevas oportunidades en el sector creativo y cultural? ¿Existen algunos riesgos asociados?

Las tecnologías digitales emergentes están transformando diversas facetas de las industrias creativas y culturales, especialmente porque han cambiado y se espera que sigan cambiando la forma en que se produce, protege y consume

3 Al respecto, puede visitarse su sitio web: https://www.sonidosinmersivos.cl/

el contenido. Todo esto debido a que tienen el potencial de ofrecer herramientas para la creación de nuevos productos y servicios que bien aprovechados pueden crear nuevas fuentes de ingresos económicos, potenciar la experiencia de los usuarios y contribuir con el mejoramiento de la calidad de vida de las personas.

Aunque varias de estas tecnologías existen desde antes de la pandemia del COVID-19, esta aceleró los procesos de transformación digital en diversas áreas. Muchas empresas que lograron mantenerse —e incluso crecer— en los últimos tres años están relacionadas con el sector tecnológico, por eso se espera que la tecnología, después de la crisis generada por la pandemia, sea una aliada que ayude a consolidar negocios, productos y servicios digitales más dinámicos, eficientes y capaces de resistir futuras dificultades.

Las tecnologías digitales son y seguirán siendo importantes en el futuro próximo, entre otras cosas porque, como hemos visto, aportan valor añadido a las experiencias de los usuarios. De ahí que convenga aprovechar las nuevas y variadas oportunidades que ella ofrece en tiempos tan desafiantes como los que vivimos.

Ahora bien, sacar el máximo provecho de estas oportunidades requiere reflexionar y entender las implicaciones del carácter emergente que las rodea, el cual hace que muchas veces no estén del todo claros o se malinterpreten los límites de los usos que pueden o deben darse. En ese sentido, si pensamos en que hoy en día podemos ser usuarios de la tecnología (en tanto que consumidores de ella) y también generadores de nuevos productos y servicios en el entorno digital, podremos comprender que en dicho entorno existen también derechos y obligaciones.

Así, como veremos a lo largo de nuestra guía, es importante tener presente que, en uno u otro caso, el aprovechamiento de las tecnologías debe alinearse siempre con el respeto y la protección de los derechos e intereses, los cuales no dejan de estar presentes en el mundo digital, de las demás personas y el medio ambiente.

En el mundo digital existen áreas en las que debemos ser especialmente cuidadosos, no solo porque existen nuevas categorías de derechos pensados para él (la autodeterminación informativa o a la protección de datos personales), sino además porque existen nuevos riesgos (los relacionados

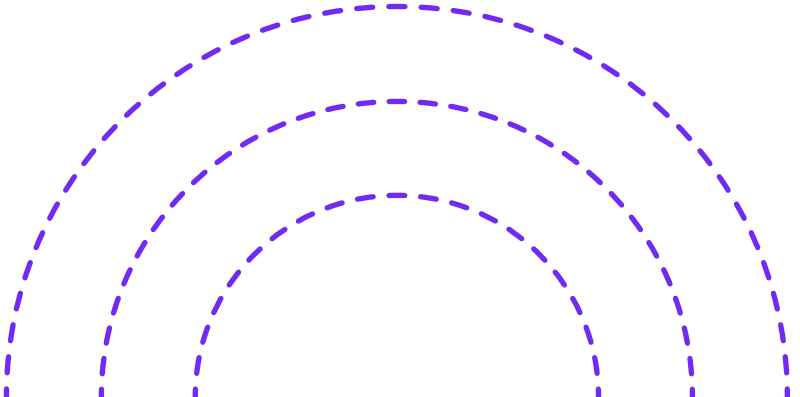
con los ciberataques). Esto se relaciona, por ejemplo, con la información de carácter personal que es necesario captar, almacenar y tratar en las interacciones con los consumidores y con terceros que tienen acceso a nuestros productos y servicios a través de canales y aplicaciones digitales. Mucha de esta información, como veremos en la sección correspondiente, puede tener el carácter de dato personal o incluso de dato sensible, por lo que debe ser cuidadosamente tratada para no vulnerar ningún tipo de derechos. Además, desde otro punto de vista, debemos ser igualmente cuidadosos y conscientes del valor de nuestra propia información (personal y empresarial) y la protección específica de ella para evitar ser víctimas de posibles ataques informáticos.

En ese sentido, tal como su título sugiere, las próximas secciones de nuestra guía están dirigidas de forma especial al sector creativo y cultural, a quienes se pretende ofrecer orientación sobre qué son las tecnologías emergentes y cómo pueden aprovecharse en este sector. Así, queremos promover la generación de valor a través de la creación de nuevos y mejores productos y servicios por medio del uso y adopción de herramientas digitales. En ese sentido, esperamos brindar orientaciones que faciliten la detección de oportunidades para el uso de tecnologías actuales o futuras, teniendo en cuenta los riesgos y oportunidades, con el fin de ser eficientes, seguros y respetuosos de los derechos y libertades fundamentales.

Sección 2

LA IRRUPCIÓN DE LA INTELIGENCIA ARTIFICIAL EN EL SECTOR CREATIVO Y CULTURAL

Sebastián Sánchez Polanco



Introducción

Desde hace algún tiempo, la inteligencia artificial ha venido cobrando cada vez más protagonismo en los procesos creativos. Las distintas expresiones artísticas la han empezado a usar como una herramienta para la búsqueda de información, el mejoramiento de técnicas, potencializar sus procedimientos y posicionarse en redes sociales. Buena parte del debate en este campo se centra en si es una mera herramienta o si por el contrario puede tener aún más protagonismo dentro del proceso creativo. Ese protagonismo puede pensarse desde la injerencia que tenga la inteligencia artificial en el proceso creativo: ¿Puede ser autora? ¿Puede ser titular del algún derecho?

En esta sección abordaremos la inteligencia artificial como tecnología emergente que explora ciertos impactos en el sector creativo y cultural. Luego de dar la definición, explicaremos algunas de las normativas que resultan aplicables en Colombia y en Chile para abordar las situaciones planteadas; después, presentaremos algunos casos de uso antes de hablar sobre las oportunidades de esta tecnología y cerrar con unos consejos prácticos para su aprovechamiento.

¿Qué es la inteligencia artificial?

Antes de entrar a ver la definición de inteligencia artificial, resulta necesario definir sus componentes, es decir: "inteligencia" y "artificial" por separado. De acuerdo con la RAE, podemos entender por "inteligencia" aquella "capacidad de entender, comprender o resolver un problema". Y también como "la habilidad o destreza en ciertos aspectos" (RAE, 2022).

A partir de esta definición de la RAE podemos interpretar que la inteligencia es una capacidad que se desarrolla con el paso de los años, lo que permite analizar el entorno e ir tomando decisiones a lo largo de la vida. También se puede entender como la *expertise* en un tema o aspecto específico de la vida en el que se logra cierto nivel de entendimiento.

Ahora bien, siguiendo con la RAE, se entiende por "artificial" aquello que no es natural, que está hecho por el humano, lo que ha salido de su ingenio (RAE, 2022). Se puede inter-

pretar entonces que lo artificial es aquello que los humanos, con base en su inteligencia, pueden crear. Dicha creación tiene como fundamento su ingenio e inspiración.

Por otro lado, la inteligencia artificial se define como una: "Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico" (RAE, 2022). Esta última definición enfoca la inteligencia artificial como una disciplina, o campo de estudio, en el que se ejecutan técnicas y operaciones mediante programas informáticos. Es decir, podemos pensar que la inteligencia artificial viene como un desarrollo del *software*[4] o como la nueva era de las computadoras.

Así las cosas, la inteligencia artificial llegó para ayudar a los seres humanos en sus tareas más rutinarias, hasta para aquellas que demanden un esfuerzo físico. En ese sentido, teniendo en cuenta la definición precitada en la que se alude al razonamiento lógico, la inteligencia artificial puede aprender cómo llevar a cabo una tarea con éxito.

En el 2018, la Comisión Europea emitió una comunicación al Parlamento Europeo, al Consejo Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre Inteligencia Artificial para Europa, en la que se define esta tecnología como: "sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción – con cierto grado de autonomía – con el fin de lograr objetivos específicos" (Comisión Europea, 2018). De la comunicación de la Comisión se puede pensar, tal como se dijo anteriormente, que estos sistemas emulan la inteligencia humana, pues desarrollan aquella capacidad de analizar el entorno y tomar decisiones dependiendo de las tareas que se les hayan asignado. Lo que se debe tener en cuenta a la hora de usar estos sistemas, y catalogarlos como inteligentes, es el grado de autonomía que pueden tener los mismos. Se debe analizar el grado de injerencia que pueda tener el humano dentro del proceso que lleve adelante la inteligencia artificial, pues esto podría determinar en un futuro el grado de generación de obras que pueda tener el sistema.

En conclusión, podemos decir que la inteligencia artificial se refiere a sistemas que emulan la inteligencia humana para llevar adelante procedimientos, analizando su entorno y

4 Para ver más sobre esto en: "Aspectos Jurídicos de las aplicaciones de plataformas" dirigido por Darío Veltani.

nutriéndose de datos, para llegar a un resultado concreto. En el mundo creativo, como veremos en esta sección, esa capacidad de autonomía y adaptabilidad hace posible crear resultados o productos, que para algunos pueden llegar a ser verdaderamente creativos, y, por tanto, establecen diversas situaciones en las que debe analizarse quién es el verdadero creador —en caso de existir alguno—, a quién pertenece dichos producto, y cuáles son los derechos que se derivan de estos.

¿Qué normativa o legislación se aplica a los productos creativos? ¿Se aplicaría, también, a los productos generados por la inteligencia artificial?

Como punto de partida para responder a este interrogante, debemos tener en cuenta que existe una disciplina jurídica que se encarga de proteger los derechos que, por el solo hecho de haber creado una obra, adquieren los autores de obras de la "inteligencia" (en los dominios literarios, artísticos y científicos), cualquiera sea su forma de expresión. Esta disciplina se llama derecho de autor. En esta esta sección analizaremos las normas correspondientes a derecho de autor que se aplican en Colombia y en Chile, veamos:

Colombia

Si bien Colombia es un país cuyas leyes de derecho de autor se encuentran en constante actualización, es importante resaltar que aún no se cuenta con normas específicas respecto a la titularidad o autoría de las creaciones de la inteligencia artificial. Sin embargo, analizaremos algunos instrumentos que dan luces al respecto.

Ley 23 de 1982

La norma rectora en temas de derecho de autor para Colombia es la Ley 23. En su articulado se regulan los principales aspectos de la materia. Esta norma es de 1982 y no hace referencia en su articulado a

la inteligencia artificial, a pesar de las reformas que ha tenido. Esta ley de derecho de autor pone al ser humano en el centro de la creación, pues de acuerdo con su articulado se considera autor la persona que aparezca como autor en la obra. Por otro lado, la ley habla del término de protección de la obra. Este será la vida del autor más ochenta años (1982, 2022). Así, se confirma entonces que la ley pone en el centro de la creación autoral al ser humano, pues lleva características que solo este cumple. En conclusión, de esta norma se puede interpretar que el uso que se le puede dar a la inteligencia artificial en el proceso creativo es el de una herramienta.

Ley 1915 de 2018

Dentro del ordenamiento jurídico colombiano, esta ley es la más actual. Se debatió en el Congreso de la República de Colombia con el objetivo de actualizar algunos aspectos de la Ley 23 y para regular otras disposiciones. Una de las características de esta Ley es que, con su sanción, Colombia entró a los países que pertenecen a la OCDE. El artículo 1 de la Ley establece la presunción de autoría en favor de las personas que aparezcan mencionados en la divulgación de la obra, siguiendo así las características de la Ley 23 mencionada anteriormente. Uno de los principales aspectos de esta Ley es llevar los derechos exclusivos que tienen los autores y titulares al entorno digital. Esto es un avance para reconocer la interacción de las obras en internet y así darles a los autores las herramientas jurídicas necesarias para hacer valer sus derechos patrimoniales en el entorno digital. (2018, 2022).

Documento CONPES 3975 – Política Nacional para la Transformación Digital e Inteligencia Artificial de Colombia.

Recientemente, el Gobierno Nacional impulsó un documento CONPES[5] (Política Pública) sobre

5 Consejo Nacional de Política Económica y Social.

Inteligencia Artificial. En este documento se compensan las líneas de acción que sirven de guía para transformar el Estado de lo analógico a lo digital. Una de las primeras líneas de acción del documento invita a actualizar el marco normativo colombiano para aprovechar las nuevas tecnologías, crear competencias que sirvan de herramientas a los ciudadanos y con el fin de estructurar un Estado moderno. Dentro de la misma línea se invita a aprovechar, con tecnología de Inteligencia Artificial, la gestión de activos intangibles (Departamento Nacional de Planeación , 2019). La autoridad de observancia, la Dirección Nacional de Derecho de Autor[6], invita a implementar expedientes digitales para modernizar la rama ejecutiva y brindar un mejor servicio a los ciudadanos de la mano de la tecnología (Departamento Nacional de Planeación , 2019).

Este documento CONPES nace porque no existe aún una norma específica que regule el tema, e invita a aprovechar el momento que se vive para que las normas respondan a este hecho y se reglamente el papel de la Inteligencia Artificial en el Derecho de Autor, y en la Propiedad Intelectual en general, pero también que se utilice en aras de un Estado más eficiente.

Chile

Si bien no existen todavía leyes que se refieran específicamente a la inteligencia artificial, similar a lo que ocurre en Colombia, sí existe una legislación especial en materia de derecho de autor que puede aplicarse para analizar los dilemas planteados. Por otra parte, en lo específicamente relacionado con la inteligencia artificial, cabe destacar que el año 2021 fue muy importante para el futuro desarrollo normativo de dicha área en Chile, ya que se presentó la primera Política Nacional de Inteligencia Artificial, documento que sirvió como hoja de ruta para encausar diversas iniciativas.

6 Unidad Administrativa Especial Dirección Nacional de Derecho de Autor – DNDA, adscrita al Ministerio del Interior.

Ley 17.336 de propiedad intelectual

En el caso de Chile, es la Ley 17.336, sobre propiedad intelectual, la que establece las normas aplicables al régimen del derecho de autor. De esta forma, para saber si un sistema inteligente puede considerarse "autor", por el momento, es ahí donde tendríamos que hallar alguna respuesta. Según esta ley, el derecho de autor se refiere a "los derechos que adquieren los autores de obras de la inteligencia en los dominios literarios, artísticos y científicos, cualquiera que sea su forma de expresión, y los derechos conexos que ella determina", pero, no define expresamente lo que debe entenderse por "autor". A pesar de ello, los autores nacionales concuerdan en que hay elementos en ella que permiten concluir que un autor es "la persona natural (ser humano) que crea una obra literaria, artística o científica que es objeto de la protección que da la ley" (Walker, 2020, p. 96). De esta forma, se entiende que no podrían ser autores las personas o entidades no humanas.

Ahora bien, esto es distinto a otras situaciones en las que se pueden tener algunos derechos en torno a esta ley. Y ahí se distingue entre el "autor" y los "titulares de tales derechos", los cuales pueden ser dichos autores (por ejemplo, los escritores, compositores, cineastas, etc.), artistas intérpretes o ejecutantes -como cantantes, actores, etc.; productores de fonogramas (discos, CDs, etc.) y organismos de radiodifusión (radios, canales de TV, etc.), que son titulares de los llamados "derechos conexos", u otras personas a quienes éstos hubieran cedido sus derechos.

Para ver la diferencia entre unos y otros, piénsese en una persona natural que escribió un libro y decidió ceder los derechos de esta a una persona jurídica, que puede ser la empresa para la cual trabaja, con el fin de explotar comercialmente la obra. El primero es el "autor", por ser quien creó la obra (el libro), el segundo es la empresa, "titular" de derechos de explotación, pero que no puede abrogarse

la autoría. Esta distinción es importante, entre otras cosas porque, como regla general, el autor tiene derechos sobre su obra por el simple hecho de haberla creado; en cambio, si no se es autor, para ser titular de derechos se requiere que una ley, contrato u otro documento análogo, así lo establezcan.

Política Nacional de Inteligencia Artificial

El Gobierno chileno, con ayuda de la academia y diversos actores de la sociedad civil, impulsó esta política nacional que busca que el país avance en procesos tecnológicos para implementar la Inteligencia Artificial, con el fin de proteger el bienestar de los ciudadanos y su servicio público. El plan que propone esta política es a diez años y cuenta con 70 acciones y alrededor de 185 iniciativas sociales, académicas y económicas. Para esto, es importante tener en cuenta que convivimos con la Inteligencia Artificial todos los días, desde las actividades más rutinarias hasta la toma de decisiones simples, y que, con el paso de los años, estas interacciones se harán cada vez más comunes (Ministerio de Ciencia, Tecnología, Conocimiento e Innovación , 2022).

Además de este reconocimiento, Chile avanza en la necesidad e importancia de incentivar el I+D+I+e para que el país esté orientado estratégicamente al crecimiento de su innovación. Esta innovación va de la mano con el reconocimiento de las nuevas formas de pensar el Derecho, los datos, la tecnología, pero, sobre todo, las necesidades del Estado (Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, 2022).

Por otro lado, en relación con la Propiedad Intelectual, esta política expresa que es fundamental reconocer la comunión entre Inteligencia Artificial y el sistema de Propiedad Intelectual, así como los retos que esto supone. En los últimos años, Chile ha evidenciado con cifras la creciente utilización de la tecnología en activos intangibles, lo que permite ver una alerta temprana de entendimiento (Comité de

Expertos IA Chile, 2021). Los activos intangibles generados con ayuda de la Inteligencia Artificial, que son protegidos por la Propiedad Intelectual, son protagonistas en el desarrollo de la cuarta revolución industrial. Es por eso que el objetivo 3.4.1. propone un debate sobre estas dos ramas para mantener la novedad y actualización al respecto, con la intención de mejorar el sistema de Propiedad Intelectual y la remuneración de los autores (Comité de Expertos IA Chile, 2021).

Decreto 20 del 3 de diciembre de 2021.

Mediante este Decreto se aprobó la Política Nacional. El Decreto empieza reconociendo los devenires del debate mundial que supone la Inteligencia Artificial, lo rápido que avanza y los múltiples detalles que giran alrededor del mismo. Asimismo, este Decreto sostiene que para la construcción de todo el proceso se crearon espacios de participación donde se escucharon a las partes interesadas y se recaudaron datos para establecer una hoja de ruta que le permitiera al país avanzar en esta tecnología.

Este Decreto marca el camino de implementación de la política, sus acciones e iniciativas, puesto que define la Inteligencia Artificial, aborda su nivel de impacto e interacción, presenta los ejes a tener en cuenta, ejemplifica los diferentes tipos de Inteligencia Artificial que conviven, da fuerza jurídica a los objetivos propuestos y hace la proyección como país. (Ministerio De Ciencia, Tecnología, Conocimiento e Innovación, 2022).

¿Qué tipo de usos puede darse a la inteligencia artificial en el sector creativo y cultural? ¿Se pueden generar algunos problemas?

Como hemos dicho antes, el sector creativo, y por tanto el derecho de autor, no han sido ajenos a la irrupción de la inteligencia artificial. En ese sentido, los creativos tienen la gran posibilidad de utilizarla como herramienta dentro de su proceso para completar o mejorar sus obras. Terminar de escribir libros, mejorar partituras, corregir imperfecciones en arte plástico, interpretar alguna canción o declamar poesía son algunos de los múltiples usos que se le puede dar a la inteligencia artificial a la hora de crear. El creativo tiene en sus manos un sin fin de posibilidades para probar y satisfacer las necesidades del mercado.

Sin embargo, estas nuevas interacciones han generado también muchos retos, especialmente en temas como la determinación de la "autoría" y "titularidad" de las obras.

¿En qué consisten los problemas de "autoría" y "titularidad" de las obras generadas por la inteligencia artificial? ¿Existen casos que hayan resuelto estos tipos de problemas?

Como se indicó arriba, los conceptos de autor y titular de derechos pueden ser distintos, pero, en todo caso, según las leyes vigentes en muchos países, requieren de un paso previo y es que exista un autor (persona natural), sin el cual no hay obra, y, por tanto, no hay derecho de autor. El detalle suscita en que no está muy claro cuál debería ser la solución cuando se crean productos mediante sistemas de inteligencia artificial. En algunos casos, porque se entiende que la participación humana es nula o tan irrelevante que no justifica el nacimiento de ningún tipo de derechos; y, en otros casos,

porque, aunque hay alguna forma de actividad humana relevante (como programar al sistema, entrenar los algoritmos o suministrar los datos) quizás no lo es para el resultado que este es capaz de lograr. Aunque parece claro que la inteligencia artificial no puede ser autor, ¿debería significar esto que no haya nadie que pueda ser al menos titular de algún derecho bajo este sistema? Revisemos algunos de los casos más conocidos hasta la fecha de elaboración de nuestra guía:

a) Derechos sobre un artículo

En China hubo un litigio entre las empresas TENCENT y SHANGHAI YINGXUN TECHNOLOGY COMPANY porque el algoritmo denominado "IA Dreamwriter" escribió un artículo que fue publicado en una página web sin autorización de TENCENT (dueña del sistema de IA que lo escribió). El Tribunal del Distrito de Nanshan de la provincia de Guangzhou (China) reconoció la existencia de derechos de autor sobre ese artículo que fue escrito por un algoritmo de inteligencia artificial (Vázquez, 2020).

En el fallo se afirma que el artículo se puede proteger como una obra literaria, pues cuenta con los requisitos formales de protección, argumentando que el artículo es razonable y cuenta con expresión lógica y clara. Se consideró que la página web era responsable y se condenó a pagar 196 euros a la demandante por las pérdidas económicas que se causaron tras la publicación sin autorización (Vázquez, 2020). Este fallo es realmente disruptivo, pues fue la primera vez que se reconoció un derecho a una obra generada por inteligencia artificial, ya que anteriormente la tendencia, en general, era negar esta posibilidad. Así, según este precedente, lo que se genere por estas tecnologías puede estar protegido por Derecho de Autor, siempre y cuando cumpla con los requisitos formales, y le da herramientas a su titular para poder invocar protección ante cualquier uso sin autorización.

Otro elemento para afirmar que el fallo es disruptivo es la posición de las leyes de Derecho de Autor en el centro de la creación autoral. Es decir, si las obras creadas por los humanos, protegidas por el Derecho, son susceptibles a reclamaciones ante posibles infracciones, esto, de una u otra forma, abre la puerta para que las obras creadas por la Inteligencia Artificial también deban estar protegidas legamente en caso de alguna infracción.

b) Derechos sobre una pintura

Quizás el caso más sonado y famoso sobre las interacciones entre la inteligencia artificial, el arte y el derecho de autor es El Nuevo Rembrandt. Se utilizó un sistema de inteligencia artificial para hacer un retrato emulando el estilo del célebre pintor neerlandés Rembrandt. Para ello, se usaron sus obras y datos que fueron procesados para llevar a cabo este avance. Lo que más impresionó de todo esto fue la rapidez y la precisión del resultado. Muchas de las cuestiones que se plantearon alrededor de este retrato fue la percepción con la que la inteligencia artificial logró captar el estilo del autor. Esta disrupción es una prueba de la injerencia de la tecnología en la capacidad de "crear arte", de poder ser generadora/autora o poder participar en el proceso creativo. (Pitol, 2017).

A partir de capacidades como la descrita, se establecen dos grandes debates en el campo de la inteligencia artificial y el derecho de autor: uno, por la autoría de las obras; otro, por la titularidad de estas. Recordemos que la autoría hace referencia a quién es el autor de la obra, su creador, y la titularidad hace referencia a quién ostenta la capacidad de decidir sobre la explotación económica de esa obra. Aunque antes hemos dicho que solo puede ser autor el ser humano que crea la obra, hay situaciones que no siempre resultan sencillas de dilucidar cuando lo que se crea surge en proyectos como el mencionado, por lo que surgen preguntas como: ¿Cuáles son las cuestiones que necesitan una solución respecto a derecho de autor? Pues bien, aquí lo que se debe esclarecer es quién es o debe ser el autor de una eventual obra, ¿el humano que programó al sistema?, ¿el humano que alimentó con datos al sistema?, ¿la tecnología o sistema en sí mismo?, ¿el dueño del sistema?

Si bien hoy en día la conclusión suele ser que no existe una real autoría en aquellos casos en los cuales no hay intervención creativa relevante de personas humanas, estas cuestiones de autoría aún se discuten y no siempre existe una respuesta única. A pesar de esto, la tendencia es que se debe proteger al humano como el único capaz de crear obras. En todo caso, para que dicha autoría se reconozca en la persona humana tendría que existir algún aporte creativo de esta. Por otra parte, en la medida en que el sistema no es una "persona" y no puede tener derechos, no puede ser considerada estrictamente como "autora".

Por este último motivo, el sistema tampoco podría ser en sí mismo titular de derechos. Aunque sí podría serlo la empresa dueña de la máquina o los humanos que intervinieron en el proceso. De hecho, hemos visto en la primera sección de nuestra guía cómo algunas empresas que ofrecen su software para generar imágenes de forma autónoma con inteligencia artificial, a partir de un simple *prompt*, ya están estableciendo algunas licencias en las que aclaran los usos que podemos hacer de ellas. Sin embargo, debemos advertir que todavía no existe un acuerdo en cuanto a este último dilema, por lo que es todavía objeto de discusión. Esperamos que estas dudas puedan ser aclaradas con el avance del tiempo.

c) Derechos sobre música

La música no ha sido ajena a estos efectos de la inteligencia artificial. Como ejemplo, podemos mencionar el caso de la décima sinfonía de Beethoven que un algoritmo ayudó a completar, denominado El famoso caso de la sinfonía inconclusa. Algunos científicos se dieron a la tarea de sacarle provecho a esta tecnología para llevar adelante el proceso de completar esta sinfonía. La inteligencia artificial se alimentó de bocetos y anotaciones del autor, además de datos importantes de autores contemporáneos (DW, 2021), para esbozar cómo sería el complemento perfecto de esta obra. Esta no fue la primera vez que un programa de inteligencia artificial ayudó a completar una pieza musical, pues tal como lo expresa el portal DW: "Después de que ordenadores ya hayan completado las composiciones inacabadas de los compositores Gustav Mahler y Franz Schubert, ahora le toca el turno a Ludwig van Beethoven" (DW, 2021).

Las preguntas que saltan son las mismas que se han venido reiterando: ¿qué pasa con la autoría? Y ¿qué pasa con la titularidad? En este punto esperamos que saque usted sus propias conclusiones.

Finalmente, podemos afirmar que la inteligencia artificial es una herramienta que está cobrando un protagonismo considerable dentro de las distintas expresiones artísticas. Es una verdad a voces que cada vez más los creativos la usarán (¿por qué no?) para mejorar sus procesos o perfeccionarlos.

¿Existe futuro en el uso de la inteligencia artificial en el sector creativo y cultural? ¿Qué otros usos pueden hacerse de la inteligencia artificial en este sector?

Muchas cosas se pueden decir sobre cómo sacarle provecho a todo lo expuesto, pero pensemos en las oportunidades más significativas para luego dar algunos consejos prácticos con que pueden utilizarse en el espacio creativo.

a) Oportunidades

La primera oportunidad que salta a la vista es la de poder complementar el arte a través del aprendizaje de la inteligencia artificial. Esto puede ser visto desde el proceso creativo como una oportunidad para aprovechar la tecnología, pues con los datos que la integren, sumado a una programación eficiente y a su constante actualización gracias al internet, es posible conocer técnicas, procesos y herramientas nuevas para mejorar una obra o completarla.

Los escritores tienen una oportunidad de oro como: poder revisar su estilo, citas y gramática. Lo que antes podría ser una tarea demorada y engorrosa, hoy la inteligencia artificial puede simplificar la tarea en unos cuantos pasos. Un sistema que integre esta tecnología puede ayudar y mejorar errores de estilos, prevenir faltas gramaticales y advertir posibles plagios. Es importante destacar que estos programas se configuran para que cada vez sean más rigurosos en estos procesos.

Desde otro punto de vista, la inteligencia artificial puede brindar grandes oportunidades en el posicionamiento en internet de sus productos y servicios. Como hemos explicado en nuestra primera sección, ciertas aplicaciones de aprendizaje automático hacen posible acercar a los creadores con lo creado y a los usuarios con los contenidos. En ese sentido, los creativos que intenten comprender cómo funcionan los algoritmos para posicionar su trabajo tienen en sus manos el progreso de la sociedad.

Hoy en día la presencia en internet es tan o más importante que tener un local u oficina y muchas veces no requiere

de grandes inversiones. Sin embargo, dicha presencia tampoco es suficiente en sí misma si no se sabe cómo sacar provecho de ella. Saber hacerlo le permitirá difundir su arte y poder llegar a más personas en el mundo. Para esto es importante conocer cómo funciona el SEO (*Search Engine Optimization*, que significa "optimización para motores de búsqueda"), en aras de mejorar la visibilidad y posicionamiento en los buscadores. Asimismo, es importante "entrenar" a los algoritmos de sus redes sociales para posicionar publicaciones que "trabajen para usted", poniéndolo en contacto con personas que pueden estar interesadas en sus contenidos, productos y servicios. Saber aprovechar lo que el internet en general tiene para ofrecer puede abrir muchas puertas para los negocios, darse a conocer, internacionalizarse y contactar con sus pares y potenciales clientes.

b) Consejos

Sin duda, el primer consejo que se debe dar es perder el miedo. Está latente el temor de que las máquinas nos invadirán, nos dejarán sin trabajo y nos desplazarán de las actividades humanas que realizamos. No obstante, para aprovechar las oportunidades que brinda la inteligencia artificial se debe dejar atrás ese miedo y tener la disposición de conocerla, explorarla y encontrar los mejores beneficios.

En segundo lugar, lo que se debe hacer es aprender. Esperamos que no se malentienda este consejo, la idea no es necesariamente aprender a programar, sino aprender a conocerla y a sacarle provecho. El proceso de aprendizaje humano – inteligencia artificial se debe dar en un escenario de convivencia, en el que la persona pueda usar la herramienta y saber cuáles son los puntos más importantes para hacer ese match con su arte.

Por último, y no menos controversial, es que nunca algo que pueda ayudar al crecimiento del arte y del conocimiento se debe ver como un gasto. Los creativos del siglo XXI deben invertir en su crecimiento intelectual, sobre todo en tecnologías y derecho de autor, conocer los debates, sus derechos y empoderarse de todo ese conocimiento que excede al espacio artístico pero que será de mucha ayuda en su proceso.

Conclusiones

Mucho se puede decir sobre inteligencia artificial, pero lo primero que se debe resaltar es que es no hay respuestas claras, sobre todo en materia de autoría y titularidad. El debate está muy abierto y ni la doctrina, ni las leyes ni la jurisprudencia han unificado criterios para dar soluciones al respecto.

Falta mucho por hacer en cuanto al conocimiento, la exploración y el aprovechamiento que se le puede hacer a esta tecnología; no obstante, lo que sí está claro es que, sin lugar a duda, llegó para cambiarnos la vida. Por otra parte, es necesario que se establezca la protección de las obras que se generen por inteligencia artificial, puesto que así también se cuida la inversión de quien desarrolla la tecnología y el oficio del creador humano.

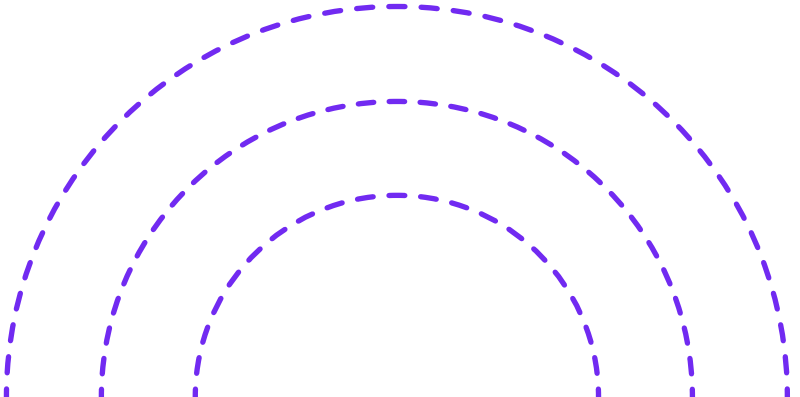
Los creativos tienen un vasto camino para dejar volar su imaginación y darle rienda suelta a la inteligencia propia y artificial para llegar a resultados sorprendentes.

Sección 3

BLOCKCHAIN Y NFTS: UNA GUÍA PARA CREADORES

Paula Amaya Villegas

Felipe Osorio Umaña



Introducción

La tecnología avanza día a día y con ella vienen nuevas formas de interacción. La evolución del internet, actualmente conocida como la "Web3", ha cambiado la forma en cómo nos relacionamos dentro de los ámbitos digitales, ha abierto la puerta a nuevos modelos de negocio, formas de hacer arte y fuentes de ingresos y financiación para proyectos artísticos, generando nuevas posibilidades para aquellos artistas independientes que buscan impulsar sus proyectos de formas no tradicionales.

Durante los últimos años, hemos experimentado una explosión de interés alrededor de la creación y venta de *Non-fungible Tokens* (NFTs). Este interés ha aumentado luego de que el creador del GIF Nyan Cat, Chris Torres, publicara y pusiera a la venta el token de su creación, la cual fue subastada en 300 ETH (equivalente a US$ 337.000)[7], o que la artista Grimes lograra subastar una serie de 10 obras en alrededor de 6 millones de dólares[8], o luego del lanzamiento del último disco de *Kings of Leon* a través de un NFT que otorga a quién lo compra una copia digital del álbum, una edición limitada del disco vinilo y un álbum de arte coleccionable[9].

Aun cuando los NFTs han logrado atraer la atención de artistas en búsqueda de una plataforma para comercializar sus obras y de usuarios para comprar copias únicas y exclusivas de obras de arte, lo cierto es que aún no hay claridad respecto de la estabilidad del mercado de NFTs (Munster, 2021), sus consecuencias legales o, incluso, potenciales daños al medio ambiente que puede generar la infraestructura que soporta el mercado de NFTs (Calma, 2021).En esta sección ofrecemos una guía para aquellas personas que buscan una introducción a los NFTs.

Es decir, en esta sección revisaremos:

- Un panorama general de qué son y cómo operan los NFTs.

7 Véase : https://foundation.app/@NyanCat/foundation/219.

8 Véase : https://www.theguardian.com/music/2021/mar/02/grimes-sells-digital-art-collection-non-fungible-tokens.

9 Disponible en: OpenSea en el siguiente link: https://opensea.io/assets/ethereum/0x557430421f8f3ed0a92aca211f1c05ad7b606288/0.

· La relación entre los NFTs y el derecho de autor. Cubriremos qué es el derecho de autor y qué derechos otorga a los creadores.

· Finalmente, los beneficios y riesgos que tiene la utilización de los NFTs para explotar creaciones artísticas e intelectuales.

¿Qué es un NFT?

Antes de explicar qué son los NFTs, es necesario entender la tecnología sobre la que éstos operan. Los NFTs nacen en el contexto de las tecnologías basadas en *blockchain*, que es una base de datos capaz de registrar información y de asegurar que cada adición a dicha base de datos sea consistente con sus registros anteriores. El *blockchain* asegura la veracidad de su información y la posibilidad de hacer cualquier cambio de manera descentralizada, es decir, no necesita que exista una persona encargada de verificar, por ejemplo, que X ha traspasado 100 bitcoins a Y, sino que todos los participantes de la red *blockchain* verifican la información y sus modificaciones; una vez verificadas, la información o sus modificaciones se registran en la mencionada base de datos. De esta forma, las tecnologías basadas en el *blockchain* aseguran la transparencia e inmutabilidad del registro de la información y las transacciones (Valiente y Tschorsch, 2021).

En ese sentido, el *blockchain* logra asegurar la transparencia e inmutabilidad del registro mediante una función critpográfica que permite almacenar los datos y metadatos de una transacción. Así, el *blockchain* opera a través de un protocolo de consenso en que todos los miembros de la red deben verificar o aprobar que se ha realizado correctamente una transacción. De esta forma, la posibilidad de modificar un bloque de la cadena de manera fraudulenta se torna una tarea extremadamente costosa.

Podemos entender esta tecnología como un libro al cual todos los participantes de la red tienen acceso. Dicho libro constituye un registro inmutable de todas las transacciones que se llevan a cabo por parte de sus participantes. Cada transacción, a su vez, es registrada una sola vez en dicho

libro. Junto con esto, el *blockchain* impide que algún participante de la red cambie o falsifique una transacción una vez que ésta ha sido registrada en el libro, pues cada transacción debe ser consensuada, como ya se mencionó arriba, por todos los otros participantes de la red.

Ahora bien, imaginemos una serie de bloques encadenados entre sí, en el que cada eslabón contiene información o *metadata* que vincula un cierto activo (dinero, por ejemplo) a un titular. En este contexto, podemos preguntarnos: ¿cómo puede el titular del activo traspasarlo a otro participante de la red *blockchain*? Aquí adquieren importancia los llamados *contratos inteligentes* o *smart contracts*. Como podrás ver con mayor detalle en otras secciones de esta guía, estos contratos no se encuentran escritos en un papel, sino que son un código computacional que verifica el cumplimiento de sus condiciones de manera automática; en otras palabras, son autoejecutables (Valiente y Tschorsch, 2021).

En un contrato normal, cada una de las partes redactaría las condiciones necesarias para que pueda cumplirse. Por ejemplo, se podría acordar que cuando *X* pague a *Y* 100 dólares, *Y* traspasará a *X* la última pintura de su colección. En principio, cualquier problema que surja entre *X* e *Y* deberá ser resuelto por un juez que escuchará a las partes y juzgará si una de ellas cumplió o no con el contrato de acuerdo con las pruebas que le presenten.

El *blockchain* y los contratos inteligentes pueden hacer que el proceso frente al juez sea innecesario, puesto que los contratos inteligentes son un código computacional binario, es decir, confirman automáticamente el cumplimiento o el incumplimiento de sus condiciones. A diferencia de los contratos tradicionales, los contratos inteligentes confirman el cumplimiento o incumplimiento de sus condiciones a través de *blockchain*: como la base de datos es capaz de registrar todas las transacciones que se realizan, el contrato inteligente, en tanto código computacional, es capaz de revisar las distintas transacciones que se han hecho y verificar si X ha pagado o no a Y. Si es que ha pagado, el contrato traspasará de manera automática el activo a Y, registrando dicho traspaso en la cadena de bloques. También, por eso se dice que el contrato inteligente y *blockchain* permiten que las transacciones entre distintas personas se ejecuten y registren de manera pública, transparente e inmutable.

Hasta aquí, solo hemos hecho referencia al *blockchain* y a los contratos inteligentes. Pero, ¿qué quiere decir que ciertos activos sean NFTs y cómo se relacionan con lo que hemos dicho hasta ahora? Para entender los NFTs debemos conocer sus dos componentes: (i) es un token (ii) tiene la característica de ser no fungible.

En primer lugar, un token puede ser descrito como una unidad de valor digital escaza, cuyas características y circulación se encuentran determinadas por un código computacional (Ferrari, 2020, p.326). Los tokens, por tanto, pueden tomar distintas formas: una moneda (como el Bitcoin), garantías, acciones, etc. (Giannopoulou *et. al.*, 2021). La característica que une a los tokens es que éstos son un código computacional que constituyen una representación digital de algo que se encuentra registrado en la base de datos *blockchain* (Giannopoulou et. al., 2021).

Un claro ejemplo de esto pueden ser los certificados de autenticidad entregados por grandes marcas como Rolex o Nike, que mediante códigos únicos e inmodificables dentro de la *blockchain* certifican la autenticidad de ciertos productos que se lanzan al mercado. Estos códigos son representados a su vez como un NFT que garantiza la veracidad del producto original. Es decir, en estos casos, el NFT representa una imagen digital del producto que lleva consigo el código de certificación de este.

Los tokens —es decir, las unidades de valor digital—, pueden ser fungibles o no fungibles. Que ciertos bienes sean fungibles quiere decir que pueden ser intercambiados o sustituidos por otro bien que se corresponda a su valor. El mejor ejemplo de un bien fungible es el dinero. En el contexto de las tecnologías basadas en *blockchain*, el ejemplo paradigmático de un bien fungible son las *criptomonedas*, pues es posible dividir cada criptomoneda e intercambiarlas por otros bienes. Por otro lado, los bienes *no fungibles* son bienes que por su naturaleza son únicos y, por tanto, no pueden ser intercambiados por bienes equivalentes. Ejemplos de bienes no fungibles son los productos hechos a medida, obras de arte limitadas o únicas, artículos de colección, etc.

Para entender mejor la diferencia entre bienes fungibles y no fungibles les traemos el siguiente ejemplo: Ana necesita comprar una chaqueta para el próximo invierno. Supongamos que Ana escoge una chaqueta que es de su gusto y que

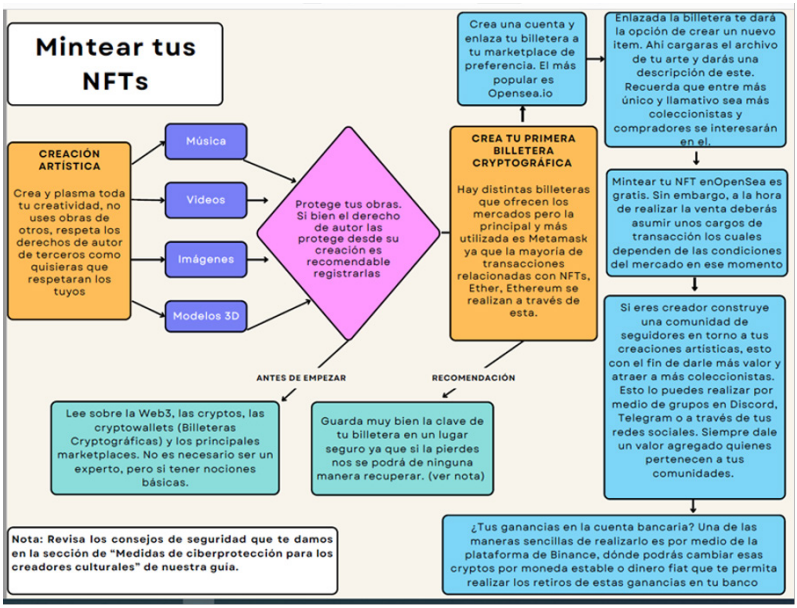
se encuentra dentro de su presupuesto. Una vez que Ana ha encontrado la chaqueta que quiere comprar, se da cuenta de que la tienda tiene 30 ejemplares de su talla. En principio, para Ana es irrelevante cuál chaqueta, dentro de todas las tallas de la chaqueta que le gusta, es la que finalmente comprará y llevará a su casa. Lo que le importa a Ana es tener la chaqueta que le gusta para el invierno. En este ejemplo, todas las chaquetas que cumplían los requisitos que estipulaba Ana eran *fungibles* entre sí, es decir, eran intercambiables. Por el contrario, si Ana hubiese querido comprar una obra original de Van Gogh, para ella no era irrelevante que la pintura no fuera original. De hecho, la originalidad de la obra es una cuestión esencial para comprarla: si a Ana se le ofreciera una pintura falsificada de Van Gogh, seguramente no estaría interesada en comprarla, ya que lo que ella quiere es una obra original del artista. En este sentido, la pintura original es *no fungible*. Para Ana el cuadro pintado por Van Gogh no es intercambiable o no tiene el mismo valor que la falsificación. Cuando se adquiere un NFT es como si Ana tuviese ese activo único digital que nadie más puede comprar al ser este único en su especie.

Entonces, los NFTs son *tokens* únicos que representan en *blockchain* un activo digital o físico. Es decir, el activo que se registra en la base de datos es único. Como el NFT garantiza el carácter único (o no fungible) del activo que es registrado en el blockchain, permite la creación de un mercado de compra y venta de *tokens*. Esto es particularmente interesante para artistas y creadores. Por regla general, los artistas y creadores producen obras únicas (o en el lenguaje del derecho de autor, originales). Los NFTs permiten que los artistas y creadores puedan transar sus obras en el mundo digital asegurando, en principio, que el comprador será el único titular del NFT.

Ahora bien, para poder funcionar, los NFTs necesitan del *blockchain*. Esta plataforma es la infraestructura que permite realizar las transacciones de NFTs de manera transparente y segura. Sin embargo, ¿cómo puedo ingresar mi obra de arte a la red de *blockchain*? Para poder trasladar una obra al registro del *blockchain* es necesario acuñarla (en inglés se usa la palabra *mint* para referirse a esta acción). Cuando una obra que existe fuera de la red *blockhain* es acuñada o *minted*, quiere decir que es registrada dentro de la base

de datos. En otras palabras, al acuñar la obrar, esta pasa a existir dentro de la red, asociada a quien la ha acuñado. Así, quien acuña una obra es el titular o dueño de ella dentro del *blockchain*.

Una vez dentro de la red, el NFT puede ser transado en distintos servicios que actúan como intermediarios. Así, cada transacción que se haga del NFT quedará registrada en la secuencia de bloques, siendo posible identificar quién creó el NFT y quiénes lo han comprado (o vendido en caso de más de una transacción). El registro, por tanto, no solo permite asegurar que el NFT es único, sino también identificar quién es su dueño (Giannopoulou et al., 2021).



Fuente: Elaboración propia.

Ya hemos señalado que un *token* no fungible es la representación digital de un activo, la cual se acuña y, por tanto, entra a la red *blockchain* vinculándose a quien la ha acuñado. En este sentido, por regla general, los NFTs no son más que un metadato que se encuentra registrado en la red *blockchain* y que certifica que dicho *token* es único. Pensemos en un NFT de una obra de arte (digital o física). Tenemos, por una parte, a la obra de arte y, por otro lado, el NFT que forma parte de

la red *blockchain* específica en la cual se ha acuñado. Es decir, el NFT no es equivalente a la obra, por el contrario, este es solo un metadato que señala al objeto digital que ha sido acuñado y quién lo ha acuñado en primer lugar (Giannopoulou *et al*., 2021; Guadamuz, 2021a).

Habiendo revisado de manera general cómo operan los NFTs, continuaremos con una breve explicación de qué es y qué derechos otorga el derecho de autor en este caso.

¿Qué es el derecho de autor?

Hemos dicho que los NFTs nos permiten autentificar y transar obras de arte en el mercado (en este caso, dentro de una red *blockchain*). Sin embargo, para entender las consecuencias jurídicas que el uso de NFTs puede generar, es necesario contemplar la rama del Derecho que tradicionalmente ha regulado la creación, diseminación y transacción de obras de arte: el derecho de autor. La interacción entre los NFTs y el derecho de autor es relevante, pues este último regula las condiciones bajo las cuales una persona puede declararse autor o dueño de una obra y, por tanto, las condiciones para que las transacciones que se hagan con respecto a la obra sean lícitas. Veamos entonces algunas particularidades del derecho de autor.

En general, el derecho de autor (o propiedad intelectual en sentido estricto) es la rama del Derecho que regula la creación, circulación y explotación de las obras del intelecto humano (Bently *et al*., 2018, p.1). En otras palabras, y siguiendo el Convenio de Berna para la protección de las obras literarias y artísticas (en adelante, el Convenio de Berna), el derecho de autor se encarga de proteger los derechos de los autores de obras literarias, artísticas y científicas, cualquiera sea su forma de expresión. Así, el derecho de autor protege los derechos de los creadores de libros, pinturas, música, obras dramáticas, esculturas, grabados, etc. En este sentido, las obras digitales representadas por un NFT podrían encontrarse protegidas por el derecho de autor.

Esta es una definición general, sin embargo, el contenido específico de esta rama del Derecho depende de cada país. Es decir, es posible encontrar distintos requisitos para

proteger las obras, distintos plazos de protección e incluso distintos derechos, dependiendo del país en el que nos encontremos. A pesar de que el contenido del derecho de autor depende de cada país, existen una serie de tratados internacionales que establecen los requisitos mínimos que cada legislación debe reconocer. Dentro de esos tratados, dos tienen una especial importancia debido a la cantidad de países que los han ratificado: el Convenio de Berna y el Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio (ADPIC).

¿Qué requisitos debe cumplir una creación para ser protegida por el derecho de autor?

De acuerdo con el Convenio de Berna y el ADPIC, las creaciones intelectuales deben cumplir con una serie de criterios para poder ser protegidos por el derecho de autor.

En primer lugar, estos tratados establecen que la creación del autor debe ser una *expresión* y no una mera idea. Es decir, lo que el derecho de autor protege es la manera particular en que el autor ha expresado su obra y no la idea que se encuentra detrás de esta expresión. Así, por ejemplo, si alguien pinta un paisaje, el derecho de autor le protegería la forma específica en que dicho paisaje fue pintado, de modo que otra persona podría pintar también un paisaje de una forma diferente sin infringir sus derechos de propiedad intelectual.

En segundo lugar, la expresión del autor debe ser *original*. La noción de originalidad es central para el derecho de autor: solo aquellas expresiones originales se encuentran protegidas. Ahora bien, ¿qué significa que una obra sea original? En términos simples, al menos se requiere que la obra no haya sido copiada y haya sido originada por el autor. Existen, sin embargo, distintos criterios para determinar si una obra es original o no. En general, al menos dentro de los países con influencia del derecho continental (entre los que suelen encontrarse América Latina y el Caribe), el requisito de originalidad se traduce en la necesidad de que la obra refleje o

muestre el sello personal del autor (Dutfield y Sutharsanen, 2020:108).

Es posible que aun cuando la creación sea una expresión original no se encuentre protegida por el derecho de autor debido a razones de política pública. Por ejemplo, de acuerdo con el derecho internacional, para que una obra se encuentre protegida, además de ser una expresión original, requiere no estar excluida expresamente. En este contexto, el Convenio de Berna, en su artículo 2 *bis*, permite a cada país excluir de la protección, por ejemplo, a los discursos políticos o discursos pronunciados en debates judiciales.

Por último, de acuerdo con el artículo 5(2) del Convenio de Berna, si una creación intelectual es una expresión original que no se encuentra excluida por razones de política pública, ésta adquiere protección de manera automática, sin la necesidad de cumplir con ninguna formalidad o registro.

En el caso de Chile, en general, la Ley Nº 17.336 sobre Propiedad Intelectual (LPI chilena) comparte los mismos requisitos impuestos por el derecho internacional. Esto es, para que una obra sea protegida por el derecho de autor chileno requiere ser una expresión original del autor que no se encuentre excluida por razones de política pública. Asimismo, el derecho chileno no exige formalidad alguna para que la obra se encuentre protegida por el derecho de autor[10]. Sin embargo, aun cuando no sea necesario registrar la obra para que esta se encuentre protegida por el derecho de autor chileno, es importante realizar dicho registro ante el Departamento de Derechos Intelectuales dependiente del Servicio Nacional del Patrimonio Cultural del Ministerio de las Culturas, las Artes y el Patrimonio, pues la ley considerará a quién la ha registrado como su autora (salvo prueba en contrario)[11].

Por su parte, como hemos dicho antes en nuestra guía, en Colombia las bases para la protección del derecho de autor se encuentran en la Ley 23 de 1982, pero además en la Decisión 351 de la Comunidad Andina de Naciones, donde, de una manera similar, una obra es una creación intelectual y original del ser humano materializada en todo medio conoci-

10 El artículo primero de la Ley Nº 17.336 sobre propiedad intelectual señala que el derecho de autor "protege los derechos que, por el solo hecho de la creación de la obra, adquieren los autores de obras de la inteligencia en los dominios literarios, artísticos y científicos, cualquiera sea su forma de expresión".

11 Art. 8 LPI.

do o por conocerse. Estas creaciones de la mente, el talento e ingenio humano pueden materializarse en obras literarias de cualquier tipo, obras artísticas como lo son los dibujos, esculturas, fotografías, pinturas, obras audiovisuales, composiciones musicales e invenciones. Para que dichas obras sean protegidas por el derecho de autor deben ser realizadas por una persona natural.

Al igual que en el derecho chileno, en Colombia la protección es concedida desde el preciso instante en que esta es creada y materializada, es decir, no se requiere cumplir con ninguna formalidad jurídica: la protección al autor y su potestad para ejercer su derecho como autor no está supeditada a un primer registro ante alguna entidad oficial. Sin embargo, siempre recomendamos a los autores realizar el registro de sus obras ante la Dirección Nacional de Derechos de Autor con fines probatorios, esto es, que a pesar de no ser obligatorio su registro es recomendable realizarlo, ya que, en caso de conflicto o disputa por los derechos de autor sobre la obra, el registro puede servir como medio de prueba y certificar quién ha sido el verdadero autor y si hay lugar a algún plagio o no.

¿Qué derechos otorga el derecho de autor?

Los derechos que otorga el derecho de autor pueden agruparse en dos grandes categorías. Por una parte, nos encontramos con derechos económicos o patrimoniales. Estos derechos buscan asegurar el bienestar económico de los autores, permitiéndoles prohibir una serie de usos no autorizados de sus obras en el mercado y garantizando al autor una participación económica por cualquier explotación de su obra (Dutfield y Suthersanen, 2020, p.115). Estos derechos patrimoniales son limitados en el tiempo y pueden ser transferidos y/o licenciados a terceros total o parcialmente.

Por otra parte, el derecho de autor también reconoce los derechos morales. Estos derechos buscan resguardar la relación personal existente entre el autor y su obra, es decir, el vínculo que existe entre estos dos desde su creación, desligando componentes monetarios y haciendo referencia

al reconocimiento de la autoría y conservación de la obra original. A diferencia de los derechos económicos o patrimoniales, los derechos morales, por regla general, no se encuentran limitados en el tiempo, es decir, son perpetuos. Además, los derechos morales no pueden ser transferidos o licenciados a terceros.

Ahora bien, los derechos económicos o patrimoniales y morales específicos que otorga el derecho de autor dependerán de cada país.

La LPI chilena, en su artículo 18, otorga los siguientes derechos económicos o patrimoniales:

- El derecho a publicar la obra mediante cualquier medio de comunicación al público.
- El derecho a reproducir o copiar la obra.
- El derecho a adaptar la obra a otro género o usarla de un modo que signifique su adaptación, incluyéndose el derecho a traducir la obra.
- El derecho a ejecutar la obra públicamente mediante radio o televisión, discos, películas, cualquier otro soporte que puede ser reproducido mediante sonido y voces, con o sin imágenes, o por cualquier otro medio.
- El derecho a distribuir la obra mediante su venta.

Es decir, nadie puede publicar, reproducir, ejecutar en público o distribuir la obra sin la autorización expresa del titular del derecho de autor[12]. Por último, el artículo 10 de la LPI chilena establece que los derecho económicos o patrimoniales expiran una vez transcurridos 70 años después de la muerte del autor de la obra.

El derecho chileno también reconoce el derecho de participación o *Droit de Suit*. Este derecho se diferencia de los derechos económicos o patrimoniales en que solo beneficia al autor de la obra. Es decir, aun cuando el autor transfiera todos sus derechos patrimoniales, este mantendría su derecho de participación. De acuerdo con el artículo 36 de la LPI

12 Art. 19 y 20 LPI chilena.

chilena, el derecho de participación otorga al autor chileno de una pintura, escultura, dibujo o boceto, el derecho a recibir el 5% del mayor valor que obtenga aquella persona que adquirió la obra y luego la vendió en una subasta pública o a través de un comerciante establecido.

En cuanto a los derechos morales, la LPI chilena, en su artículo 14, otorga los siguientes derechos:

- El derecho a la paternidad, es decir, a reivindicar la autoría de la obra.

- El derecho a la integridad, es decir, oponerse a cualquier deformación o modificación de la obra hecha sin el consentimiento expreso y previo del autor.

- El derecho a mantener la obra inédita.

- El derecho a autorizar a terceros a terminar la obra inconclusa.

- El derecho a que se respete la voluntad del autor de mantener la obra anónima o bajo seudónimo mientras ésta no pase al dominio público luego de expirados los derechos económicos o patrimoniales.

Como señalamos, estos derechos son perpetuos, pues no expiran con el paso del tiempo. Asimismo, no pueden ser transferidos o cedidos a terceros, siendo el autor el único titular del derecho moral.

Por su parte, el derecho colombiano también agrupa los derechos concedidos en los derechos morales y los derechos patrimoniales o económicos, concediendo cada uno de estos facultades y prerrogativas distintas. Los derechos morales corresponden únicamente a la persona natural que ha materializado su creación intelectual; en consecuencia, estos derechos son intransferibles, irrenunciables, inembargables e inalienables y no podrán ser transferidos a ningún tercero. En virtud del derecho moral de autor, éste podrá decidir sobre la modificación y divulgación de la obra, y, a su vez, tendrá el derecho de paternidad sobre la obra, lo cual significa que éste podrá pedir que siempre se mencione o se indique

su nombre en la utilización de la misma, incluyendo la facultad de solicitar que su nombre se oculte y se refiera a él como anónimo o bajo cualquier seudónimo que este escoja.

Por otro lado, se encuentran los derechos patrimoniales o económicos, los cuales, a diferencia de los derechos morales, pueden transferirse a terceros mediante acuerdo entre las partes o por disposición legal, ya sea a título gratuito u oneroso, como lo es, por ejemplo, en el caso de los herederos de los grandes artistas que siguen recibiendo frutos por las creaciones de sus ascendientes, durante un periodo determinado por la ley. En particular, el derecho colombiano otorga al titular de los derechos económicos la facultad de autorizar o prohibir acciones independientes como la comunicación y distribución pública, reproducción, traducción, adaptación, edición, transformación, explotación, entre otras.

¿Cómo se relacionan los NFTs y derecho de autor?

Como vimos en la introducción, los NFTs han adquirido importancia en el contexto de transacciones de obras de arte. Históricamente, las obras de artes se han vinculado directamente con el objeto físico que las contiene. Esto hacía que la posibilidad de generar copias exactas de la obra fuese muy baja. Pensemos, por ejemplo, en una pintura de un autor reconocido. Ciertamente, existía la posibilidad de crear copias de la obra, pero estas solo podían ser creadas por un pintor con las capacidades técnicas para recrearla y, además, el replicador necesitaba acceso a la obra física. Sin embargo, con la aparición de las tecnologías digitales, las posibilidades de generar réplicas exactas de obras de arte aumentaron exponencialmente. Hoy en día es posible escanear pinturas o copiar archivos MP3 para replicar obras musicales, de manera rápida, fácil y gratuita. Asimismo, internet permite diseminar dichas copias con la misma facilidad. En este contexto, es muy difícil que una obra digital (o digitalizada) tenga un valor económico debido a su accesibilidad.

Los NFTs permitirían a artistas revalorizar sus obras digitales al hacerlas escasas pues, como señalamos en la sección anterior, los NFTs se encuentran vinculados a determinadas

obras de arte digitales. Sin embargo, al garantizar que la copia que se encuentra acuñada en la red *blockchain* es única, los NFTs permiten diferenciar a la obra original de sus copias. Solo aquella persona dueña del NFT es poseedora de la obra original y cualquier otra copia sería precisamente eso, una copia. En este sentido, el NFT operaría como un certificado de autenticidad de la obra. Al poder distinguirse entre obras digitales auténticas y sus copias, se genera un mercado de obras digitales; aquella obra registrada en la red *blockchain* se transforma en un bien no fungible (único, insustituible), el cual puede volver a venderse por un precio mayor al originalmente pagado. Asimismo, como la transacción del NFT se realiza a través de la red *blockchain* y mediante contratos inteligentes, es posible asegurar que solo el dueño del NFT puede transarlo y obtener las ganancias derivadas de dicha transacción.

Puesto que los NFTs otorgan un registro inmutable sobre su dueño, en principio podrían entenderse como una solución tecnológica para resguardar los derechos de los autores y para asegurar la titularidad de la obra. Sin embargo, podemos encontrar una serie de cuestiones problemáticas en la interacción entre los NFTs y el derecho de autor, tal como veremos a continuación:

a) Beneficios

En primer lugar, los NFTs pueden ayudar a los artistas a encontrar una manera fácil, transparente y considerablemente segura para explotar sus obras de arte. Al utilizar *blockchain*, los autores pueden acuñar sus obras y, por tanto, asociarlas directamente a ellos. Esto les permitiría aparecer frente a terceros como los titulares del NFT. Asimismo, al utilizar la plataforma tecnológica del *blockchain* y los contratos inteligentes, el artista puede transferir de forma segura el NFT, sin riesgo de no recibir el pago por dicha transferencia.

Además, los NFTs y el *blockhain* permitirían a los autores poder ejercer de manera más fácil y transparente su derecho de participación. Como cada transacción del NFT quedará registrada en el *blockchain*, el traspaso de los porcentajes correspondientes al autor se podrá realizar de manera automática. Así, por ejemplo, la plataforma *OpenSea* permite a los desarrolladores y artistas que la utilizan para transar sus

NFT, determinar el porcentaje de comisión que desean recibir por cada transferencia a título de creadores del NFT[13].

Ahora bien, es necesario dejar claro que el NFT no es lo mismo que la obra de arte; es solo una representación digital de la obra en el *blockchain*. Por tanto, lo que se traspasa al vender un NFT no es la propiedad sobre la obra, sino solo la titularidad sobre el token (Guadamuz, 2021a; Guadamuz, 2021b). De esta forma, es importante que el artista tenga claro si los términos y condiciones de la plataforma en que transa su NFT transfiere, además, derechos de autor sobre la obra original. En este sentido, la posibilidad de que el comprador del NFT adquiera los derechos de comunicación al público, reproducción, adaptación de la obra, ejecutarla públicamente o venderla, dependerá de si, junto a la transferencia del NFT, se transfieren dichos derechos al comprador.

b) Riesgos

En primer lugar, quien acuña o *mintea* el NFT no necesariamente es el dueño o autor de la obra original contenida en él. Es decir, es posible que se acuñen NFT de obras cuyos artistas no han otorgado el consentimiento para tales efectos. Esto es muy relevante, pues ya se han documentado casos de subastas de NFTs correspondientes a obras de arte creadas por autores que no estuvieron involucrados en su tokenización (Guadamuz, 2021c). Esto es particularmente importante para los artistas y creadores, ya que existen muchas dudas acerca de si la tokenización de una obra ajena supone una infracción de los derechos de autor del creador de la obra. Como el NFT no contiene una copia de la versión original, sino solo una versión acuñada de esta, que generalmente se traduce en un enlace hacia la obra original, en realidad no se estaría copiando o comunicando la obra (Guadamuz, 2021c; Lapatoura, 2021).

Ahora bien, en el caso chileno, reclamar la autoría de una obra ajena a través de un NFT puede configurar la hipótesis de plagio contenida en el artículo 79 bis de la LPI en caso de suprimir o cambiar el nombre del autor o el título de la obra.

En ese sentido, es discutible la posibilidad de infringir los derechos económicos de los autores, sin embargo, si se crea un NFT de una obra ajena y se designa un autor distinto al que creó la obra original se podría estar frente a un caso de

13 Véase : https://docs.opensea.io/docs/frequently-asked-questions.

infracción de derechos morales, el cual puede ser sancionado. Por su parte, la legislación colombiana de derechos de autor, bajo este supuesto, también configura como un plagio no reconocer la paternidad de la obra y desconocer el nombre del autor original conforme a la Ley 23 de 1982 en su artículo 30, causando un grave menoscabo a los derechos morales del titular. Sobre este aspecto volveremos en la sección relativa a las "Medidas de ciberprotección para los creadores culturales".

Segundo, como se señaló anteriormente, es necesario que el artista conozca los términos y condiciones de la plataforma en que transará su NFT. Al vender un NFT, por regla general, el autor solo está vendiendo un interés (similar a un derecho de propiedad) sobre la información o meta-data contenida en el enlace que representa a la obra protegida por el derecho de autor. Por tanto, salvo que la venta este acompañada por un contrato en que se estipule expresamente la transferencia de los derechos económicos o patrimoniales junto al NFT, el artista no está transfiriendo más que la meta-data que apunta a una obra original (Mezei *et. al*., 2021).

Adicionalmente, se debe evitar la apropiación de material perteneciente al dominio público. Como hemos dicho, el derecho de autor es limitado en el tiempo. Una vez que los derechos económicos o patrimoniales expiran, la obra pasa a formar parte del dominio público. Esto quiere decir que nadie puede reclamar un derecho de propiedad sobre la obra y todos podemos, entonces, utilizarla del modo que queramos (respetando, al menos en la tradición continental, los derechos morales del autor). Sin embargo, que una obra se encuentre en el dominio público no quiere decir que esta puede ser digitalizada y vendida como si fuese una obra original. Si una artista decide utilizar una obra en el dominio público para crear una obra diferente, es libre de hacerlo siempre y cuando el producto final sea original. Es decir, el derecho de autor no protege a una persona que simplemente ha digitalizado una obra que se encuentra en el dominio público. De hecho, algunas legislaciones (como la chilena), sancionan este tipo de actividades[14].

14 De acuerdo con el artículo 80 a) y b) de la Ley de Propiedad Intelectual chilena, si un artista reproduce, distribuye, pone a disposición o comunica al público una obra perteneciente al dominio público bajo un nombre que no sea el del verdadero autor o reclama derechos patrimoniales sobre dicha obra, puede ser sancionado con pena de multa de 25 a 500 unidades tributarias mensuales.

Por tanto, la venta de NFTs que representen meras digitalizaciones de obras en el dominio público son altamente cuestionables: quien la ha acuñado no tiene ningún derecho sobre esa obra y, por tanto, no puede traspasar ningún derecho al comprador (Guadamuz, 2021c).

Conclusiones

Los NFTs pueden ser una herramienta muy útil para que los artistas y desarrolladores puedan capitalizar económicamente su trabajo. Otorgan una plataforma transparente y confiable para que los artistas encuentren una manera fácil, transparente y considerablemente segura para explotar sus obras de arte en el mundo digital.

Sin embargo, es necesario destacar que los NFTs no son equivalentes a la obra creada por el autor; son una mera representación en el mundo digital de dicha obra. En otras palabras, son un enlace (dentro una plataforma blockchain) que direcciona al titular a la obra de arte.

Tanto los artistas, desarrolladores y consumidores de NFTs deben verificar qué derechos patrimoniales o económicos son efectivamente transferidos al momento de vender un NFT, pues es posible que no se estén transfiriendo ningún derecho o que se estén transfiriendo todos estos derechos.

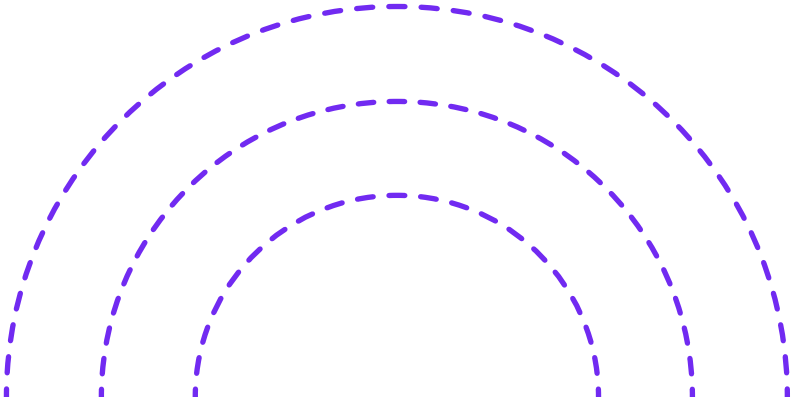
Además, los artistas y desarrolladores deben verificar que no han infringido derechos de autor de terceros al momento de crear sus obras. Si la obra representada por el NFT no es original, el artista o desarrollador puede enfrentar demandas por infracción de derechos de autor de terceros.

Sección 4

CONTRATOS INTELIGENTES "SMART CONTRACTS"

Sebastián Bozzo Hauri

Betty Martínez-Cárdenas



Introducción

En esta sección explicaremos lo que son los contratos inteligentes y por qué están revolucionando la forma de realizar transacciones en el mundo digital. Abordaremos primero lo que significa un contrato en el sentido tradicional del término, antes de pasar al concepto de contrato inteligente y cuáles son sus potenciales riesgos y beneficios.

¿Qué es un contrato?

Es un acuerdo que crea derechos y obligaciones. Es decir, permite que a través de un acuerdo, como podría ser un contrato de compraventa, tengamos el derecho como comprador de exigir la cosa y como vendedor de exigir el dinero por ella; o el contrato de arriendo, en el que una persona, el arrendador, tiene el derecho de exigir el canon de arrendamiento, y el arrendatario de poder habitar el inmueble.

¿Para qué sirven los contratos?

Los contratos están presentes en casi todas las actividades que realizamos diariamente. Cuando nos subimos al transporte público y pagamos el pasaje estamos acordando un contrato de servicio de transporte; cuando compramos el periódico o vamos al café estamos celebramos un contrato de compraventa; cuando nos vamos de vacaciones y deseamos usar una cabaña por un tiempo limitado estamos celebramos un contrato de arriendo. Nuestra vida está rodeada de contratos que facilitan acuerdos y transacciones comerciales entre las personas.

Ahora bien, ¿qué es un smart contract o contrato inteligente?

Todo contrato tiene como objetivo transformar nuestra realidad. Un contrato de alquiler le da facultades al inquilino para que pueda usar la vivienda arrendada y el arrendador recibir un precio por dicho uso. Los *smart contracts* permiten hacer lo mismo, pero agilizando los acuerdos entre las partes, ya que (y esto es una de las características más interesantes) se pueden autoejecutar.

Para entender lo que eso significa, volvamos al ejemplo del contrato de arriendo. Como veremos de inmediato, un *smart contract* permitiría que el arrendatario pueda utilizar la cosa arrendada y el arrendador reciba el precio acordado por dicho arriendo de forma ágil y segura. ¿Cómo lo haría? Gracias al uso de algoritmos y *blockchain*.

Como se mencionó en la sección anterior de nuestra guía, un *smart contract* permite registrar un determinado acuerdo o regla, verificar su cumplimiento, y luego autoejecutarse. Esto último, la autoejecución, se realiza sin la intervención humana. Así las cosas, en el registro del acuerdo interviene la tecnología subyacente que permite darle seguridad al negocio, es decir, el *blokchain* registra el acuerdo, y luego los algoritmos verifican el cumplimiento de la regla acordada en el contrato permitiendo que se autoejecute.

En este sentido, el contrato inteligente es como una moneda de dos caras. Por una parte, es un contrato, porque es un acuerdo de voluntades que crea derechos y obligaciones, y, por otra parte, dicho acuerdo se registra en un lenguaje de códigos informáticos que autoejecuta los términos de un contrato, es decir, la regla que las partes acordaron que se cumpla si se verifica el presupuesto querido. De esta manera, también es posible determinarlos como *smart contract code* (desde una perspectiva informática) o *smart legal contract* (desde una perspectiva jurídica).

Siguiendo con nuestro ejemplo del contrato de arriendo, ¿cómo se puede programar un contrato inteligente?

1. Cada vez que la Sra. María Amenábar llegue al aeropuerto internacional de la ciudad de San Francisco podrá disponer de un automóvil de dos puertas descapotable a un precio determinado, según una tarifa flexible, que le ofrece la compañía Jhonnycar.

2. La aplicación de Jhonnycar, qué utiliza algoritmos, está conectada con la base de datos del aeropuerto y puede verificar si la pasajera María Amenábar aterrizó en el aeropuerto internacional de San Francisco.
3. Al bajar del avión, María, con solo poner su huella digital en una aplicación, podrá abrir la puerta del automóvil y utilizarlo.

4. En el momento en que María abre el auto para usarlo, se transferirán criptomonedas a la cuenta de la compañía Jhonnycar. Una vez que María lo devuelva, se transferirán a las arcas de la compañía otro monto de criptomonedas por los días de alquiler.

En este ejemplo se puede ver cómo se registra una regla, se verifica su cumplimiento y se autoejecuta, sin necesidad de que haya la intervención de un persona en cada fase del procedimiento.

¿Por qué se le llama contrato inteligente?

Porque permiten que una transacción comercial se simplifique al máximo, sin necesidad de generar un contrato en soporte físico, y sin necesidad -siguiendo con nuestro ejemplo- de que el arrendatario concurra a una oficina para firmar el contrato, acreditar su identidad, dejar una fianza o recoger las llaves del vehículo. Gracias al *Blokchain* y a la programación de algoritmos, todo este procedimiento se puede automatizar para simplificar la operación y ahorrar dinero para las partes. Así, la inteligencia del contrato radica en la posibilidad de que la regla que se establece en él se autoejecute luego de verificar su cumplimiento.

La principal característica de este tipo de contratos es que no pueden ser controlados por ninguna de las partes implicadas en el mismo. Este es un sistema descentralizado, que al momento de programarse las condiciones, y depositada la firma por ambas partes, se registra en un *blockchain* que impide su modificación.

No obstante, con la irrupción del Internet de las Cosas (IoT)[15], y la llegada del 5G, este escenario está cambiando, y los contratos podrán no solo autoejecutarse, sino que también podrán acordarse de manera autónoma.

¿Cómo podría acordarse un contrato de manera autónoma?

Por ejemplo, un refrigerador puede tener integrado un software que distingue los alimentos que almacena, y configurarse de tal forma que sugiera y haga la compra de los alimentos que hagan falta en un cierto *stock*. Esta compra la realizaría el programa, seleccionando los productos que estén bajo el stock y enviando dicho pedido a una tienda *online* de alimentos para que se despache al domicilio indicado en la orden.

La instalación de un GPS y un software programado para dicho efecto pueden establecer acuerdos con las tiendas disponibles cerca del domicilio. Incluso es posible que el refrigerador también envíe el listado de alimentos que requiere a diferentes tiendas para recibir varias cotizaciones antes de efectuar la compra.

¿Cuáles serían las principales características de esta formación del consentimiento?

- **Autonomía:** no necesitan de un tercero para ejecutarse, sino que lo hacen automáticamente. Esto,

15 Internet de las Cosas (IoT) es un concepto que se refiere a interconectar distintos dispositivos a través de internet.

como señalamos anteriormente, implica que no pueden ser manipulados por agentes externos a la relación contractual.

• **Seguridad:** se ejecutan operaciones firmadas por ambas partes, siempre y cuando las identificaciones de estas sean verificadas con rigor.

• **Descentralización:** no requiere de un organismo regulador que verifique las transacciones que de ellos se deriven.

• **Velocidad:** son transacciones extraordinariamente veloces, puesto que pueden darse de manera casi instantánea al verificarse el cumplimiento de la condición en cuestión.

¿En qué casos prácticos se utilizan smart contracts?

En la actualidad encontramos casos ejemplares del uso de los *smart contracts* en las industrias creativas y culturales. Por un lado, se encuentran los *smart contracts* que contribuyen a que el artista pueda concentrarse en su actividad de creación (a); por otro, los destinados a asegurarle que pueda continuar con dicha actividad de manera transparente y confiable (b).

a. Smart contracts al margen de la actividad creativa, pero que contribuyen a que el artista pueda enfocarse en ella.
En este caso tenemos grandes ejemplos como el de Restart Energy o la empresa aseguradora. Veamos:

Energía inteligente, el caso de Restart Energy.

Democratizar el acceso a la energía es posible gracias a la utilización de *smart contracts*, *blockchain* y criptomonedas.

Plataformas como *Restart Energy*[16] permiten que todos podamos ser parte del mercado energético, comercializando la energía que se dispone ya sea en los domicilios como en el comercio en general.

Restart Energy es una criptomoneda que opera a través de la plataforma Ethereum, llamada también (MWAT). Esta es parte de RED, una plataforma de energía social diseñada especialmente para revolucionar la forma en la que interactuamos con la energía. Esta franquicia surge como la primera de venta de energía 100% digital, la cual utiliza la tecnología *blockchain* de la Unión Europea desarrollada por Restar Energy.

La franquicia RED le permite a cualquier persona o empresa realizar la apertura de "un negocio de energía virtual" para generar dinero por la venta y consumo mensual de electricidad y gas natural. Añadido a esto, la empresa da un incentivo de 6 meses sin costo por el servicio y luego establece una tasa mínima de MWAT para el cliente, dependiendo del tamaño de la franquicia.

RED otorga comisiones generadas por la venta de 1 MWh de energía, esto por cada 1 MWAT apostado en la operación. Cada franquicia tendrá una cantidad de MWAT asignada, si la contabilización de esta excede el límite impuesto se puede solicitar una extensión de este límite para incrementar la cantidad de MWAT conseguida. El número de franquicias para cada país está limitado a 1 franquicia por cada 10.000 habitantes.

Seguros, beneficios para los consumidores

Un contrato inteligente puede compensar automáticamente al viajero en caso de retrasos. Evitando que los clientes asegurados se agolpen afuera de la oficina para reclamar una indemnización por el retraso del vuelo. Esto evidentemente se traduce en un ahorro de tiempo y productividad para la empresa que no tendrá que tramitar las solicitudes.

16 Véase https://www.tecnologia.press/que-es-restart-energy-mwat-y-como-conseguirlo/

¿Cómo funciona?

Como ya sabemos, el contrato de seguro puede codificarse para que se pueda autoejecutar sin la necesidad de intervención humana. Para esto, es necesario establecer cuál será la regla que debe cumplirse para que el contrato se autoejecute. En el caso de seguros por retraso de vuelos, debemos conocer si el pasajero está en un determinado avión y si dicho vuelo ha sufrido un retraso. En caso de cumplirse ambos supuestos, el contrato se autoejecutará, indemnizando al asegurado con el monto establecido en el contrato.

b. Smart contracts para garantizar la transparencia y confiabilidad en el manejo de los recursos provenientes de industrias creativas[17].

Tenemos dos ejemplos de *smart contracts*: el primero, relativo a la creación de un *crowdfundings*; y el segundo, destinado a la gestión y distribución de los royalties de creaciones musicales.

¿Qué es y cómo funciona el crowdfunding?

Pensemos en esto: quiero plasmar todo lo que he moldeado en la imaginación en una obra, ya sea una escultura, un cuadro, un concierto, o, incluso, una película, pero no tengo los fondos suficientes para realizarlo. Necesito financiación. Sin embargo, el acceso al crédito para el arte no es sencillo y, en algunos casos, simplemente impensable. Aquí es cuando entra el *crowdfunding* como una solución y una forma de financiación con base en aportes colectivos o comunitarios (Best, Sherwood D, & Jones, págs. 3-5) a través de una comunidad virtual que trabaje, con ayuda de la tecnología, en el logro de este objetivo.

17 Disponible en https://www.mckinsey.com/industries/media-and-entertainment/our-insights/how-can-creative-industries-benefit-from-blockchain?_ga=2.215091731.500178860.1538565620-1832155541.1519980753

Las ventajas de esta forma de financiación privada pueden ser resumidas así: "Esta infraestructura tecnológica hace viable el acceso a un amplio colectivo de usuarios en unas condiciones de interacción directa y multilateral, bajo coste y alcance territorial y subjetivo absolutamente desconocidas e inalcanzables mediante las fórmulas tradicionales de financiación por captación del ahorro público" (De las Heras Ballell, 2013, pág. 105).

Hasta la fecha se conocen cuatro tipos de *crowdfunding: donation-based, reward-based, equity-based* y *lending* o *debt-based*.

El primero está destinado específicamente para proyectos sociales sin ánimo de lucro o artistas que requieran donaciones. A través de un *smart contract* en la plataforma respectiva, los donantes podrán recibir la información sobre el estado de avance del proyecto y al mismo tiempo relacionarse con otros donantes y/o beneficiarios.

El segundo tiene el mismo propósito, pero con el ánimo de recibir un estímulo que no puede ser una utilidad o ganancia por los aportes. En efecto, en este modelo los aportantes esperan que al desarrollarse el proyecto se les entregue una "recompensa". Esta recompensa no puede ser ni financiera ni equivalente al aporte realizado, sino más bien una suerte de retribución simbólica. El *reward-based crowdfunding* es particularmente interesante para financiar la realización de eventos tales como conciertos, obras de teatro, exposiciones o producciones cinematográficas[18]. Las recompensas pueden consistir en entradas VIP, un backstage con el artista, copias de libros o programas firmados de manera original o invitaciones a premieres, entre otras. En América Latina, la plataforma Idea.me es una de las más conocidas, para este tipo de financiación, entre los artistas de Argentina, Chile, Brasil, Colombia, México y Paraguay (Idea.me, 2021).

Finalmente, se encuentran los *equity-based* y *debt-based crowdfunding*, en los que los aportantes prepagan lo que esperan obtener mediante una compra grupal colaborativa (De las Heras Ballell, 2013, pág. 109). Sin embargo, es necesario advertir que los *equity-based* y *lending* o *debt-based crowdfundings* también pueden involucrar intereses más importan-

18 Ejemplos de este tipo de financiación en Europa pueden verse en la plataforma de Kickstarter, disponible en: https://www.kickstarter.com/projects/phillippyle2/the-flower-tower-0?ref=section-arts-view-more-discovery-p1 (Consultada el 07/08/2022)

tes y convertirse en verdaderas plataformas de acceso al crédito tanto para proyectos sin ánimo de lucro como para los que permiten la obtención de utilidades. Por esta razón, solo podría acudirse a ellos si son gestionados por sociedades que estén previamente autorizadas por la legislación financiera del país en las que operan para captar y aportar dinero público, con el fin llevar a cabo este tipo de actividades, y en la medida en que los aportantes cuenten también con las condiciones legales y estatutarias que les permitan recibir estas ganancias, como son, por ejemplo, *the collective investment scheme* (CIS) *model como creditonline* (Creditonline, 2022),

En Chile, por ejemplo, todavía no hay regulación específica sobre la materia, pero la Comisión por el Mercado Financiero ha hecho algunos avances y ha determinado los lineamientos generales de regulación de los *crowdfundings* financieros en un documento denominado *White Paper* (Comisión para el Mercado Financiero, CMF, 2019). En Colombia, a pesar de que la idea de los *crowdfundings* como un mecanismo de economía colaborativa fue prevista por el Decreto 1357 de 2018, también estableció algunos limites importantes para evitar justamente que se convirtiera en una actividad de captar y colocar dinero, por lo que se insta a ser cuidadosos al momento de elegir con quién invertir y, particularmente, investigar que la persona que ofrezca este mecanismo de inversión esté vigilada y/o autorizada por la Superintendencia Financiera[19].

¿Qué son y cómo funcionan los smart contracts en la protección de los derechos que los artistas tienen como autores de sus obras?

En esta área de la economía, los contratos inteligentes pueden garantizar que todos los agentes que han contribuido en la creación de una obra puedan cobrar los derechos de autoría que les corresponda. En principio, es posible que cada

19 En este sentido, y con la idea de promover el acceso al crédito para la Pequeña y Mediana Industria, la Presidencia de la República expidió el Decreto 1357 de 2018, disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=87770

pieza cultural (canción, vídeo, libro digital, etc.) pueda tener asociado un contrato inteligente que garantice el pago de los derechos de acuerdo con la fracción correspondiente a cada participante, algo muy difícil de hacer en la actualidad cuando se genera la obligación de abonar por uso o explotación de la obra.

Por otro lado, si una obra experimenta un número determinado de transacciones, se puede conocer la demanda que genera y actualizar su valor sin la necesidad de que participen terceras personas en el proceso. De esta manera, existen en el mercado *smart contracts* que se ofrecen para gestionar la actividad comercial de un artista y de todas las partes involucradas en el proceso de creación y venta de los derechos para músicos o fotógrafos, como, por ejemplo, Bloomen (Consortium, 2020).

En la siguiente figura podemos ver cómo se puede organizar el flujo de trabajo entre un fotógrafo y su publicista a través de la tecnología blockchain:

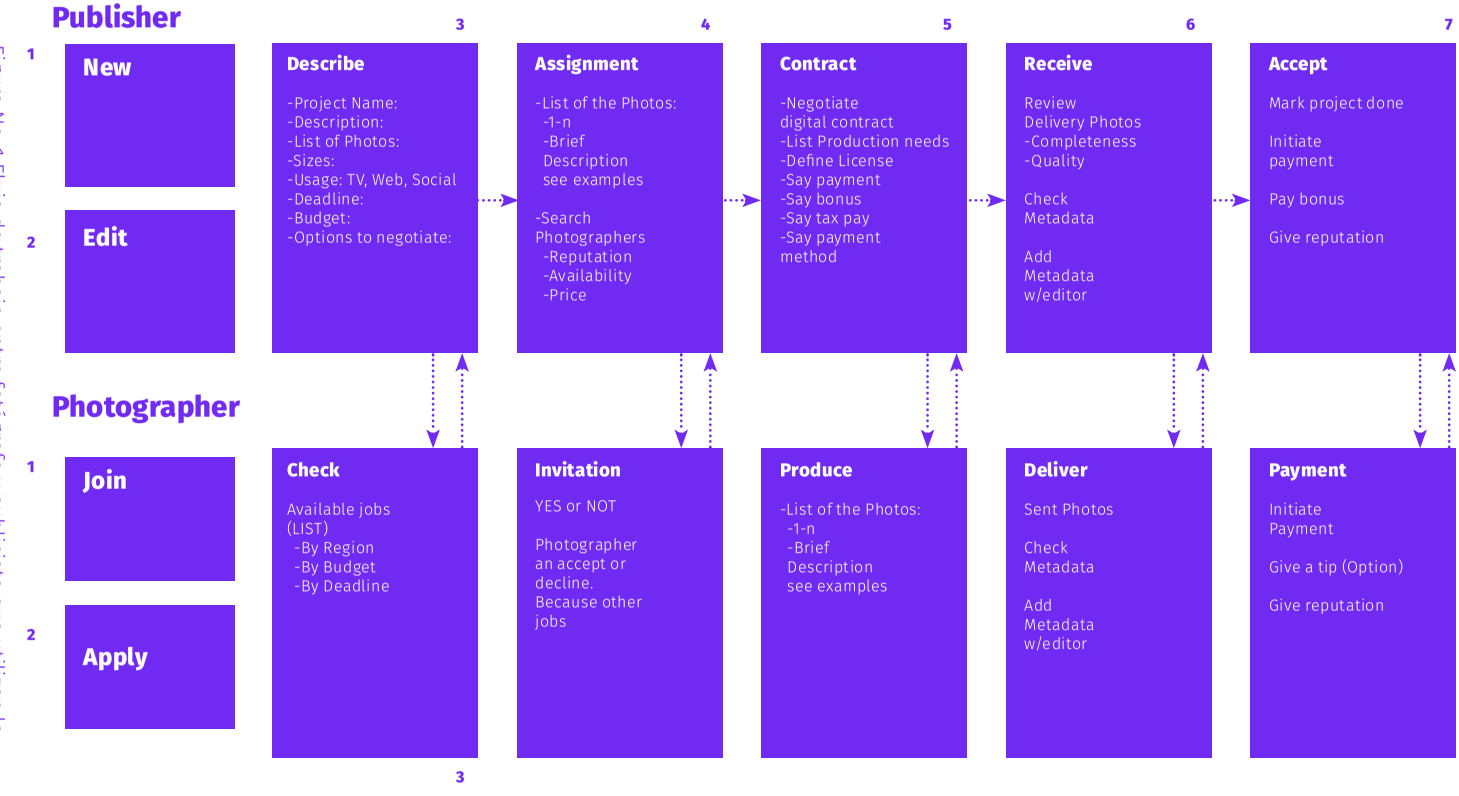


Figura No. 1 Flujo de trabajo entre fotógrafo y publicista que utilizan la plataforma Boomen (Bloomen, 2020, pág. 6)

En el mercado hay firmas consultoras que ofrecen sus servicios para asesorar la gestión de "los derechos digitales y asignación de ingresos compartidos con los colaboradores del proceso creativo" (Blue Room Innovation, s.f.), así como plataformas para el registro y cambio de propiedad intelectual sobre la obra, por ejemplo, registro de patentes, distribución de los ingresos obtenidos a través de la explotación de estas patentes, administrar el uso de servicios públicos en sus talleres, tales como la energía eléctrica a cargo de la Comisión Nacional de Energía en Chile (Herrera, 2018) y la automatización de pagos. (Superintendencia de Industria y Comercio y Centro de Información Tecnológica y Apoyo a la Gestión de la Propiedad Industrial- CIGEP, 2018);

Por otro lado, los *smart contracts* además de expandir una gran campo de oportunidades y beneficios también contempla ciertos riesgos que pasaremos a ver a continuación.

¿Cuáles pueden ser algunos riesgos y oportunidades relacionadas con los smart contracts?

a) Algunos riesgos

Los contratos inteligentes, por más que estén en lenguaje de códigos, no pierden su carácter jurídico y, por ende, los efectos que producirán tendrán las mismas consecuencias que uno tradicional para quienes los celebren. Es por esto que la concurrencia de un abogado para analizar los efectos jurídicos que comprometen a las partes es fundamental, pero además es necesario que dichos profesionales trabajen de la mano de informáticos o desarrolladores de *software*, pues son estos últimos los responsables de codificar los acuerdos, ya que si la regla está mal escrita, la autoejecución del contrato se producirá según la verificación del supuesto programado. Asimismo, es necesario contar con un sistema fiable, es decir, lo suficientemente seguro contra ataques de terceros que quieran vulnerar la infraestructura tecnológica que da sustento al desarrollo de dichos acuerdos.

Por otra parte, sobre todo si en dichos contratos intervienen consumidores o personas en un ámbito no comercial,

es necesario tener un modelo de protección de datos personales[20] y garantizar el buen uso de estos según las políticas publicadas. Lo anterior debe ser un imperativo no solo legal, sino que de carácter moral. La confianza es un valor que permite el desarrollo de estos sistemas y un mal uso de datos pone en riesgo su progreso.

b) Algunas ventajas y oportunidades

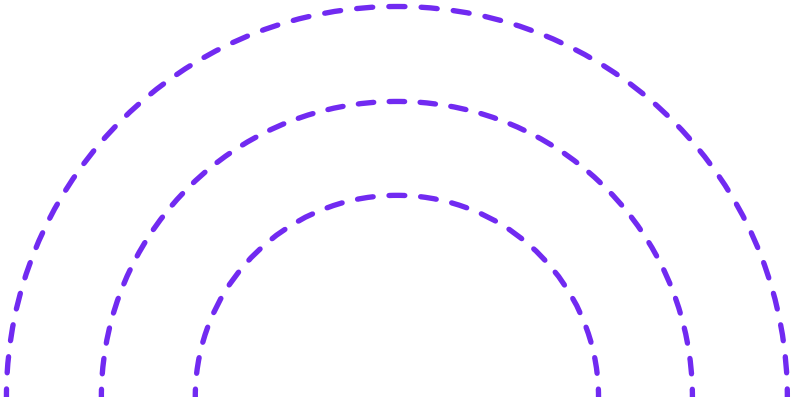
La digitalización de la economía no pasa por la firma electrónica. Si bien es un primer avance hacia la digitalización, las oportunidades que ofrece la tecnología del *blockchain* y el uso de algoritmos permiten dar un salto cualitativo en una sociedad que avanza hacia un modelo descentralizado, en el que el rol de la autoridad como única fedataria de los actos y contratos ya no es indispensable, puesto que nodos pasan a cumplir la función de control y de fe pública. Esta y otras ventajas como mayor autonomía, velocidad, confianza, menos costos y mayor seguridad son primordiales para entender hacia dónde nos llevará los avances de la tecnología.

20 En la sección 6 de nuestra guía podrás encontrar algunos consejos relacionados con la protección de datos personales.

Sección 5

RIESGOS Y OPORTUNIDADES DEL METAVERSO

María José Arancibia



Introducción

En esta sección exploraremos algunos conceptos fundamentales para comprender lo que significa el metaverso y las oportunidades que ofrece especialmente para el sector creativo y cultural.

¿Qué es el metaverso y por qué cada vez más personas hablan sobre ello?

No nos debe extrañar que en algún momento lleguemos a pensar que la Internet es una especie de "ser vivo", que se expande en diversos niveles. Así hoy hablamos de la web 3.0 que, en términos simples, lo que busca es crear sitios web más inteligentes, conectados y abierto. Un primer acercamiento a ella ha sido la implementación de la Internet de las Cosas (*IOT*). Dentro de las tecnologías incorporadas a éstas se pueden encontrar la Inteligencia Artificial (IA), *big data*, el *blockchain*, *tokens*, *NFTs*, entre otras.

De esta forma la web 3.0, por todo lo que se puede realizar con ella, representa una oportunidad y a la vez un desafío que fue tomado por Mark Zuckerberg, quien en el año 2021 anunció el cambio de nombre de Facebook a "Meta", para lanzar su Metaverso. Esta transformación no representa simplemente un cambio de nombre, es un cambio total en la forma de cómo debemos entender las redes sociales, puesto que tomará todos los elementos que se conjugan en el metaverso con la finalidad de hacer una red social que brinde experiencia mucho más inmersiva a través del uso de avatares que podrán tener todo tipo de experiencias.

Ahora bien, el origen del concepto de metaverso no es algo nuevo, ya que fue utilizado por el escritor Neal Stephenson, en su novela cyberpunk "*Snow Crash*". Así que podemos señalar que el metaverso es "todo aquello que está más allá de nuestro universo", con lo que podemos crear e interactuar (Maldonado, 2022).

Un antecedente concreto de estas plataformas, que en ocasiones se confunden, fueron los videojuegos. Estos crearon un mundo más allá del universo como, por ejemplo, *Seccond Life*[21], que es comparable con *Minecraft* o *World of Warcraft*. Tanto en este tipo de videojuegos como en el metaverso, interactuamos por medio de avatares que vienen a ser nuestras "representaciones", el medio a través del cual vamos a realizar una serie de acciones que en el mundo físico quisiéramos o no emular.

De esta manera, ¿es suficiente tener un avatar para poder interactuar? Sin duda que no. Cuando hablamos de plataformas debemos imaginar un mundo donde podemos incorporar todas las cosas que vemos en nuestra realidad convertido a 3D. Es así como museos, estadios, edificios emblemáticos, tiendas, conciertos, desfiles de moda, construcciones de todo tipo y un sinfín de cosas son las que mejor se incorporarán en este tipo de plataformas. Hablamos en plural porque, a pesar del lanzamiento que hizo Meta, no existe un único metaverso. Existen tantos otros, entre los que destacan: *The sand box, Decentraland, Bloktopia, Axie infinity, Somnium Space, Star atlas.*

21 Quienes jugaron Second lifes recordarán que en dicho juego se podía acceder mediante un avatar con el que se podían hacer un sinfín de cosas, desde comprar o intercambiar productos hasta crear una identidad totalmente nueva.

Una de las plataformas más conocidas en el metaverso es *Decentraland*, que se divide por parcelas de tierra y funciona mediante realidad virtual descentralizada 3D, utiliza la tecnología de *blockchain* para poder validar las transacciones y tiene su propio *token* llamado "Mana", con el que puedes comprar productos y servicios digitales.

A pesar de que el metaverso es una estructura compleja, no es completamente autosuficiente, pues requiere de otra tecnología para desarrollarse. Requiere de Inteligencia Artificial, diseño 3D, realidad virtual, *blockchain*, *tokens*, *NFT (non fungibles tokens)* y *smart contracts*. Todo este ecosistema interconectado es el que permite que las plataformas se puedan desarrollar e interactuar.

a) Normativa aplicable

Por el momento, el metaverso carece de una regulación legal o administrativa propia directamente aplicable. Este vacío normativo podría provocar ciertos inconvenientes en caso de existir conflictos como, por ejemplo, determinar la titularidad de los derechos por las creaciones que nazcan en el metaverso o en la apropiación de una propiedad digital ajena. También, sería necesario en cuanto a temas procesales, como en el caso de la comisión de un delito, para establecer el lugar donde ocurrió la infracción. No obstante, los conflictos que se han presentado en el metaverso, principalmente de propiedad intelectual, se han resuelto a través la normativa existente que regula estas materias. Tal es el caso de Hermès, quien demandó a Mason Rothschild, artista creador de los Metabirkins, NFTs inspirados en el bolso de Hermès. El conflicto surgió a partir del uso no autorizado de la marca registrada del diseñador, pues Rothschild alegó que, de acuerdo con la Primera Enmienda de los Estados Unidos, tenía derecho como ciudadano estadounidense de crear arte basándose en sus interpretaciones del mundo que le rodeaba, y agregó, a su vez, que todo aquello se trataba de una protesta en contra de la moda cruel que afectaba a los animales. (ALFAGEME, 2022)

De acuerdo con lo anterior, y dado que pueden existir áreas difusas en las que no existe una única plataforma, la primera medida que se debe tomar es recurrir a la autorregulación de los términos y condiciones, sin que estos contradigan la normativa nacional en vigor.

Mediante la autorregulación se busca, no evitar los problemas, sino dar seguridad en el uso de este tipo de plataformas para resolver posibles conflictos.

En estos momentos, frente a un problema de propiedad intelectual (marcas, derecho de autor, patentes de invención, diseños), protección de datos, derecho a la propia imagen, lo que se hace es un ejercicio de analogía, mediante el cual se busca aplicar la normativa pertinente para estos riesgos.

b) Posibilidades de uso

Adelantábamos que este tipo de plataformas permite la creación de una nueva realidad basándose en la nuestra. Para lograrlo, como ya lo mencionamos anteriormente, es necesario el empleo de tecnología como la inteligencia artificial, la realidad virtual, el diseño 3D, las criptomonedas, el blockchain, los *Smart contracts*, los NFT's, entre otros.

Gracias a esta tecnología se crean avatares, con los que el usuario interactúa, que pueden correr, hablar, comprar, jugar, crear cosas y experimentar otras situaciones similares a las del mundo real. Los avatares pueden ser de varios tipos: idénticos al usuario, tomando sus rasgos físicos; diseños propios o de terceros, o basándose netamente en los personajes de terceros (Delgado García - Pomadera, 2022). Cada una de estas opciones genera diversas oportunidades y riesgos de los que hablaremos más adelante.

En cuanto a las oportunidades que esto representa en otros campos, para la industria de la moda, por ejemplo, permite la creación de accesorios o prendas de vestir que el usuario podrá adquirir por medio de *tokens*. Tenemos el caso

de Nike, por ejemplo, que en el año 2021 presentó NIKELAND en la plataforma de juegos de Roblox. En ella, los avatares pueden realizar ejercicios físicos y vestirse con prendas y zapatillas de la marca. También está el ejemplo de Gucci, que vendió una versión digital de su conocido bolso Dionysus en el metaverso de Roblox, así como Dolce & Gabanna también vendió una colección de NFT's (ACHAP, 2022).

Otra de las opciones que plantea esta plataforma es la de asistir a reuniones de trabajo o de amigos. Así las cosas, son muchas las oportunidades que se generan también en el mundo de la gestión y creación artística. No obstante, en este caso es importante tener claro cuáles son los ciclos de la cultura: creación, producción, difusión y consumo (Santaella, 2021). Estos pasos, que antes los encontrábamos separados y aislados entre sí, hoy se interconectan por medio de la tecnología, como en el *blockchain*.

En cuanto a la industria creativa, el metaverso ya contempla algunos ejemplos concretos. En Chile existe una plataforma de videojuegos (la primera en Latinoamérica) llamada Otherland Music, cuya temática radica en los conciertos. Tal como encontramos en su listado de FAQ, esta es una plataforma en la que los usuarios pueden interactuar entre sí, realizar micro transacciones, comprar elementos para sus avatares o entradas para recitales, tal como ocurrió con el primer concierto virtual de Santiago Schuster en esta plataforma.

Otro gran ejemplo es la plataforma de Fortnite, en la que se han realizado conciertos de diversos artistas como Ariana Grande y Travis Scott. Estos conciertos no fueron en vivo, pero el paso siguiente es que lo sean, así como lo hizo Justin Bieber a través de la plataforma Wave, en la que los usuarios podían escribir mensajes, mandar emotices e identificarse de forma inmersiva e interactiva.

Por otro lado, encontramos que en la industria de la moda también ha pasado al siguiente nivel, pues en el mes de marzo se realizó *Metaverse Fashion Week*, que fue una experiencia virtual en la que el espectador pudo conocer las propuestas de las diferentes marcas (Infotextil, 2022). Esto representó no solo la experiencia del desfile, sino que acercó las marcas a los avatares de las personas, que bien pueden empezar a comprar, mediante tokens, ropa exclusiva y de lujo, así como otros accesorios creados especialmente para los personajes.

Otros que también se han acercado a este tipo de tecnologías han sido los museos. Por motivo de la pandemia, este proceso se adelantó para que las personas, a través de visitas guiadas pudieran, con solo mover el mouse, estar dentro del museo. Aquello fue el inicio de algo mucho mayor, pues hoy lo que se busca es replicar los espacios de un museo en alguna de las plataformas existentes en el metaverso, como Decentreland, por ejemplo, y tener las obras en formato digital para que verlas a través de los avatares.

Tal como lo veníamos adelantando, las plataformas del metaverso no se pueden entender como elementos aislados, sino como un ecosistema. Esto ha permitido que el diseño digital entrara en otra etapa, en un auge de coleccionismo y exclusividad a través de los NFT, que pueden ser denominados también "certificados de arte digital", y que se pueden encontrar gracias la tecnología *blockchain*, que asegura la trazabilidad de la obra y la propiedad de esta.

C) Riesgos u oportunidades del metaverso para el sector creativo

El riesgo más latente que se puede presentar en el metaverso son las infracciones a la propiedad intelectual. En primer lugar, puede existir un uso no autorizado de marca comercial, por lo que las empresas han comenzado a registrar sus marcas comerciales, pensando la protección integral de sus activos intangibles en las plataformas. En segundo lugar, desde el derecho de autor encontramos ciertos riesgos en el sector de la moda, en cuanto a los diseños de vestuario y accesorios para los avatares. Como ya mencionamos anteriormente, algunas marcas se han preocupado por tener una presencia en este sector mediante la creación de colecciones especiales para los avatares. Es por esto que han empezado a tomar algunos recaudos para evitar la imitación y reproducción de sus diseños.

Por otro lado, encontramos los avatares, que son creaciones complejas, ya que poseen unas habilidades concretas y están en constante evolución. Estos pueden gozar de una personalidad y son utilizados en algunos casos para la promoción y publicidad (Dolores Garayalde & Cano, 2022). Es por esto que no solo son susceptibles de protección mediante derechos de autor, sino que la propiedad industrial también

juega un papel esencial. En efecto, también pueden protegerse mediante el diseño industrial, el derecho marcario o incluso una patente.

De esta forma, las posibilidades de que existan infracciones a la propiedad intelectual son muchas, pues en la medida en que exista mayor libertad de la creación, el numero usuarios aumentará exponencialmente. En ese sentido, es probable que el diseño de un avatar afecte a otros usuarios, marcas u obras protegidas por el derecho de autor.

Otros de los riesgos – o más bien, retos – que nos depara el metaverso son los temas vinculados con la privacidad, la gobernanza y la identidad (Matinero Tor, 2022). Como sabemos, el metaverso funciona a través tecnologías como *blockchain* y los NFT's, lo que permite, a su vez, crear una identidad digital para cada individuo o empresa al momento de interconectarse con tercero (Matinero Tor, 2022). Esto puede verse como una ventaja en cuanto a la protección de datos, puesto que se pueden escoger las características que identifican a nuestro avatar; no obstante, la privacidad se diluye un poco en el espacio abierto del metaverso, ya sea por las interacciones de los mismos avatares – tengan nuestros rasgos o no – o porque se filtran algunos rasgos de la personalidad.

¿Qué debemos considerar antes adentrarnos en el metaverso?

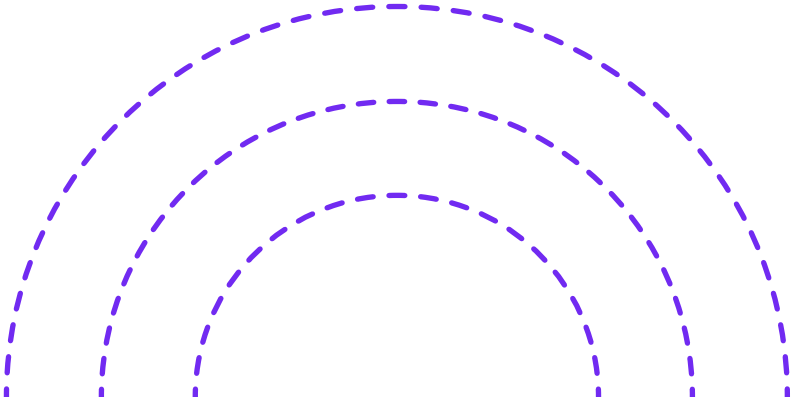
Para implementar el metaverso en la industria creativa debemos tener en cuenta que lo importante es proteger previamente lo que ingresará a la plataforma. Por eso, es fundamental cerciorarse de que las marcas comerciales estén registradas de manera adecuada. Para esto, la European Union Intellectual Property Office ("EUIPO") ha entregado algunas guías para este tipo de registros, haciendo énfasis en la virtualidad y los NFT's (TFL, 2022) con el fin de evitar contratiempos y reclamaciones. Es por esto que recomendamos lo siguiente: al ingresar en cualquier plataforma que existe en el metaverso, es fundamental detenerse a leer con cuidado los términos y condiciones, pues al no tener una regulación propia, el usuario es quien debe instar por la protección de sus datos personales, la propiedad intelectual y la titularidad de las creaciones originadas en este espacio.

Sección 6

LA PROTECCIÓN DE DATOS PERSONALES EN LAS INDUSTRIAS CREATIVAS Y CULTURALES

Juan Carlos Salazar Camargo

Pablo Viollier Bonvin



Introducción

Actualmente, existen diversas plataformas a través de las cuales los seres humanos negociamos, nos entretenemos, nos comunicamos, nos informamos y, en general, llevamos actividades propias de nuestro diario vivir. En ellas, compartimos diferentes tipos de información y, por tanto, entramos en un mundo donde se realiza un uso y tratamiento cada vez más intensivo de datos personales.

Diferentes autores, entre ellos, el doctor Nelson Remolina Angarita, señalan que: "la recolección internacional de datos alcanza su máxima expresión con la aparición y expansión de internet"[22]. De acuerdo con Remolina, "cualquier persona con acceso a internet es potencialmente un recolector —nacional o internacional— de datos en cualquier parte del mundo, tratándose de una actividad que puede alcanzar un volumen potencialmente mayor que las transferencias internacionales a medida que aumenta la tasa de penetración de internet"[23].

En ese orden de ideas, es importante que el Estado, los consumidores y los empresarios tengan claras las reglas de juego para evitar transgredir los derechos de las personas. Por eso, deben usar de manera legal los datos personales que se obtienen al momento de acceder a todas las herramientas relacionadas con las industrias creativas.

Por tal motivo, consideramos necesario realizar la presente guía, con el fin de ampliar ese desconocido mundo sobre datos personales, para que aquellos usuarios de internet, plataformas y en general, los participantes del ecosistema de las industrias creativas se concienticen sobre la importancia de estos.

1. ¿Qué es un dato personal?

Para aterrizar este concepto al territorio y la legislación colombiana en primera instancia, es necesario remitirse a lo establecido en la Ley 1581 de 2012, que en el literal b) de su artículo 3 señala que el *dato personal* es "cualquier informa-

22 Remolina Angarita, Nelson. Recolección Internacional de datos personales: un reto del mundo postinternet. Agencia Española de Protección de Datos. 2015.

23 Ibídem.

ción vinculada o que pueda asociarse a una o varias personas determinadas o determinables"[24]. Similarmente, la Ley 19.628, sobre protección de la vida privada de Chile, define un *dato personal* como "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables"[25].

Sin embargo, dentro de nuestro ordenamiento jurídico fue necesario realizar un desarrollo jurisprudencial y legal sobre los datos personales, el cual se explica a continuación:

Constitución Politica de 1991
Art 15. "(...) De igual modo, tiene derecho a conocer, actualizar y rectificar todas las informaciones que se hayan recogido sobre ellasen bancos de datos y en archivos de entidades públicas o privadas. En la recolección se respetarán la libertad y demás garantias consagradas a la constitución"

↓

Art 20. "(...) Se garantiza el derecho a la rectificación en condiciones de equidad.

↓

Ley 1266 de 2008
"Por medio de la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial de servicios y la proveniente de terceros paises y se dictan otras disposiciones".

↓

Ley 1581 de 2012
"Por medio de la cual se dictan disposiciones para la protección de datos".

↓

Decreto 1377 de 2013
"Por medio de la cual se reglamenta parcialmente la Ley 1581 de 2012".

24 Ley 1581, 2012; art 3; lit b.

25 Ley 19.628, 199: art 2, f)

Decreto 886 de 2014
"Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registri Nacional de Bases de Datos".

Ley 2157 de 2021
"Por medio de la cual se modifica y adiciona la Ley Estatutaria 1266 de 2008, y se dictan disposiciones generales del habeas data con relación a la información financiera, crediticia, comercial, de servicios y la provenientede terceros paises y se dictan otras disposiciones".

Ahora bien, la definición de los *datos personales*, no se somete única y exclusivamente a lo que establece la Ley. La jurisprudencia también ha expuesto las distintas clases en las que pueden clasificarse los datos personales. La Corte Constitucional, en Sentencia C-748 de 2011, señaló que los datos pueden clasificarse en públicos, semiprivados y privados o sensibles.

Los datos públicos son aquellos que pueden obtenerse sin reserva alguna; entre ellos, están los documentos públicos, teniendo en cuenta el mandato previsto en el artículo 74 de la Constitución Política. Esta información puede ser adquirida por cualquier persona, sin necesidad de autorización alguna para ello. Por su parte, los datos semiprivados son aquellos "que no tienen naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios". Por último, los datos privados o sensibles, "aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de Derechos Humanos, o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos".

En el caso chileno, la legislación distingue entre datos de carácter personal (ya definidos) y datos personales sen-

sibles, entendidos como aquellos que "(...) se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual"[26]. Debido a que el procesamiento de datos sensibles podría vulnerar los derechos de los titulares, la legislación los protege de forma más intensa.

Por último, la ley considera como datos estadísticos aquellos que en su origen, o como consecuencia de su tratamiento, no pueden asociarse a un titular identificado o identificable[27]. Es decir, los datos estadísticos son los que no se pueden vincular a un titular específico, siendo el opuesto a un dato personal.

2. Relación entre los titulares y sus datos personales

Durante muchos años, la protección de los datos personales fue considerada como una forma de ejercicio del derecho fundamental a la privacidad o la vida privada. De esta manera, se consideraba que proteger la información personal de los titulares[28] era también de proteger la intimidad de las personas. Es decir, de ejercer un derecho negativo de exclusión[29]: permitir a los titulares que cierta información no fuese conocida o manejada por terceros indeseados.

Sin embargo, en las últimas décadas ha habido un cambio en la forma de concebir este derecho. De un derecho negativo de exclusión se ha pasado a pensarlo como un derecho positivo de control: la autodeterminación informativa[30]. El derecho fundamental a la autodeterminación informativa implica el derecho de los titulares a elegir qué información respecto a su persona se presenta ante terceros y bajo qué modalidad. Es así como, la autodeterminación informativa

26 Ley 19.628, 1999: art 2, g)

27 Ley 19.628, 1999: art 2, e)

28 El titular de datos personales es la persona natural a los cuales refieren los datos personales. Es decir, tú eres el titular de tus datos personales.

29 En otras palabras, el derecho a excluir a otros.

30 Contreras, Pablo (2020): "El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena", en *Estudios Constitucionales* (Vol. 18, N°. 2), pp. 87-120

(qué saben otros de nosotros y de qué forma) se transforma en una forma de construcción de la identidad propia, en otras palabras, de ejercicio de la libertad de ser quienes queremos ser.

Esta nueva noción ha ido acompañada de un cambio en la forma en que concebimos la relación entre el titular y sus datos. Muchas veces se plantea el problema del tratamiento de datos personales desde una perspectiva de propiedad, lo que resulta hasta cierto punto entendible, después de todo... se trata de *mis* datos. Así, algunas propuestas que buscan proteger a los titulares incluso han sugerido que las grandes plataformas digitales deberían pagar a sus usuarios por el uso de sus datos personales[31].

Pero, entender a los titulares como meros dueños de sus datos personales puede sonar empoderador, pero en realidad tiene consecuencias indeseadas. Si el titular es simplemente dueño de sus datos personales, eso quiere decir que este puede decidir vender, ceder o arrendar sus datos personales a terceros a través de un contrato comercial con otros; contrato que luego estaría obligado a respetar. Teniendo en consideración la asimetría de información y poder que puede existir entre las personas naturales y las grandes empresas, esta posibilidad seguramente se prestaría para abusos.

Por el contrario, en la tradición legal continental (de la cual los sistemas de Chile y Colombia son tributarios), la relación entre el titular y sus datos personales no se trata de un vínculo de propiedad, sino de titularidad. Esto significa que el titular no puede simplemente vender sus datos o cederlos completamente, sino que solo puede autorizar su recolección, tratamiento y almacenamiento, pero siempre manteniendo la capacidad de recuperar el control sobre estos. Es decir, los datos personales se transforman en un verdadero atributo de la personalidad del titular, por lo que el vínculo entre la persona y sus datos siempre se mantiene y no puede ser renunciado. De esta forma, el ejercicio del derecho a la autodeterminación informativa asegura que el titular siempre pueda recuperar el control sobre la información que le concierne.

Todo esto puede sonar muy teórico, pero tiene una implicancia práctica para cualquier empresario de las industrias

31 Kaiser, Brittany (2018): "Facebook should pay its 2bn users for their personal data", Financial Times. Disponible en: https://www.ft.com/content/7a99cb46-3b0f-11e8-bcc8-cebcb81f1f90

culturales y creativas cuya actividad requiera recolectar, procesar y almacenar datos personales de sus usuarios: siempre deben recordar que esa información no les pertenece, sino que está indisolublemente vinculada a las personas a las cuales refieren, las cuales siempre tendrán la última palabra al momento de recobrar el control sobre ella. De esta forma, siempre deben proponerse actuar como custodios de buena fe de la información personal que recolectan.

3. ¿Cuándo puedo procesar datos personales?

Para procesar datos personales, es decir recolectar y hacer uso de ellos, es necesario tener en cuenta lo establecido en la Ley 1581 de 2012; puntualmente, el artículo 9 señala que, para poder hacer tratamiento de datos personales es necesario contar con la autorización de los titulares.

Una vez recibida la autorización, entran en juego dos personas muy importantes: el **responsable del tratamiento** y el **encargado del tratamiento**. Aunque suene muy parecido, ambas personas tienen funciones y características distintitas.

El primero de ellos, es decir, el responsable, es la persona natural o jurídica que decide sobre la base de datos y el tratamiento que les dará; sus deberes están establecidos en el artículo 17 de la Ley 1581 de 2012. Por su parte, el encargado del tratamiento es quien trata y utiliza los datos; sus deberes se encuentran consagrados en el artículo 18 de dicha ley.

Un ejemplo de tratamiento de datos es el siguiente: la empresa EL CREATIVO S. A. S. recolecta los datos de sus consumidores para realizar una base de datos en la que se describan los productos que más se consumen en ciertos rangos de edades. Con base en ellas, los empleados envían ofertas a los consumidores a partir de sus gustos. En este caso la empresa sería la responsable y los empleados los encargados del tratamiento de los datos.

Algo similar se puede decir respecto de la legislación chilena. Por regla general, solo se pueden procesar datos personales si la ley lo autoriza expresamente o si el titular ha consentido de forma libre, expresa e informada sobre ese tratamiento. Excepcionalmente, existen ciertas circunstancias que permiten procesar datos sin el consentimiento del titular en la legislación chilena, siendo estas: i) el hecho de que el dato se encuentre disponible en una fuente accesible

al público[32], ii) que se trate de un organismo público respecto de las materias de su competencia[33] o iii) que el tratamiento lo realizan personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquellos[34].

En cambio, estas excepciones no son aplicables al tratamiento de datos personales sensibles, los que, debido a su mayor grado de protección, solo pueden ser recolectados en tres casos específicos y excepcionales: i) cuando la ley lo autorice, ii) cuando exista consentimiento del titular o iii) cuando sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares[35]. Lo anterior quiere decir que es indispensable ser cuidadosos con aquellos datos de carácter íntimo o sensible.

4. Uso de plataformas de consumo y tratamientos personales

Al momento de entrar a internet y usar cualquier tipo de plataforma, el titular de los datos debe ser consciente de que estos serán tratados[36] (utilizados) por los portales a los que accede. Cuando un usuario acepta los términos y condiciones, debe ser consciente de que está dando en consentimiento para que sus datos sean tratados.

Esto es conocido mundialmente como el internet de las empresas. Para dar contexto, se tiene establecido que en promedio más de 3,4 billones de personas de todas partes del mundo acceden a plataformas de internet. Por ello, hay que tener precaución cuando se aceptan los términos y condiciones a las plataformas y sitios web a los que se accede. Muchas veces los datos se usan para intercambiar información entre empresa y usuario, con el fin de poder enviar co-

32 Ley 19.628, 1999: art 4, inciso 5.

33 Ley 19.628, 1999: art 20

34 Ley 19.628, 1999: art 4, inciso 6.

35 Ley 19.628, 1999: art 10.

36 Los abogados usamos el término "tratamiento" como sinónimo de procesamiento de datos. De hecho, el tratamiento de datos incluye recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir, cancelar o utilizar datos de cualquier forma. Es decir, hacer cualquier cosa con un dato que no sea pensar en ellos.

municaciones y realizar campañas de publicidad. Por lo anterior, vale la pena recordar que "si el producto es gratis, es porque tú eres el producto".

Alrededor del mundo se celebran diferentes contratos de transferencias de datos en los que las empresas administran información valiosa como la fecha de nacimiento, un correo electrónico, el número de contacto y así, poder generar un perfil del usuario. La recolección de datos se puede derivar de la compra de un boleto de un concierto, por ejemplo, o el acceso a una red wifi gratuita.

Esto no es lo único que sucede con los datos al momento de aceptar los términos y condiciones, o ingresar a la web o app. También estamos seguros de que, como usuario, has visto alguna vez que te solicitan "Aceptar las *cookies*". Estas *cookies* obtienen la información sobre tu actividad en línea y la envían a los propietarios de las páginas web o plataformas web que usaste, junto con el tiempo y la forma en la que permaneciste en ellas. Además, pueden identificar si accedes frecuentemente a estos sitios de internet y desde qué punto lo hiciste.

Otro aspecto que se debe tener en cuenta es el permiso que se le otorga a las plataformas para acceder al micrófono y a la cámara de nuestros dispositivos. Cada vez que un usuario lo hace, le brinda su autorización para escuchar y observar lo que sucede a su alrededor. También, al conectarse a una red gratuita y pública, como en parques, centros de eventos, centros comerciales o aeropuertos, y aceptar sus términos y condiciones, se están compartiendo datos con quienes prestan el servicio de Internet y ese es precisamente el costo que se paga. Los datos son la contraprestación para los dueños de esos lugares, quienes luego hacen diferentes negocios de transferencia de datos para poder enviarte publicidad e información.

Para concluir, es conveniente tener presente los derechos que tienes como titular de tus datos personales. Pero más aún, si eres responsable o encargado de la recolección y el tratamiento de datos personales, debes tener presente los deberes que la ley te obliga a cumplir, entre ellos el de obtener las autorizaciones debidas, cumplir con las medidas de seguridad de la información y en especial, abrir canales de comunicación para atender peticiones o reclamos por parte de tu usuario, relativos a sus datos personales.

5. Principios aplicables

Si estás leyendo esta guía es muy probable que no hayas estudiado leyes, o si lo hiciste, tal vez no te hayas especializado en materias relacionadas con el *derecho* y las *nuevas tecnologías*. Se trata de un área especialmente técnica, novedosa y compleja. Por ello, nadie puede pretender ser un experto de la noche a la mañana o simplemente leer la regulación sectorial y entenderla de buenas a primeras.

La buena noticia es que no necesariamente tienes que ser un abogado experto o hacer un posgrado para abordar de forma satisfactoria situaciones que involucran el tratamiento de datos personales de terceros, a propósito de la entrega de bienes y servicios en las industrias creativas y culturales.

Si bien existen situaciones cuya complejidad o potencial para afectar los derechos de terceros hace necesario recurrir a asesoría jurídica especializada, la existencia de principios rectores en la disciplina de la protección de datos personales cumple el rol de una guía de conducta respecto al cumplimiento de las normas en esta área.

En otras palabras, entender el espíritu de la legislación y la correcta aplicación de los principios que la inspiran hace más factible que al encontrarte en una situación que involucre el tratamiento de datos personales de terceros, seas capaz de optar por un camino que no vulnere los derechos de terceros ni implique un incumplimiento de la regulación vigente. Por lo mismo, y con la intención de fomentar una intuición informada en el lector, vamos a repasar los principios más relevantes de la legislación de datos personales que han sido adoptados por la regulación colombiana y chilena.

a. Principio de licitud del tratamiento

En simple, este principio establece que los datos personales solo pueden recolectarse, almacenarse o procesarse si existe una fuente legal para dicho tratamiento, es decir, en la medida en que se realice con sujeción a la ley. Es decir, por regla general, solo se pueden tratar los datos personales que la ley habilita expresamente o cuando el titular ha dado su consentimiento. Esto es relevante porque este principio no nos permite, como suele suceder, "hacer todo lo que no esté prohibido". Por el contrario, establece que solo se puede procesar un dato personal bajo una causal legal de tratamiento.

Así, el responsable de banco de datos siempre debe verificar que se cuente con el consentimiento libre, informado y explícito del titular de los datos o estar amparado en algunas de las excepciones explícitas a este requisito, contenidas en la ley. Por ejemplo, muchas regulaciones de datos personales eximen las actividades periodísticas de su aplicación o permiten el procesamiento de datos personales sin el consentimiento del titular para uso doméstico (como mantener una libreta personal de números telefónicos).

> **Recuerda:** siempre se debe obtener el consentimiento expreso, libre e informado del titular para procesar sus datos personales. Si no es posible, verifica que exista una causal legal que te permita procesar esa información.
>
> **¿Dónde se encuentra?:** artículo 4 de la ley de protección de la vida privada (Chile) y artículo 9 de la Ley 1581 de 2012 (Colombia).
>
> **Ejemplo de la vida real:** tu emprendimiento no tiene nada que ver con la información de tus clientes. Sin embargo, aquellos que compran en la tienda *online* necesariamente deben entregar ciertos datos personales para hacerles llegar el producto: nombre, dirección de entrega, datos de tarjeta de crédito, etc. Por lo anterior, es importante que dichos clientes consientan al uso de esa información y su finalidad, previo a ser recolectada.

b. Principio de finalidad

Los datos personales deben ser tomados con fines específicos, explícitos y lícitos. El tratamiento de esta información debe limitarse al cumplimiento de estos fines. Este principio, se establece como protección en dos sentidos: 1) limita la información recolectada a aquella necesaria para el objetivo declarado y 2) impide que sea utilizada indebidamente. En otras palabras, al momento de obtener datos personales siempre debe declararse cuál es el objetivo de dicha recolección y luego limitar el uso que se le dé a estos.

> **Recuerda:** siempre se debe declarar una finalidad para la recolección de datos personales y luego restringir el uso de estos exclusivamente a dicho objetivo.

¿Dónde se encuentra?: artículo 9 de la ley de protección de la vida privada (Chile) y artículo 12 de la Ley 1581 de 2012 (Colombia).

Ejemplo de la vida real: con el fin de recolectar fondos para una organización de beneficencia, decides organizar un sorteo con tu producto como premio. Luego de finalizado el concurso, tu socio te propone utilizar los correos electrónicos de los participantes para añadirlos a la lista de personas que reciben publicidad dirigida. Conociendo el principio de finalidad, le respondes que los titulares entregaron sus datos con la finalidad de participar de un concurso de beneficencia, no de enterarse de novedades de un producto específico.

c. Principio de proporcionalidad

Los datos personales procesados deben limitarse a aquellos que resulten necesarios en relación con los fines del tratamiento. Deben ser conservados solo por el período de tiempo que sea necesario para cumplir con los fines del tratamiento. En adición, sirve para restringir los tipos de datos a recolectar, de forma tal que no sean excesivos, por esto, muchas veces también se le llama principio de minimización de datos.

Recuerda: nunca se recolectan datos que no sean realmente necesarios (excesivos) para la finalidad para la cual fueron tomados.

¿Dónde se encuentra?: artículo 23 de la ley de protección de la vida privada (Chile) y artículo 12 de la Ley 1581 de 2012 (Colombia).

Ejemplo de la vida real: estás pensando en añadir un *newsletter* al paquete de servicios que tus clientes y seguidores reciben, pero te das cuenta de que la plataforma que estás utilizando solicita a los potenciales suscriptores llenar un formulario con información excesiva, innecesaria y sensible (número de identidad, género, tipo de sangre, domicilio, etc.). Te das cuenta de que esto vulnera el principio de proporcionalidad,

puesto que es solo necesario que los suscriptores entreguen su correo electrónico y su nombre o alias para recibir el *newsletter*; por lo anterior, decides cambiar de plataforma.

d. Principio de calidad

Los datos personales deben ser exactos, completos y actuales, en relación con los fines del tratamiento. El responsable de base de datos tiene la obligación de mantener los datos actualizados, de forma tal que reflejen la realidad.

Recuerda: que puedes resultar legalmente responsable si la información personal que procesas no se encuentra actualizada o no refleja la realidad.

¿Dónde se encuentra?: artículo 9 de la ley de protección de la vida privada (Chile) y artículo 11 de la Ley 1581 de 2012 (Colombia).

Ejemplo de la vida real: tu negocio consiste en operar una plataforma que permite a distintos artistas mostrar su trabajo y a eventuales interesados en la organización de espectáculos en vivo ponerse en contacto con los artistas. Por un error en el código de la plataforma, el número de contacto de los artistas no se modifica cuando estos lo actualizan, impidiendo que los potenciales clientes se pongan en contacto con ellos. Esta infracción del principio de calidad (información personal desactualizada) afecta directamente a los artistas.

e. Principio de responsabilidad

Este principio establece que quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de conformidad a la ley. Puede implicar el pago de multas y también la indemnización por perjuicios causados.

Recuerda: tener presente que el incumplimiento de la legislación de datos personales puede acarrear sanciones y el pago de indemnizaciones económicas a los afectados.

¿Dónde se encuentra?: artículo 23 de la ley de protección de la vida privada (Chile) y artículo 13 de la Ley 1581 de 2012 (Colombia).

Ejemplo de la vida real: eres el fundador y administrador de un sitio web y aplicación móvil que busca poner en contacto a personas solteras con intereses similares. No solo tienes cientos de miles de usuarios, sino que para llenar su perfil estos tienen que otorgar información sensible (orientación sexual, estado civil, género, ubicación geográfica, etc.). Si esa información se llegara a filtrar, la afectación de un número tan grande de usuarios probablemente puede significar la bancarrota de tu negocio.

f. Principio de seguridad

Se deben garantizar estándares adecuados de seguridad aplicando para ello las medidas técnicas u organizativas apropiadas. Se busca evitar el tratamiento no autorizado, pérdida, filtración, daño o destrucción de los datos.

Recuerda: utilizar servicios seguros u obtener asesoría de un experto en seguridad digital.

¿Dónde se encuentra?: artículo 11 de la ley de protección de la vida privada (Chile) y artículos 17 y 18 de la Ley 1581 de 2012 (Colombia).

Ejemplo de la vida real: eres el mánager de un importante artista que está a punto de lanzar su nuevo disco. Por descuido abres un correo sospechoso y un sitio de Torrent es capaz de entrar a tu computadora y copiar los archivos que contienen las canciones inéditas del artista y subirlas para que sean descargadas de forma ilegal en sitios pirata. ¡Oh, no! Tu descuido le acaba de costar millones a tu cliente.

g. Principio de confidencialidad

El responsable de datos personales y quienes tengan acceso a ellos deben guardar secreto o confidencialidad acerca de estos. El responsable establecerá controles y medidas ade-

cuadas para preservar el secreto o confidencialidad, incluso luego de concluida la relación contractual de las partes.

> **Recuerda:** recolectar datos personales te convierte en custodio de estos.
>
> **¿Dónde se encuentra?:** artículo 7 de la ley de protección de la vida privada (Chile) y artículo 17 y 18 de la Ley 1581 de 2012 (Colombia).
>
> **Ejemplo de la vida real:** la policía sospecha que uno de los autores de un crimen había asistido el mismo día a un concierto organizado por tu productora de eventos. Entonces, exigen obtener acceso a la lista completa de asistentes, junto con toda la información disponible sobre ellos. Puesto que te tomas en serio el principio de confidencialidad, les exiges que te presenten una orden judicial que justifique dicha diligencia antes de acceder a la entrega de la información.

6. Recomendaciones

A lo largo de este capítulo nos hemos propuesto entregarles a los participantes del ecosistema de las industrias creativas y culturales las herramientas básicas que les permitan aproximarse al fenómeno de la protección de los datos personales. A pesar de que esta materia suele considerarse especialmente técnica (tanto desde la perspectiva jurídica como tecnológica), esperamos que esta inducción introductoria les permita a los lectores tomar las decisiones correctas ante aquellas situaciones que impliquen la recolección, procesamiento y almacenamiento de información personal de sus clientes o usuarios.

El solo hecho de poder identificar aquellos casos en donde la información involucrada cumple con la definición legal de dato personal ya es un paso en la dirección correcta, puesto que muchos de los errores en esta materia se producen al no estar conscientes de que se trata de información personal y que, por tanto, hay una serie de requisitos legales que deben cumplirse. Luego, el conocer las hipótesis legales de tratamiento le servirá a los lectores para enterarse bajo qué circunstancias se encuentran legalmente habilitados para procesar los datos personales que se proponen tratar.

A su vez, estar familiarizado con los principios generales que orientan e inspiran la legislación de protección de datos personales significa que, en la mayoría de los casos, los lectores serán capaces de tomar decisiones correctas al enfrentarse a un caso concreto que implique el tratamiento de datos personales de terceros, sin la necesidad de estar al tanto de la legislación a cabalidad. Por supuesto, ante casos complejos y cuya resolución no resulta evidente al aplicar los principios generales, siempre será necesario obtener asesoría especializada.

Nuestra recomendación final es la siguiente: ante un caso concreto que implique el procesamiento de información personal de terceros siempre es una buena idea errar por el lado de la precaución. Actuar con prudencia implica tener presente que se está cumpliendo todos los principios generales, pero también que, en caso de dudas, es mejor idea obtener el consentimiento libre, informado y expreso del titular para procesar sus datos. Así mismo, cabe recordar que la protección de los datos personales es un derecho fundamental, y que infringir los resguardos para su tratamiento puede vulnerar gravemente la autodeterminación informativa, la dignidad y la privacidad de las personas afectadas. Por fortuna, aplicando lo aprendido en este capítulo te puedes asegurar de que esto nunca llegue a suceder. De esta manera, podrás decir con orgullo que tu plataforma, servicio, aplicación o negocio opera de forma íntegra y respeta la protección de datos personales de sus usuarios.

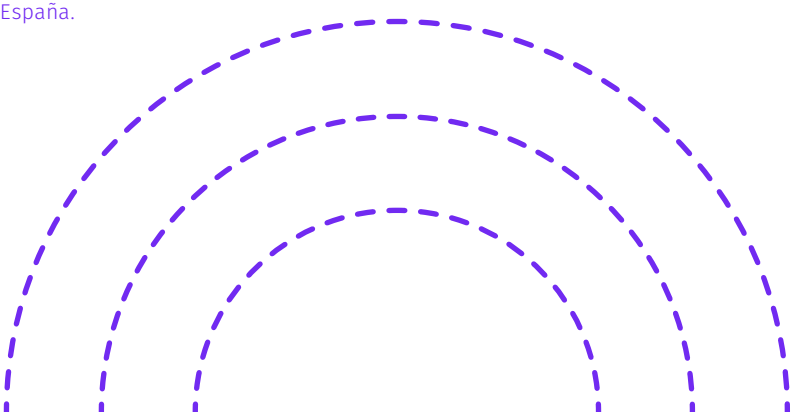
Sección 7

MEDIDAS DE CIBERPROTECCIÓN PARA LOS CREADORES CULTURALES

Francisco Bedecarratz Scholz

Roberto Navarro Dolmestch[37]

37 Esta colaboración se ha elaborado en el marco del Proyecto de investigación "La responsabilidad de la inteligencia artificial: un desafío para las ciencias penales" (PID2020-112637RB-I00), financiado por el Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia, Subprograma Estatal de Generación de Conocimiento, del Ministerio de Economía y Competitividad, España.



1. ¿Debo protegerme en el mundo cibernético?

La convergencia entre las tecnologías digitales y la industria artística está teniendo un profundo efecto disruptivo, transformando la forma en la que los creadores culturales crean contenido y este último es ofrecido a la audiencia. Tecnologías tales como la IA, el *blockchain* y la realidad aumentada ofrecen interesantes oportunidades en las industrias de la música, televisión, publicidad, literatura, juegos, arquitectura, artes, diseño o la moda, entre otras; para producir contenido de manera más expedita, a menor costo y alcanzar a un público mayor. Sin embargo, de esta interacción surgen también nuevas fuentes de riesgos de naturaleza digital o virtual para los artistas y el mundo creativo.

Estos riesgos poseen un elemento diferenciador respecto de los del mundo físico: no son tangibles o perceptibles directamente por los sentidos, porque existen en contextos tecnológicos que hacen difícil reconocerlos para quienes no tienen conocimientos de informática. Solo nos percatamos de ellos cuando ya se han materializado y sentimos sus efectos. A partir de lo anterior y en general, se es menos consciente de los peligros del mundo virtual a los que, sin embargo, estamos expuestos a diario. A pesar de eso, tendemos a adoptar una actitud pasiva o de indiferencia respecto a ellos, lo que significa que se implementan escasas o nulas medidas de protección. Frente a la expansión del mundo digital y la migración del trabajo de muchos creadores culturales a ese entorno, resulta fundamental adquirir conciencia de dichos riesgos y las medidas necesarias para protegerse.

La presente sección tiene como objetivo describir los riesgos producto de tecnologías emergentes más importantes a los que se ven expuestos los creadores culturales, las medidas de prevención que pueden adoptar para minimizarlos y qué hacer en el caso de, lamentablemente, experimentar un resultado lesivo o un ataque malicioso.

2. ¿Qué son los riesgos digitales y la ciberseguridad?

La implementación de tecnologías emergentes en una actividad conlleva un riesgo de consecuencias negativas: pérdida de datos, divulgación de información privada, copia de terceros, entre otras. Este riesgo es propio del mundo digital (inherente) y cuando interactuamos en él, tenemos iguales posibilidades de enfrentarnos a tal riesgo como de no hacer-

lo (aleatorio). Esto es lo que se denomina como riesgo digital. También la creación y divulgación de contenido cultural está expuesta a dicha clase de riesgo, por lo que es esencial adoptar las medidas de seguridad necesarias para minimizar la probabilidad de su materialización.

La ciberseguridad consiste en la protección de computadores, servidores, aparatos móviles, sistemas electrónicos, redes y datos informáticos de ataques maliciosos. Esta constituye un aspecto fundamental en caso de exposición frente a cualquiera de las tecnologías objeto de la presente guía, pues permite aprovechar todos sus beneficios y garantizar, al mismo tiempo, que estas no generarán efectos negativos para el usuario o terceros.

Las medidas de ciberprotección pueden ser clasificadas en generales y especiales. Las primeras tienen por objeto aumentar los niveles generales de resguardo del sistema informático frente a amenazas, y que deben ser implementadas por todos quienes desarrollen todo o parte de su trabajo en el mundo digital, incluidos los creadores culturales. Entre las medidas generales es posible enumerar las siguientes:

a) Resguardar la identidad digital del usuario: ajustar configuraciones de privacidad de todas nuestras cuentas en redes sociales (Facebook, Instagram, WhatsApp, Linkedin, etc.) y demás plataformas digitales, procurando exhibir a terceros un mínimo de información personal; depurar constantemente la lista de contactos; realizar barridos periódicos en buscadores para detectar filtraciones de datos personales, etc.

b) Mantener controles estrictos de acceso a equipos o cuentas de usuario empleadas: a través de contraseñas alfanuméricas con símbolos especiales; cambio periódico de estas; autentificación multifactor para información importante; utilizar herramientas especializadas para la gestión segura de contraseñas.

c) Implementar sistemas de privacidad frente al monitoreo de actividad en línea por terceros: contratar un servicio de red privada virtual (VPN).

d) Generar periódicamente copias de seguridad de datos e información relevante, y garantizar su acceso en caso de un ataque informático.

Las medidas especiales, por su parte, se enfocan en uno o más riesgos concretos y deben ser adoptadas en caso de exposición frente a estos últimos. En relación con los creadores culturales, resulta indispensable tener presentes los siguientes peligros específicos y las medidas de resguardo respectivas, según se describen a continuación.

3. Ataques informáticos

El primer riesgo que enfrentan los creadores culturales está representado por los ataques informáticos, también denominados ciberataques. Estos se definen como cualquier explotación intencional y maliciosa que tenga como objetivo a los sistemas informáticos, las redes como Internet y los dispositivos personales, como nuestra computadora, nuestra tableta o nuestro *smartphone* (Alexandrou, 2022, p. 235).

No debemos olvidar que, además del uso intensivo de la red Internet –de la que nos hemos vuelto dependientes–, cada vez estamos incorporando más objetos de uso cotidiano que requieren de la red para funcionar. Internet no solo puede usarse a través del teléfono, sino que también en forma integrada en nuestros hogares u oficinas, desde los sistemas que nos permiten remotamente encender la luz, la calefacción o activar la lavadora, hasta un equipo mezclador digital, sistemas antiplagio o galerías digitales de arte. El uso de la red en objetos distintos a una computadora (lo que se denomina internet de las cosas o *Internet of Things*, *IoT*) está evolucionando a paso tan acelerado que ya se habla de la internet de todo, la *Internet of Everything*, *IoE* (Denardis, 2020; Miraz *et al*., 2015). La revolución informática es por hoy un fenómeno presente en casi todos los aspectos de nuestras vidas, mucho más allá de la sola utilización de un ordenador.

A pesar de los impresionantes avances en estas áreas, no hemos sido, sin embargo, capaces de desarrollar programas y máquinas completamente seguras, es decir, tecnologías a prueba de la intrusión de terceros malintencionados. El *software*, en especial, puede adolecer de errores o fallas en su programación que representan vulnerabilidades en su seguridad (Bambauer y Day, 2011, p. 1060). El problema se produce

porque hay personas, con distintas intenciones, dispuestas a explotar esas vulnerabilidades. Tales intenciones pueden ir desde la simple curiosidad, el deseo de demostrar ante colegas especiales habilidades descubriendo y explotando vulnerabilidades, hacer activismo reivindicando alguna causa o interés, obtener beneficios económicos ilícitos o provocar daño patrimonial o personal a personas, empresas o gobiernos.

Es imposible hacer un listado exhaustivo de las formas y tipos de ataques informáticos, porque los *modus operandi* evolucionan a diario sin más límites que los que ofrecen la tecnología y la creatividad humana. Sin perjuicio de ello, se puede establecer una tipología de ataques informáticos que es útil para conocer los riesgos a los que nos enfrentamos en el cibermundo.

a) Los accesos ilícitos

Caso N.° 1: el hacker H accede ilícitamente al computador del músico M y realiza una copia no autorizada de una pieza musical elaborada por este. H luego la sube a una plataforma de reproducción en un metaverso y la ofrece a terceros por vía de *streaming*, previo pago de una suscripción.

La conducta base en la mayoría de los ciberataques la constituye el acceso ilícito a un sistema informático (computador, tableta, teléfono inteligente u otro). La bibliografía especializada ha descrito varias formas en las que se puede lograr dicho acceso y obtener el control de este. De acuerdo con Donaldson *et al*. (2015, pp. 281-ss), este se puede lograr con la ayuda de diversos mecanismos.

Uno de ellos es el *phishing* que, en su variante más simple, consiste en el envío masivo de correos electrónicos o de mensajes de texto que, bajo una apariencia de legitimidad, requieren que los destinatarios envíen datos personales o ingresen a un enlace malicioso que, a su turno, otorga el buscado acceso. En su forma más sofisticada denominada *spear-phishing*, los mensajes están dirigidos a víctimas específicas e incluyen información personal de esta o de su entorno que los hacen más verosímiles e incrementan, de tal forma, la probabilidad de que esta acceda al envío de información o ingrese a los enlaces contenidos en la página.

Captura de pantalla de un mensaje de correo de phishing, supuestamente enviado por un banco chileno. Nótese que el mensaje no se envió desde una casilla institucional del banco (BancoEstado), sino de una que pertenece al servidor "plusconsulting.cl". Otro elemento que permite identificar la falsedad del mensaje es el uso incorrecto del lenguaje (faltas de ortografía, errores de redacción). Fuente: Twitter (@Fipee).

Captura de pantalla de un mensaje de texto (SMS) de phishing recibido supuestamente desde el mismo banco. En él, se solicita al cliente pinche el vínculo, lo que lo llevará a una página que no es del banco en el que se requerirá a la víctima que proporcione su número de identificación y las claves de acceso a su cuenta bancaria. Fuente: Twitter (@Rockitradiocl)

Los correos electrónicos pueden contener también adjuntos maliciosos, denominados *malware*, es decir, programas destinados a infectar y "causar daño a una computadora, al usuario de una computadora, a una red de computadoras, servidor o a un dispositivo móvil en el ciberespacio" (Ngo *et al*., 2020, p. 795). Estos pueden ser de varios tipos según su modo de funcionamiento, siendo los más conocidos los virus, gusanos y troyanos.

Los virus fueron las primeras formas de *malware* conocidos, y se caracterizan por infectar un archivo específico que pertenece a un programa o aplicación, a un sector específico de las partes físicas de un dispositivo (como el disco duro o una memoria externa) o se insertan dentro de una macro, que son partes de lenguaje de programación que usan, por ejemplo, las aplicaciones del paquete Office de Microsoft (Word, Excell, Powerpoint y Access). Reciben este nombre porque imitan el comportamiento de los virus biológicos, adhiriéndose e infectando archivos limpios, dañando lo que tales archivos están programados para hacer (Benias y Leventopoulos, 2019, p. 66). Por su parte, los gusanos son piezas de código malicioso que "pueden efectuar copias completamente funcionales de sí mismas y viajar a través de una red informática o de la Internet por gran número de medios" (Chawki *et al*., 2015, p. 42). A diferencia de los virus, los gusanos no atacan un archivo específico; lo que los distingue es esa capacidad de autopropagarse por una red infectando muchos dispositivos (Anchugam, 2021, p. 142). La tercera clase de *malware*, denominado *troyano*, equivale a "programas maliciosos que se cuelan en la computadora de una víctima disfrazados de software inofensivo" (Chawki *et al*., 2015, p. 42).

Como se indicó, el acceso ilícito constituye una acción preliminar y preparatoria, en la cual el atacante se gana una puerta de entrada al sistema computacional para lograr realizar otro tipo de actos. Una de las posibles acciones del atacante puede consistir en lograr capturar los nombres de usuario y las claves de acceso que la persona afectada usa en su dispositivo. Por ejemplo, un atacante podría conocer cuál es el nombre de usuario y la clave de la cuenta de correo electrónico, de la cuenta del banco o de un mercado digital de la víctima, lo que le permitiría entrar en tales sistemas, suplantándolo, y utilizarlo en beneficio propio. Dicho proceso puede automatizarse mediante programas especiales de-

nominados *keyloggers*, que registran todas las entradas de teclado que un usuario realiza en un sistema, incluidas las contraseñas.

Las técnicas anteriores generalmente tienen como objetivo la sustracción de identidad digital de los usuarios legítimos de servicios, plataformas y redes sociales. Las identidades sustraídas –nombres de usuario, claves, números de tarjetas de crédito, etc.– son luego utilizadas para hacer operaciones como compras online, pagos de servicios o se venden en el mercado negro digital que opera en la *Darknet* o *Deep Web*. Es importante destacar, además, que todas estas técnicas tienen por objeto que la víctima no se percate del actuar del atacante.

De esta forma, cuando se recibe un correo electrónico y se abre para leerlo, puede estar ejecutando un *malware* y, con ello, puede estar entregando el control de su dispositivo a un atacante, pero sin siquiera darse cuenta, lo cual constituye la idea fundamental del ataque (Ngo *et al*., 2020, p. 797). Esto significa que un tercero puede estar extrayendo no solo las claves de acceso del usuario, sino información importante como obras o creaciones en las que esté trabajando y que pueden llegar a ser plagiadas o copiadas.

Los procedimientos y las herramientas más relevantes para impedir este tipo de ataques son los siguientes:

a) Mantener los sistemas operativos y aplicaciones actualizados conforme a las especificaciones de los desarrolladores.

b) Revisar la configuración de seguridad del *router* de wifi: usar cifrado actualizado (a la fecha de edición de la presente guía es el WPA2), cambiar la contraseña de acceso que viene predeterminada de fábrica, mantener actualizado el software controlador (*firmware*) y desactivar posibilidad de acceso remoto al *router*.

c) Configurar adecuadamente los filtros de correo no deseado o *spam*.

d) Elegir e instalar antivirus efectivos[38].

38 La elección del antivirus debe ser cuidadosa, pues la oferta es amplia y no

e) Activar cortafuegos o *firewalls* incorporados en los mismos antivirus o instalados independientemente.

f) Contratar un servicio de red privada virtual o VPN y mantenerlo activado durante la navegación en internet.

g) En caso de redes de equipos o sistemas de *IoT*, realizar test de penetración o *pentesting* para evaluar las vulnerabilidades de los distintos aparatos conectados.

Más allá de estas medidas técnicas, el principal riesgo no emana de vulnerabilidades de los sistemas informáticos propiamente, sino que del factor humano. Los ataques maliciosos más efectivos hacen uso de estrategias de manipulación y de coerción en contra de los usuarios para lograr sus objetivos, lo cual se denomina ingeniería social: se selecciona como objetivo a personas específicas, se les manipula para que otorguen el acceso a sistemas informáticos, divulguen información confidencial o incluso ejecuten inadvertidamente los ataques en contra de sus propios sistemas (Krombholz *et al.*, 2014, p. 2).

En razón de lo anterior, la principal medida de resguardo es mantener una actitud crítica frente a contactos de terceros no solicitados, verificar siempre la identidad del tercero en caso de solicitud de datos personales, e investigar los funcionamientos atípicos o anormales de nuestros equipos o servicios computacionales. La precaución es la herramienta más efectiva para prevenir un ataque o, en caso de haberse iniciado, limitar sus consecuencias.

b) Los ataques propiamente tales

Los ataques en el mundo de las computadoras y las redes de información pueden estar dirigidos a causar cinco tipos de impacto: distorsionar, interrumpir, destruir, revelar o descubrir información (Simmons *et al.*, 2009).

De esta forma, un ataque mediante un malware puede estar orientado a modificar la información que la persona afectada tiene guardada en su dispositivo o en una nube en la que almacena sus archivos con los que trabaja. Se trata

siempre beneficiosa. Algunos programas de este tipo en realidad incorporan funcionalidades de registro de actividad en línea y recolectan datos personales que luego son incorporados a bases de datos.

de la distorsión de información y, en virtud de este tipo de ataques, usted puede descubrir que un archivo en el que ha trabajado durante un tiempo, de un momento a otro, ha perdido su formato o parte de su contenido.

La interrupción es la forma de afectación que persiguen algunos tipos de ataques y que significa que ciertos servicios no estarán disponibles durante un período cuya duración puede ser variable. Piense que un día usted necesita ingresar a su cuenta del banco para realizar una gestión urgente en ella; a pesar de que ha escrito bien la dirección web de su banco en el navegador y que su conexión a Internet funciona correctamente, le es imposible acceder a ella. En este caso, es muy probable que su banco haya sufrido un ataque cibernético de los que se conocen como denegación de servicio (*Denial-of-Service, DoS*) o denegación de servicio distribuido (*Distributed Denial-of-Service, DDoS*). Los sitios web que visitamos a diario están en distintas computadoras, cada una de las cuales recibe el nombre de servidor (*host*).

Cada servidor tiene la capacidad de atender a muchos usuarios a la vez, es decir, muchas personas que están requiriendo ingresar al mismo tiempo a esa página web. No obstante, aunque la capacidad para atender usuarios es alta, es, sin embargo, limitada. Un ataque de denegación de servicios se produce cuando intencionadamente se generan miles o millones de requerimientos a un sitio web que hacen que el servidor no pueda procesarlos todos y, en consecuencia, el servidor no es capaz de atender a ninguno de los pedidos. ¿El resultado?: la página web se cae y deja de prestar servicios. Los ataques de denegación de servicio se han transformado en un método común de ataque (Harper et al., 2018, p. 507). La palabra Mirai seguramente le es familiar porque es el nombre de la protagonista de una película de animación (Japón, 2018, escrita y dirigida por Mamoru Hosoda; producida por el Studio Chizu), pero es también el nombre de un malware de tipo "gusano" que fue el causante de dos ataques de denegación de servicios en 2016, considerados de los más grandes de su tipo y que afectaron al blog de seguridad de Brian Krebs y a los servicios de nube de la empresa francesa OVH (hoy OVHCloud).

Otro aspecto interesante de estos ataques es que ellos fueron ejecutados no desde computadoras infectadas, sino desde dispositivos del internet de las cosas, es decir, desde

routers domésticos, cámaras de vigilancia de casas particulares y grabadores digitales de video.

El *malware* Mirai buscó incesantemente a través de la Internet dispositivos a los que infectar tan solo con un listado de 62 nombres de usuarios y claves de seguridad usuales. Aunque parezca increíble, Mirai logró infectar miles de dispositivos asociados al internet de las cosas cuyas medidas de seguridad eran débiles: los nombres de usuario y las claves de esos dispositivos eran comunes (como claves 1111) o porque muchos de sus usuarios no habían cambiado las *passwords* que, por defecto, venían configuradas de fábrica. Los miles de dispositivos infectados por Mirai actuaron como un ejército de *botnets* (contracción de las palabras *robot* y *network*, robot y red) que, al mismo tiempo, se conectaron con los sitios webs atacados, lo que produjo una cantidad de requerimientos que superaba las capacidades de los servidores, haciendo que estos dejaran de funcionar.

Su computadora, su lavadora, su Tablet o cualquier dispositivo que esté conectado a Internet puede ser usado por un hacker como un *botnet* para un ataque de denegación de servicios. Así, mientras usted está trabajando en su *laptop*, y sin que tenga conocimiento ni aun sospechas, ella puede estar contribuyendo a un ataque de esta naturaleza porque previamente fue infectada por un malware que hizo que su dispositivo se comportara de esta forma.

Un ataque especialmente grave que puede darse en materia de interrupción (también de destrucción y revelación de información) es el que se conoce como *ransomware* (Ryan, 2021, p. 17), una denominación que engloba un conjunto de ataques con comportamientos heterogéneos (Seth *et al.*, 2022, pp. 157–160). En este tipo de ataque, un dispositivo individual o un conjunto de dispositivos conectados a una red de empresa, por ejemplo, son infectados por un *malware* que bloquea el acceso a la información contenida en ese dispositivo, haciendo que este deje de estar disponible.

Los atacantes, llamados secuestradores, amenazan con borrar la información bloqueada o de difundirla públicamente si no se paga un rescate por esta. Algunos de estos secuestros pueden ser reversados con relativa facilidad por personas expertas; pero otros más sofisticados, encriptan la información, lo que la hace irrecuperable a menos que se co-

nozca la clave de desencriptación[39] y para obtenerla, se debe pagar o cumplir la condición impuesta por el secuestrador (Anchugam, 2021, p. 142). Cualquiera de nuestros dispositivos puede ser objeto de un *ransomware* (de *ranson* y *software*, secuestro y programa) que, como se dijo en el apartado anterior, puede llegarnos, por ejemplo, a través de un correo electrónico con apariencia inocente.

Mensaje que recibieron miles de víctimas del ataque por el ransomware "WannaCry" en mayo de 2017. Este anunciaba: "Sus archivos importantes están encriptados. [...] Nadie puede recuperarlos sin nuestro servicio de descifrado. [...] Envíe el equivalente a 300 dólares en Bitcoin, o sus archivos se perderán por siempre".

Dentro del impacto de interrupción de un ataque informático debe mencionarse un tipo específico de estos que se denomina *webnapping*. Esta modalidad se dirige a los activos intangibles de personas, organizaciones o empresas que

39 La encriptación es el "proceso de convertir información ordinaria en una forma incomprensible y la desencriptación, el proceso de revertir una encriptación o de convertir información incomprensible a una forma ordinaria" (Ngo *et al*., 2020, p. 801). La encriptación tiene una larga historia y fue el método usado por el ejército Nacional-Socialista durante la II Guerra Mundial para hacer que sus comunicaciones fueran indescifrables para los enemigos con la ayuda de una máquina mecánica de cifrado llamada Enigma. Los británicos lograron descifrar los códigos alemanes gracias al genio de Alan Turing (considerado uno de los padres de la informática) y del matemático Gordon Welchman, quienes diseñaron una computadora analógica de desencriptación. Este hallazgo, según los historiadores, habría acortado la duración de la guerra en dos años, salvando la vida de millones de personas.

solamente están protegidos por una cuenta en línea, tales como las claves de acceso al mantenimiento de su sitio web, las cuentas de la organización en redes sociales, canales de comunicación u otros servicios. El atacante sustrae las credenciales de acceso de estos sitios o cuentas y luego, las usa para difundir su propia información o para cobrar un rescate por la restitución de tales claves (Donaldson et al., 2015, p. 289). Si usted tiene un sitio web o una cuenta en redes sociales (por ejemplo, en Twitter, Facebook o Instagram) que usa para difundir su trabajo, comunicar información sobre este o contactar con otros creadores, ese sitio o esas cuentas son un activo; y se clasifican como intangibles porque ellos representan un valor (que puede ser muy alto), pero no es un objeto material como una computadora. Ese sitio web o esa cuenta en redes sociales le reporta beneficios económicos o profesionales, directos o indirectos. Al tener un valor, ella se transforma en un activo y, adicionalmente, en un objetivo para un atacante.

Si usted es víctima de un ataque del tipo *webnapping*, perderá el control que tiene sobre su sitio web o su cuenta en redes sociales, por lo que el uso que hace de ellos será interrumpido. Aunque la mayoría de las plataformas cuenta con sistemas de seguridad y de atención al cliente que pueden ayudarle a recuperar el control perdido de tales servicios por el ataque, es necesario que usted haya activado esos mecanismos de seguridad, según veremos en el apartado siguiente.

El *webnapping* es una forma de secuestro (*hijacking*) en general. Como consecuencia de este, el usuario es despojado del control de los servicios web que utiliza; y tal control, asumido por el atacante, es utilizado por este para ejecutar sus propios objetivos ilícitos, como enviar *malware* o *links* maliciosos, dañar la reputación de la víctima o hacer una declaración política (Donaldson et al., 2015, p. 289).

La destrucción de información puede ser el tercer aspecto de impacto de un ciberataque. Este se produce cuando el ataque borra archivos o elimina información importante. La destrucción es el impacto más dañino que puede causar un ciberataque porque implica la pérdida de información por parte del afectado (Simmons *et al.*, 2009, p. 5). En virtud de esta acción perjudicial, una persona puede perder todo su trabajo si no adoptó medidas preventivas adecuadas como el

respaldo. Un ataque de destrucción equivale a la sustracción de la computadora producto de un robo.

Entre los ataques de destrucción destaca el conocido como quemado (*burndown*) que destruye toda la infraestructura del sistema informático de la víctima, o una parte importante de ella, lo que hace que la persona afectada no pueda usar sus sistemas informáticos, "haciéndola retroceder a la era del lápiz y el papel" (Donaldson *et al.*, 2015, p. 292); y, lo que es más preocupante, perdiendo todo el tiempo y recursos que haya invertido en la búsqueda, recopilación o elaboración de la información destruida.

El cuarto tipo de impacto es de la revelación de información. En este caso, el ataque tiene por objeto capturar información relevante del afectado y luego revelarla, haciéndola pública. Este tipo de ataques puede tener impacto económico, pero también en otros derechos como la intimidad de la víctima. Lo anterior, porque la información revelada no solo se refiere a cuestiones vinculadas con los desarrollos o creaciones en las que la víctima haya estado trabajando y que por culpa de la divulgación pierden su valor económico, sino porque la información hecha pública pueden ser datos privados, confidenciales o sensibles de la persona afectada y que estaban almacenados en un dispositivo informático.

En la categoría de impacto de revelación, el ataque de difamación adquiere transcendencia. En este caso, la información se usa para lesionar el honor de la persona víctima, haciéndola perder o disminuir la estima que sus pares tienen de ella.

El espionaje es también un tipo de ataque que se relaciona con la revelación, ya que, en este caso, el atacante conoce el trabajo de la víctima que esta había decidido mantener en secreto mientras aquel no se concluyera. Piénsese en el manuscrito de una novela, en un proyecto artístico o un diseño en elaboración. Un atacante podría usar esa información y venderla, entregándole a otro "creador" una ventaja indebida por el conocimiento anticipado de los proyectos en los que la persona afectada estaba trabajando.

Un tipo de ataque que tiende a ser subvalorado en su real dimensión dañina, es lo que se conoce como *graffiti* y que consiste en que el atacante logra tomar el control de una página web o un *fanpage* en Facebook de la víctima, por

ejemplo, y altera su contenido para transmitir los mensajes o las reivindicaciones en las que el atacante está interesado. De un momento a otro, su página web puede aparecer defendiendo causas con las que usted no solo no se identifica ni le interesan, sino que, además, pueden ser contrarias a sus propias convicciones. El *graffiti* como forma de ataque puede provocar a la víctima un deterioro de su imagen pública, una confusión de sus clientes o seguidores o una pérdida de confianza de estos. Todos esos daños pueden traducirse, directa o indirectamente, en pérdidas económicas.

4. Violaciones de marca y defraudaciones

Caso N.º 2: la artista A diseña prendas y accesorios digitales inspirados en productos de propiedad de la empresa de moda M, los transforma en NFT (Non-Fungible Token), y los vende a consumidores en el mercado digital. La empresa M presenta una demanda en contra de A, reclamando una infracción de marca y, con ello, que A le pague los perjuicios sufridos por dicha infracción (indemnización de perjuicios). Al percatarse de la falta de originalidad de los NFT, los compradores, por su parte, denuncian a A ante la policía o la fiscalía porque se consideran víctimas de un delito de estafa por parte de A.

La incorporación de tecnologías emergentes en la generación y divulgación de contenido artístico o cultural también implica riesgos específicos para los involucrados. Esto es especialmente evidente en el contexto de la masificación en el uso de NFT para la creación de arte digital. Los creadores culturales buscan con ello aprovechar las ventajas de no fungibilidad, transferibilidad y la certificación de autenticidad que ofrecen estos instrumentos, para realizar transferencias de contenido artístico en mercados digitales de modo directo, rápido y seguro.

Sin embargo, como vimos antes, los NFT, al basar su arquitectura en la tecnología *blockchain*, poseen una serie de características relevantes desde el punto de vista criminal (Bedecarratz, 2018, pp. 86 y ss.). Es por ejemplo posible que determinadas creaciones culturales tales como una pintura o un diseño gráfico sean objeto de un NFT, distinto del objeto original, pero igualmente no fungible y transferible. En el último tiempo ha alcanzado notoriedad la conducta de terceros que crean NFT respecto de creaciones artísticas, en rela-

ción con las cuales no tienen ningún derecho. Dichos sujetos luego enajenan los NFT a título propio y con ánimo de lucro. La conducta descrita configura el delito de plagio, que consiste en copiar en todo o en parte una obra ajena sin hacer mención a su autor, privándolo del derecho a ser conocido como el autor de esa creación.

El delito de plagio puede implicar para los compradores una decepción en cuanto a una característica esencial del objeto transado, que es su fuente u origen: este es generado por un tercero, no por el artista original. El problema se agrava, precisamente, por la facilidad de creación y pseudoanonimato que rodean a los NFT, que dificultan la persecución penal de los sujetos que se sirven de este tipo de instrumentos para lesionar intereses de artistas y de compradores.

Con el fin de reaccionar a tiempo frente a este tipo de conductas, se sugiere realizar búsquedas regulares en los mercados digitales más relevantes para el rubro cultural en el que se desenvuelve, con el fin de comprobar que una obra propia no ha sido plagiada por un tercero. En caso de detectarse la venta no autorizada por parte de terceros de NFT representativos de una creación cultural propia, lo que corresponde es denunciar el hecho a los administradores del mercado digital en concreto.

Diversos sitios (por ejemplo, OpenSea o Cent) han comenzado a implementar políticas de cero tolerancia frente a este tipo de fraudes, por lo que en caso de ser detectados, las ofertas son suprimidas. Si lo anterior falla, la forma más efectiva de lograr la eliminación del material plagiado de las plataformas es denunciar el hecho a través de los canales institucionales y ejercer presión sobre el sitio dándole adecuada publicidad en redes sociales y comunicacionales.

5. Falsificaciones

Caso N.° 3: una persona utiliza un algoritmo basado en IA para sustituir el rostro de una participante de un video pornográfico, por el de una actriz de televisión, lo que resulta en un *Deepfake*. Este video adulterado, luego es difundido en portales de adultos, lo que ocasiona un daño a la imagen pública de la actriz y obliga a la propia víctima a realizar desmentidos.

La IA constituye una tecnología de uso dual: puede ser utilizada para fines beneficiosos o dañinos (Brundage et al.,

2018, p. 16). Lo anterior ha sido demostrado, entre otros episodios, por la masificación de pornografía no consensual mediante *Deepfakes* a partir de 2017. Terceros maliciosos aprovecharon las capacidades de generación gráfica de la tecnología IA para crear videos para adultos con las imágenes de terceras personas y difundirlos a través Reddit y otros foros masivos en Internet. El progreso en las capacidades de generación gráfica de la IA también puede ser utilizado con fines delictivos y derivar en profundos daños en la imagen de las víctimas.

El riesgo descrito no se circunscribe a materia de pornografía no consensual. La capacidad creadora de la IA, así mismo, es empleada para presentar obras artísticas falsificadas tales como un diseño gráfico, una pieza de arte digital o una composición musical, imitando el estilo, los trazos o incluso la voz de los autores originales, con el fin de vender luego estas creaciones en el mercado digital. De tal modo, se crea mediante un algoritmo una pieza artística original con la apariencia de haber emanado de un artista determinado, pero que en realidad es falsa y replica exactamente su estilo. Se trata de una reedición digital del caso de los Huevos Fabergé falsificados: piezas de arte con un estilo particular y muy preciadas, que luego son replicadas y vendidas por terceros. Al igual que en este ejemplo histórico, se crea una falsificación que lesiona a los artistas originales y defrauda a los compradores, que piensan estar adquiriendo una obra verdadera y no una imitación.

Falso NFT de Bansky que fue subastado por un coleccionista de arte en un Marketplace digital en septiembre de 2021 por un valor de $335.000 dólares. Los NFT también pueden ser usados en conductas complejas que combinan distintos tipos de fraude, como ocurrió en este caso.

Las capacidades de la IA permiten hoy en día la generación de contenidos culturales con tales características en el ámbito de la pintura, el diseño digital, música, la poesía y otras. Al mismo tiempo, el uso de herramientas cada vez más sofisticadas para producir imitaciones tales como las redes generativas antagónicas[40], dificultan progresivamente los análisis de originalidad por parte de compradores.

Galería de rostros generados por IA (Fuente: https://generated.photos/)

Debido a lo anterior, la medida de protección más relevante es realizar un control estricto de los mercados digitales en los que se difunden las creaciones culturales, asegurándose de que la comercialización de contenidos propios provenga siempre de fuentes visadas por el autor. En ese sentido, puede ser recomendable tercerizar la gestión de contenido a curadores digitales de arte que cuenten con los conocimientos y las herramientas adecuadas para detectar, denunciar y perseguir creaciones fraudulentas. Por otra parte, sería aconsejable el uso de *softwares* para la detección de falsificaciones, similares a los desarrollados el último tiempo para la identificación de *Deepfakes*, lo cual permitiría tomar las medidas correspondientes en la plataforma respectiva.

6. Fui víctima: ¿qué hago?

Como ya vimos, la medida más relevante y efectiva para hacer frente al riesgo digital es el autocuidado. Es indispensable tomar las precauciones descritas en el presente capítulo, con el fin de disminuir la probabilidad de ser víctimas de un

40 Sistema conformado por dos redes neuronales que compiten entre sí: la primera una generativa, que produce nuevas imágenes sobre la base de la información que se le ha suministrado; la segunda una discriminadora, que juzga si las creaciones de la primera son reales o falsas. Ambas redes neuronales interactúan constantemente, aprendiendo a generar mejores imitaciones o a detectar más exactamente su veracidad, respectivamente. Dicha herramienta ha redundado, por ejemplo, en rostros artificiales cada vez menos distinguibles respecto de uno real.

ataque, fraude o falsificación en el contexto de las tecnologías emergentes. Sin embargo, si ello no ha sido suficiente y se es de todos modos víctima de una acción maliciosa de terceros, en tal caso es esencial tomar una serie de medidas.

La prioridad inicial es contener y controlar los resultados negativos, en lo posible contrarrestando el ataque, fraude o falsificación, lo cual requiere una actitud persistente y extendida en el tiempo. En ese sentido se recomiendan las siguientes medidas inmediatas:

- Identificar, siempre que sea posible, al o a los autores iniciales del ataque, falsificación o defraudación, idealmente a la persona, pero, en su defecto, a las cuentas de usuario involucradas.

- Reportar y denunciar perfiles, publicaciones o mensajes conectados con el ataque, falsificación o defraudación en la plataforma, mercado digital o metaverso respectivo. Estos generalmente contemplan como política la clausura de cuentas involucradas con este tipo de hechos.

- Reportar los mensajes vinculados al acto malicioso en las redes sociales en las que se haya verificado o difundido el hecho (Facebook, Instagram, TikTok, Twitter), con el fin de limitar sus repercusiones negativas.

Con todo es necesario tener presente, que las acciones que se tomen no pueden tener como expectativa eliminar completamente el acto malicioso, sino que solamente limitar sus efectos negativos. Debido a lo anterior y, en segundo lugar, es indispensable activar la institucionalidad encargada de resguardar nuestros derechos digitales y realizar las siguientes acciones:

- Denunciar los hechos ante la unidad de cibercrimen de la policía respectiva (Policía de Investigaciones de Chile, Policía Nacional de Colombia, según el caso) para que inicien investigaciones respecto del hecho y las personas responsables.

• Evaluar, según el caso y previo análisis de costo beneficio, la posibilidad de iniciar acciones legales en contra de los responsables por las siguientes vías:

- Querella penal para intervenir activamente en el proceso penal.

- Demanda infraccional por vulneración de los derechos de autor.

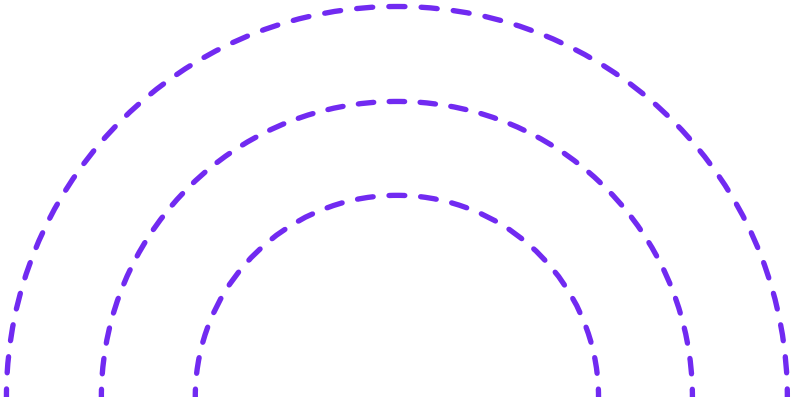
- Demanda civil por indemnización de perjuicios.

Sección 8

RECOMENDACIONES PARA LA PROTECCIÓN DE DERECHOS DE LOS CONSUMIDORES EN EL USO DE TECNOLOGÍAS EMERGENTES

Betty Martínez-Cárdenas

Sebastián Bozzo Hauri



1. ¿Cuál es el régimen legal para la protección de los consumidores en el uso de tecnologías emergentes?

Ni en Colombia ni en Chile existe una reglamentación exactamente destinada a los consumidores que utilizan tecnologías emergentes. Durante mucho tiempo se ha entendido que la reglamentación existente para el comercio análogo puede aplicarse por aproximación al comercio digital, con algunos ajustes particulares incluidos en los estatutos generales de protección al consumidor y en algunos reglamentos o guías expedidos por las entidades fiscalizadoras. En este capítulo se presentarán tanto las normas que, por analogía, pueden ser aplicadas en materia de comercio desarrollado con el uso de tecnologías emergentes, como los especiales cambios legislativos que se han introducido en este sentido, tanto en el ámbito legal propiamente dicho, como en el reglamentario. Estos cambios tienen como base fundamental la guía que para comercio electrónico elaboró la OCDE en 2001, y la muy reciente guía 2021 IA, todo lo cual será mostrado a continuación.

1.1. ¿Cuál es la reglamentación aplicable al comercio con el uso de tecnologías VPN emergentes?

Como lo señalábamos previamente, para una mejor comprensión del tema, debemos comenzar por las guías transnacionales de la OCDE, para luego determinar quiénes son sujetos de respetar estas medidas de protección.

1.1.1. Las guías transnacionales de la OCDE y la protección al consumidor que usa tecnologías emergentes

Son dos los desafíos más importantes en materia de regulación para la protección del consumidor. El primero, es el de las fronteras territoriales y la fragmentación del mercado; el segundo, el que el exceso de regulación frene la competitividad en la región. Si bien, de un lado, el comercio electrónico es, por naturaleza, transnacional; del otro, los estatutos de protección al consumidor son territorialistas y de orden público dentro del territorio en el que rigen, así que la pregunta que se formula acá es: ¿Cómo regular la protección del con-

sumidor en el orden transnacional y promover la competitividad al mismo tiempo?

Para responder a esta pregunta, agencias internacionales encargadas justamente de la promoción del desarrollo, en particular para los países que son miembro de ellas, han redactado guías que permiten a los Estados adecuar su regulación interna hacia un propósito común. Este propósito respeta los intereses transnacionales, y la "suavidad" de la guía (*soft law*) permite dar a las normas la flexibilidad adecuada para evitar, o al menos intentar evitar una fragmentación del mercado y el desarrollo de la tecnología de manera abierta.

Para Colombia y Chile, por ser países miembros de la Organización para la Cooperación y el Desarrollo Económico (OCDE), es indudable que las guías expedidas por esta organización son fundamentales para la comprensión y el desarrollo de la reglamentación interna.

Desde el año 1999, y en particular con la "Recomendación del consejo de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico" expedida en el año 2001, se han dado los parámetros básicos para la protección al consumidor en estos dos países. Pero, la labor de la OCDE no quedó allí. A continuación, presentamos el cuadro de las recomendaciones que ha emitido en materia de comercio electrónico e inteligencia artificial hasta la fecha:

Cuadro 1. Recomendaciones de la OCDE para la protección del consumidor en el marco del comercio electrónico y el uso de sistemas con apoyo en la inteligencia artificial.

Norma	Fecha	Hipervínculo
Recomendación del Consejo de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico.	17 de mayo de 2001	https://doi.o g/10.1787/9789264065680-es
Directrices de la OCDE para la protección de los consumidores de prácticas comerciales transfronterizas fraudulentas y engañosas	17 de mayo de 2004	https://doi.org/10.1787/9789264065840-es
Recomendación del Consejo sobre Seguridad en los Productos de Consumo	2020	file:///C:/Users/Usuario/Downloads/e82d-c1e3-05af-42db-b281-e6468826105f.pdf
Recommandation du Conseil Sur l'intelligence artificielle	2022	file:///C:/Users/Usuario/Downloads/OECD-LEGAL-0449-fr%20(1).pdf

1.1.2. ¿Quiénes deben proteger al consumidor que contrata con el uso de tecnologías emergentes?

Las recomendaciones de la OCDE están dirigidas a todos los actores en el comercio electrónico, con lo cual, si bien puede haber obligaciones que se impongan a algunos de ellos de manera específica, el espíritu de estos lineamientos es fomentar una cultura de cuidado entre todos los partícipes del mercado. Así, los lineamientos se dirigen "i) a los gobiernos para la revisión, formulación e implantación de leyes, prácticas, políticas y regulaciones en materia de consumo, para lograr una efectiva protección del consumidor en el contexto del comercio electrónico; ii) a las asociaciones empresariales, grupos de consumidores y organismos autorregulatorios, proporcionándoles la orientación relativa a los principios básicos que deben considerarse en la formulación e instrumentación de esquemas de autorregulación en el contexto

del comercio electrónico; iii) de manera individual a los empresarios y consumidores involucrados en el comercio electrónico, proporcionándoles una clara guía sobre las características fundamentales que debe contener la información que se difunda por este medio, así como de las prácticas comerciales equitativas que los empresarios deben realizar y que los consumidores tienen derecho a recibir en el contexto del comercio electrónico" (OCDE, 2001, págs. 2, 3).

2. ¿Cuál es el contenido de la protección?

En conjunto, este cuerpo de recomendaciones, políticas, leyes, reglamentaciones y guías han venido perfilando tendencias en la protección al consumidor que podemos mostrar claramente durante toda la relación de consumo o iter contractual, así como otras que se dirigen a cada una de las etapas del contrato, y aquellas que pudieran estar a cargo del consumidor.

2.1. ¿Cuáles son las herramientas de protección del consumidor durante todo el iter contractual?

2.1.1. Obligación de transparencia en la información

La obligación de transparencia en la información consiste en garantizar que el consumidor se entere, de manera efectiva, de todos los elementos necesarios para contratar, para retractarse, para activar la garantía y las acciones que correspondan según el caso.

Así, básicamente, aquel que ponga a disposición el bien o el servicio a través del comercio electrónico, antes de llevarse a cabo la compra, debe presentarse, esto es, dar información sobre la empresa, que llevaría a evitar justamente un error sobre la persona; segundo, debe presentar los bienes o servicios, lo que llevaría a evitar un error sobre la sustancia; y, tercero, deberá dar la información relativa a la transacción, que resguardaría al consumidor a incurrir en un error sobre el tipo de contrato[41].

41 En Chile, el detalle de cada uno de estos tipos de información ha sido especificado por el Decreto 6 de 2021 del Ministerio de Economía, Fomento y Turismo, de forma tal que es posible realizar un seguimiento sobre la manera como fue dada esta información al consumidor. En Colombia, el contenido de la obligación de información y su eficacia a partir de la transparencia se presenta de manera más general y en forma de recomendación en la Guía para la Protección del Consumidor en el Comercio Electrónico de la Superintendencia de Industria y Comercio. Sin embargo, cabe aclarar que, en esta guía se hace una distinción

¿Quiénes son los que tienen a su cargo la obligación de información?

Básicamente, el vendedor es quien tiene a su cargo la obligación de información. Ahora bien, cuando la venta se realiza a través del comercio electrónico y mediante el uso de tecnologías emergentes, los actores pueden ser varios, según si el productor no es el mismo vendedor, y si utilizan o no su propia plataforma electrónica o *market place* para realizar la transacción. En consecuencia, diremos que en conjunto son sujetos de la obligación de información el productor, proveedor y los intermediarios, esto es, las plataformas electrónicas que no pertenecen ni al productor ni al distribuidor, sino que actúan como meros intermediarios, y como tales, están regidos por las normas del contrato de mandato.

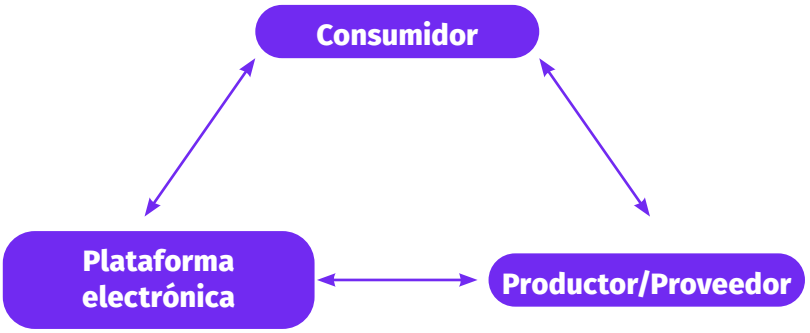
¿Cómo debe cumplirse la obligación de información?

La manera como debe cumplirse esta obligación de información depende del rol que dicho vendedor juegue dentro de la relación. Aquí, es muy importante comprender que el uso de un intermediario o de una plataforma electrónica no exime al proveedor de las obligaciones que ponen a su cargo la obligación de información, pero que, es la manera como va a cumplir esas obligaciones la que puede cambiar. Así, cuando es el productor/proveedor quien utiliza su propia plataforma electrónica, estaríamos hablando de una relación de consumo, y, por tanto, es él quien directamente debe dar cumplimiento a la obligación de información; en tanto que cuando el productor/proveedor utiliza los servicios de la plataforma como un mero intermediario, dependerá de lo que se haya acorda-

entre los actores del comercio electrónico, y en particular, al establecer que el operador de una plataforma electrónica puede ser un simple portal de contacto, cuando dicha plataforma electrónica se utilice únicamente para "que personas naturales o jurídicas puedan ofrecer productos para su comercialización y a su vez los consumidores puedan contactarlos por ese mismo mecanismo", con lo cual, el operador tendría únicamente un rol de intermediario.

do en el contrato de intermediación (o mandato) determinar hasta qué punto el intermediario asumió la carga de informar al consumidor. No obstante, estos acuerdos entre proveedor/productor e intermediario son solo oponibles entre ellos; frente a terceros, como los consumidores, dichos acuerdos no tienen validez debido a que la obligación de información impuesta por los Estatutos de Protección al Consumidor es de orden público, por lo que ningún acuerdo contractual interno puede variar su naturaleza ni efectos. La única diferencia es que, frente al consumidor, ya no se estaría ante una relación de consumo, sino ante un ciclo de consumo.

Es por ello que, con independencia del rol que se asuma, la información siempre debe llegar completa al consumidor, sea porque el productor/proveedor la suministre directamente a través de su propia plataforma electrónica, sea porque la entregue al intermediario para que, a su vez, sea este último quien la haga llegar al consumidor.



¿En qué consiste la obligación de información?

Previamente mencionamos que se trata de, primero, dar información sobre la empresa; segundo, presentación de los bienes o servicios; y, tercero, deberá dar la información relativa a la transacción. Además, agregaremos un cuarto punto, relativo a la información sobre el uso de sistemas con apoyo en la inteligencia artificial (ia).

a. Información sobre la empresa

Se trata de la información tanto del productor/proveedor del bien o del servicio, como del operador de la plataforma electrónica. Recordemos que esta información debe estar destinada a evitar que el consumidor incurra en un error en la persona con quien contrata. En consecuencia, datos como la identificación (documento de identidad), nombre o razón social, dirección de notificación judicial, teléfono, correo electrónico y otros (registros de prestadores de servicios turísticos o ante Cámaras de Comercio, por ejemplo) son fundamentales en esa etapa.

En relación con los influenciadores que utilizan sus espacios en redes para publicitar productos o servicios, la Superintendencia de Industria y Comercio de Colombia recomienda identificarse como anunciante y explicar al consumidor de forma clara en qué consiste su rol como tales (SIC, 2022, pág. 18).

b. Información sobre la naturaleza de los bienes o servicios ofertados

Segundo, para brindar información sobre los bienes o servicios ofertados, es importante mostrar las características y propiedades de estos, de manera tal que queden suficientemente individualizados frente a otros similares en el mercado, con el fin de que el consumidor pueda hacer comparaciones y tomar una decisión libre e informada.

c. Información sobre la transacción en línea

Tercero, sobre la transferencia, las recomendaciones de la OCDE velan porque haya una absoluta transparencia y veracidad en el precio y la forma de pago. Así, se exige "(i) un desglose de los costos totales cobrados y/o impuestos; (ii) notificación de la existencia de otros costos aplicados rutinariamente al consumidor, y que no son cobrados y/o impuestos por la empresa; (iii) términos de entrega o prestación del servicio; (iv) términos, condiciones y formas de pago; (v) restricciones, limitaciones o condiciones de compra, tales como requerimientos de autorización de los padres o tutores, restricciones geográficas o de tiempo; (vi) instrucciones para el uso adecuado del producto, incluyendo advertencias de seguridad y cuidado de la salud; (vii) información relativa a la disponibilidad de servicios posteriores a la venta; (viii)

información y condiciones relacionadas con la retractación de la compra, terminación, devolución, intercambio, cancelación y/o políticas de reembolso; y (ix) pólizas y garantías disponibles" (OCDE, 2001, pág. 7).

d. Información sobre el uso de sistemas con apoyo en la inteligencia artificial (IA)

Finalmente, si para la transacción y, además, para facilitar la prueba de quién y cómo fue suministrada la información al consumidor por parte del operador de la plataforma, este acude a sistemas de información con apoyo en la IA, de conformidad con la Circular Interpretativa sobre protección de consumidores frente al uso de sistemas de inteligencia artificial del SERNAC, es necesario que el operador de la plataforma informe al consumidor sobre la utilización de estas herramientas tecnológicas.

Así, el operador, sin perjuicio del contenido de la obligación de información relativa al consumo de un bien o servicio, debe, durante todo el contrato y adicionalmente: a) velar porque el consumidor sepa que está interactuando con un sistema de IA; b) informar si el sistema de IA contiene a su vez un sistema de reconocimiento de emociones y de categorización biométrica; c) informar si el sistema de IA genera o manipula imágenes o contenido de audio y video, y si este puede a su vez ser manipulado de manera artificial; d) informar sobre el tratamiento que se les dará a los datos personales que son empleados por el sistema.

Es así como, no solo se siguen respetando los roles asignados por los Estatutos de Protección al Consumidor, sino que se mantiene el objetivo de garantizar que el consumidor acceda de manera transparente a la información y se contribuya a consolidar la confianza en el mercado electrónico, incluso cuando se utilicen sistemas con apoyo en la IA.

2.2. Herramientas de protección previstas para la etapa precontractual

La gran mayoría de estas herramientas se refieren a las obligaciones que de buena fe se imponen a las partes antes de contratar en beneficio del consumidor Esta buena fe, en materia de consumo y, en particular, de comercio digital, se traduce en aumentar las exigencias

frente al productor/proveedor/operadores de plataformas electrónicas, al paso que aligeran las obligaciones del consumidor (Picod & Davo, 2010).

Por ejemplo, en Chile, en un principio, los Estatutos de protección al consumidor se ocuparon de que cuando un productor/proveedor utilizara las plataformas electrónicas con consumidores, el primero debía instruir a los segundos sobre el uso de esta y "entregar un buen detalle del producto" (Barrientos Zamorano, 2013, pág. 95) (inciso segundo del artículo 32 de la Ley 19.496), ya que el no hacerlo, la "falta de información objetiva y veraz constituye un obstáculo para la libre elección" (Isler Soto E. , 2013, pág. 746).

Posteriormente, esta tendencia a hacer más gravosas las obligaciones para el proveedor/productor continuó con el literal B. de la Circular sobre Buenas Prácticas del SERNAC del año 2018, aumentó el contenido de la obligación de información para incluir en él los datos "sobre el proceso de transacción electrónica, sus medios, alcances, seguridad, resguardos, entre otros aspectos que los consumidores requieran tomar conocimiento, evitando el ocultamiento o entrega de información confusa para aquel".

Luego, para 2021, Título II del Decreto 06 del 21 de marzo, del Ministerio de Economía, Fomento y Turismo, impuso a los operadores de plataformas electrónicas o marketplaces "el deber" de informar al consumidor no solo sobre lo previamente mencionado, sino además sobre: los datos del vendedor (entiéndase por productor/proveedor); el rol del operador de la de la plataforma, la contratación, el costo total de la transacción, stock y disponibilidad de los productos, la entrega, despacho o retiro del producto; el derecho de retracto; el soporte de contacto; los términos y condiciones del contrato y de si se trata o no de un contrato de tracto sucesivo.

Para finalizar, esta tendencia se concretó con la muy reciente Circular Interpretativa sobre protección de

consumidores frente al uso de sistemas de inteligencia artificial del SERNAC, según la cual, "en términos generales, los proveedores deben entregar al consumidor información significativa (...) respecto a "a) el objetivo o finalidad de los sistemas de IA empleados; b) su injerencia en el proceso de contratación o de ejecución del contrato (...); c) la naturaleza de la interrelación del sistema de IA con el consumidor (...) en particular, si el consumidor está interactuando con un sistema de IA y no con un ser humano; d) los datos personales que son tratados por el sistema, incluyendo todos los tipos de tratamiento que tienen lugar para llegar a una decisión por parte del sistema de IA y su finalidad" (SERNAC, 2022).

En Colombia, esa misma tendencia hacia hacer más gravosa la obligación precontractual de información para el productor/proveedor que utiliza comercio electrónico, es posible percibirla en los artículos 50 y siguientes de la Ley 1480 de 2011 y, aunque no exista por el momento reglamentación alguna en torno al uso de IA en la comercialización de bienes o servicios para el país, las recomendaciones de la OCDE sobre esta materia son particularmente importantes para evitar fragmentar el mercado. Estas recomendaciones fueron seguidas por la Circular del SERNAC que ya hemos mencionado.

En cambio, en relación con la información precontractual, tanto en Chile como en Colombia, solo existen deberes generales (Barrientos Camus, 2015), tales como el de leer la información que el proveedor/productor/operador de plataforma electrónica le suministra, mantenerse actualizado y educarse sobre los derechos que le ofrece el ordenamiento jurídico respectivo. Al no ser estos deberes una obligación, el cumplimiento de ellos no puede serle exigido al consumidor de manera coactiva ni constituyen causa de exoneración de responsabilidad para el productor/proveedor/operador de la plataforma electrónica. Sin embargo, actuar bajo estos deberes es fundamental para contribuir en la mejora

de la calidad y la eficacia de las medidas de protección que se han creado para el consumidor.
Por ello, en esta sección nos referimos a la obligación del productor/proveedor u operador de la plataforma electrónica de crear un procedimiento de confirmación en la formación del consentimiento, la obligación de advertencia, la posibilidad de insistir en la compra que el consumidor no realizó, los efectos de la huella digital del consumidor, y el especial cuidado que hay que tener con los consumidores menores y los vulnerables.

2.2.1. Procedimientos de confirmación

En efecto, en materia de consumo y, sobre todo, de comercio electrónico, el simple consentimiento no es suficiente para que nazca el contrato. En aras de proteger el consentimiento del consumidor, las directrices de la OCDE y los Estatutos prevén la necesidad de establecer una forma en la emisión del consentimiento, a través de procedimientos de confirmación (artículo 12 A de la Ley 19.496 de Chile e inciso 3, literal d del artículo 50 de la Ley 1480 de 2011 de Colombia).

Así, "con el fin de evitar ambigüedades sobre la intención de un consumidor de realizar una compra, antes de concluirla, el consumidor debe ser capaz de identificar con precisión los bienes o servicios que desea comprar; de identificar y corregir cualquier error o modificación de la orden de compra; de expresar su consentimiento para realizar la compra de manera deliberada y razonada, así como de conservar un registro completo y preciso de la transacción (...). El consumidor debe tener el derecho de cancelar la transacción antes de concluir la compra" (OCDE, 2001, pág. 7).

2.2.2. La obligación de advertencia

Este punto implica también poner al tanto al consumidor sobre el plazo de validez de la oferta de los productos, la disponibilidad de estos,

así como de eventuales dificultades o limitaciones en el uso del bien o del servicio. Por ejemplo, si el bien requiere o no de un servicio adicional técnico para su puesta en servicio, o cuáles son los límites de un servicio turístico ofrecido en un *resort*.

2.2.3. ¿Es posible obligar al consumidor a retomar una compra que él mismo declinó?

En principio, nada obsta para que el consumidor retome una compra que previamente había declinado o que no había terminado. Sin embargo, el consumidor no puede ser forzado a concluir dicha compra. Por esta razón, los operadores de las plataformas electrónicas deben velar porque los sistemas de IA empleados en el marco de una relación de consumo cumplan con los estándares adecuados de precisión, fiabilidad y efectividad técnica, basados en procedimientos confiables, para evitar que estos sirvan para engañar al consumidor sobre su deseo o necesidad de compra. Es decir, los sistemas de IA no pueden ser empleados para manipular al consumidor.

2.2.4. La huella digital

Como es de conocimiento público, "un creciente número de actividades humanas dejan su rastro en sistemas de información digitales que, *a priori*, pueden ser empleados para generar información y conocimiento, entre otros ámbitos, a través de la producción estadística oficial" (Salgado, 2016, pág. 14). Es a este rastro al que se le denomina huella digital.

La huella digital de una persona, con la ayuda de sistemas de IA, puede ser empleada para segmentarla, según el uso que haga de páginas web, de motores de búsqueda, bienes o servicios contratados, con el fin de crear perfiles destinados a fines completamente desconocidos para ella

(Quirós-García, 2021). Sin embargo, todo proveedor/productor/operador de plataforma electrónica debe tener en cuenta que toda práctica de discriminación está prohibida por nuestros ordenamientos jurídicos (Isler Soto E. , 2016).

En materia de comercio electrónico y, en particular, del uso de tecnologías emergentes, las autoridades gubernamentales advierten sobre la necesidad de evitar que estas puedan ser empleadas para crear perfiles de consumidores que puedan ser, luego, discriminados al momento de adquirir otros bienes o servicios, de un lado; o, redirigidos hacia otros bienes o servicios, lo que incluye toma de decisiones en otros ámbitos como elecciones presidenciales, por ejemplo (Schneble, Elger, & Shaw, 2018). Por lo demás, la nueva Ley proconsumidor en Chile permite que el SERNAC pueda iniciar acciones en interés colectivo o difuso contra los responsables de una pérdida de datos en materia de comercio electrónico.

2.2.5. Menores y consumidores vulnerables

Se trata de resguardar a todo consumidor que todavía no cuente con la capacidad de ejercicio o con "la capacidad para comprender la información que se otorga mediante la página web" (SERNAC, 2019, pág. 15), a través de medios que permitan, por ejemplo: a) verificar la edad o la vulnerabilidad del consumidor; b) el registro de la autorización del representante legal de la persona incapaz (art. 52 Ley 1480 de 2011 y SIC , 2022); y, c) informar efectivamente sobre la posibilidad y las forma de ejercer el derecho a retracto.

2.3. Herramientas de protección previstas para específicamente para la etapa contractual

En esta sección veremos los dos principales derechos del consumidor que, además de los que tiene como comprador, le atribuyen los distintos Estatutos de Pro-

tección al Consumidor, a saber, el derecho de retracto, las garantías, y la seguridad en la transacción con la que se lleve a cabo el pago por medios electrónicos.

2.3.1. Derecho de retracto

En Chile, la facultad que se le concede al consumidor para terminar el contrato, de manera unilateral, es conocida también como el derecho de retractación del consumidor (Rodríguez Grez, 2015, pág. 19) o simplemente derecho de retracto. Para ejercer este derecho en comercio electrónico, no solo se le permite al consumidor hacerlo por la misma vía electrónica por la que contrató, sino que se le otorga un plazo de 10 días contados desde la fecha de recepción del bien, o de la celebración del contrato de prestación de servicios, "siempre que el proveedor haya cumplido con la obligación de remitir la confirmación escrita señalada en el artículo 12 A. De no ser así, el plazo se extenderá a 90 días" (literal b, art. 3 bis de la Ley 19.496 de Chile).

En Colombia, el derecho de retracto solo se prevé para los "contratos para la venta de bienes y prestación de servicios mediante sistemas de financiación otorgada por el productor o proveedor, venta de tiempos compartidos o ventas que utilizan métodos no tradicionales o a distancia, que por su naturaleza no deban consumirse o no hayan comenzado a ejecutarse" (artículo 47 de la Ley 1480 de 2011). En estos casos, el consumidor cuenta con hasta cinco (5) días hábiles para ejercer el derecho de retracto.

Adicionalmente, el Estatuto prevé otra forma de desistimiento unilateral denominadas "Reversión del pago", cuando el contrato haya sido celebrado por medios electrónicos y el consumidor sospeche haber sido víctima de fraude, caso en el cual la Ley otorga un plazo de 5 días para la reversión mencionada (art. 51 Ley 1480 de 2011).

2.3.2. Derechos en relación con la garantía

Recordemos que "la garantía legal corresponde al derecho de los consumidores, consistente en la protección, que por ley tienen, frente a casos en los cuales el bien adquirido no cuenta con la calidad esperada, siendo, por lo tanto, inapto para el uso al cual está destinado" (SERNAC, 2019, pág. 14).

Para ejercer este derecho, el consumidor que ha adquirido un bien a través del comercio electrónico y este le ha fallado, puede solicitar, por el mismo medio a través del cual contrató, una de las tres siguientes acciones: o la reparación gratuita del bien; o la reposición de dicho bien; o la devolución de la cantidad pagada.

En Chile, el plazo para el ejercicio de este derecho se extendió a 90 días, en todos los casos (literal b, art. 3 bis Ley 19.496). En Colombia, el término de garantía se fija según la voluntad del productor/proveedor y, a falta de ello, la ley dispone que para productos nuevos será de un año, y para productos usados, tres (3) meses. Este mismo término se otorga para la prestación de servicios. En materia de bienes inmuebles, la garantía legal es de diez (10) años, y de un (1) año para los acabados (art. 8, Ley 1480 de 2011).

2.3.3. Seguridad en la transacción de pago por medios electrónicos

La seguridad debe ser efectiva en relación con los medios de pago (SERNAC, 2019), y de acuerdo con el literal f del artículo 50 de la Ley 1480 de 2011: "sin perjuicio de las demás obligaciones establecidas en la presente ley, los proveedores y expendedores ubicados en el territorio nacional que ofrezcan productos utilizando medios electrónicos, deberán (...) adoptar mecanismos de seguridad apropiados y confiables que garanticen

la protección de la información personal del consumidor y de la transacción misma. El proveedor será responsable por las fallas en la seguridad de las transacciones realizadas por los medios por él dispuestos, sean propios o ajenos.".

2.4. Herramientas de protección previstas para específicamente para la etapa poscontractual

Se tratan estos de derechos que sigue teniendo el consumidor cuando la relación contractual ya ha terminado. Trataremos en esta sección el derecho a que el consumidor desista de querer recibir información promocional o publicitaria del productor/proveedor/operador de plataforma electrónica, derecho a la protección de los datos personales y de la privacidad del consumidor.

2.4.1. Limitación de la información promocional o publicitaria

Los datos personales del consumidor deben ser usados para los fines indicados al momento de la contratación. En caso de que el consumidor haya consentido en que sus datos fueran utilizados con el fin de recibir información promocional o publicitaria del productor/proveedor/operador de plataforma electrónica, estos deben proporcionar e informar al consumidor sobre los mecanismos establecidos para suspender la recepción de dicha información. El consumidor tiene derecho a que se suspenda el envío de este tipo de información cuando él así lo solicite (art. 28B, Ley 19.496 y SERNAC, 2019, pág. 12).

2.4.2. Derecho a la protección de los datos personales y de la privacidad del consumidor

Este derecho comprende:

a. que el consumidor sea informado de las medidas tecnológicas aplicadas para el resguardo

y protección que se tendrán en relación con los datos personales otorgados con ocasión de la contratación o la relación de consumo;

b. la prohibición de que estos datos sean utilizados o recabados por terceros no autorizados expresamente por el consumidor; y,

c. la obligación del productor/proveedor/operador de plataforma electrónica de responder ante el consumidor frente a uno o los casos en que se vulneren los sistemas de protección de datos, así como en las hipótesis en que tales datos sean informados o transferidos a un tercero sin el consentimiento del consumidor.

2.5. ¿El consumidor que adquiere productos o servicios a través del uso de tecnologías emergentes también tiene obligaciones o deberes a su cargo?

Responderemos de manera afirmativa esta cuestión. En primer lugar, porque el consumidor debe actuar de buena fe. En segundo lugar, porque corresponde al consumidor el deber de informarse sobre las características del bien o del servicio que adquiere. Finalmente, porque la utilización de la tecnología puede, de un lado, contribuir a multiplicar los errores involuntarios en la oferta de bienes y servicios; y del otro poner en riesgo la propia privacidad del consumidor.

Sobre el primer punto, aunque la buena fe se presuma, nada obsta para que el consumidor se comporte de manera tal que pueda tener la "conciencia de haberse adquirido el dominio de la cosa por medios legítimos exentos de fraudes y de todo otro vicio" (artículos 706 del Código Civil chileno y 768 del Código Civil colombiano). En consecuencia, por ejemplo, frente a un precio ostensiblemente bajo o irrisorio, antes de proceder a comprar, nada obsta para que el consumidor se ponga en contacto con el productor/proveedor/

operador de la plataforma electrónica para verificar la veracidad de este precio.

En relación con el segundo, como lo recomienda la Superintendencia de Industria y Comercio de Colombia, el consumidor, en cumplimiento de su deber de actuar de buena fe exenta de culpa en la etapa precontractual, debe también informarse sobre "i) la calidad de los productos y el término de garantía otorgado; ii) las instrucciones que suministre el productor o proveedor en relación con el adecuado uso o consumo de los productos, así como de su conservación e Instalación; iii) los términos y condiciones suministrados en los contratos de consumo que celebran; iv) los derechos y deberes que ostentan en el marco de las relaciones de consumo; v) los mecanismos y herramientas disponibles para la protección de sus derechos; vi) las normas de reciclaje y disposición de desechos de bienes consumidos, para su debida observancia".

Finalmente, es un hecho que, pese a los esfuerzos de los gobiernos para limitar y encauzar el uso de la IA, este tipo de sistemas pueden recaudar datos sobre los usuarios en relación con sus hábitos personales, comportamientos o preferencias y, más tarde, utilizar estos datos para hacer inferencias sobre tendencias futuras de consumo. En consecuencia, cada vez que un consumidor acceda a una plataforma electrónica, debe asegurarse de que los datos personales que revele vayan a ser utilizados solo para los fines del contrato (artículo 16 letra g de la Ley 19.496 de Chile), y evitar dar datos excesivos.

3. ¿Cómo ejercer estos derechos en caso de conflicto con el productor/proveedor/operador de plataforma electrónica?

Con el fin de evitar que el consumidor deba acudir a un abogado, demandar en jurisdicciones extrañas a él e incurrir en importantes costos de un reclamo transnacional, con mayor frecuencia los productores/proveedores/operadores de pla-

taformas electrónicas ofrecen medios alternativos de solución de conflictos, algunas de ellas con apoyo sistemas de la inteligencia artificial. El más popular de ellos son los *Online Dispute Resoluiton* (ODR).

Así, los ODR han sido definidos como "procesos de resolución de controversias que se desarrollan en el ámbito extrajudicial y/o parajudicial y que incorporan el uso de internet o cualquier otro tipo de tecnología de la información y/o comunicación (TIC) similar, para la prevención o resolución de controversias, las cuales puede haberse generado *on-line* u *off-line*. La comunicación puede ser parcial o completamente en línea" (KATSH, 2016, pág. 329).

Hasta la fecha, "los ODR han resultado exitosos porque utilizan algoritmos que pueden darle a las partes las alternativas de valorar una determinada propuesta, según sus convicciones personales" (MARTÍNEZ-CÁRDENAS, 2022, pág. 1213).

De no prosperar esta instancia de mediación, algunas plataformas pueden remitir al Consumidor a otros métodos alternativos de solución de conflictos como el Arbitraje de Consumo, en el cual, ya no serán las partes, sino un tercero, quien solucione el conflicto.

4. Conclusiones

Colombia y Chile todavía están lejos de lograr una regulación uniforme en materia de comercio electrónico. Esto depende de comprender que cualquier regulación al respecto, debe asegurarnos que esta se convierta en un verdadero mecanismo que refuerce la sana competitividad de nuestras empresas y, por ende, la confianza de nuestros consumidores.

Sin embargo, y sin perjuicio de que en el futuro podamos emigrar hacia una regulación uniforme, el arribo de las tecnologías emergentes debe ser todo menos una justificación para desconocer lo que desde décadas sabemos que está prohibido hacer a través de los contratos, y mucho menos una licencia para desconocer los Estatutos de Protección al Consumidor.

De allí que se hace urgente para los productores/proveedores/operadores de plataformas electrónicas de nuestra región el comprender que ya cuentan con todos los medios necesarios para autorregularse, establecer mecanismos de prevención del daño y, de esta manera, mejorar su posicionamiento en los mercados y mantener la confianza en el *e-commerce*.

REFERENCIAS

REFERENCIAS SECCIÓN 1

Azuaje Pirela, M. & Finol González, D. (2017): Big Data, algoritmos y propiedad intelectual. Anuario de propiedad intelectual, Nº. 2016, 257-275.

Christensen, C. M., & Rosenbloom, R. S. (1995): Explaining the attacker's advantage: Technological paradigms, organizational dynamics and the value network. *Research Policy*, 24(2), 233-257. doi:10.1016/0048-7333(93)00764-k

Christensen, C. M. (1997): The innovator's dilemma: When new technologies cause great firms to fail. Boston: Harvard Business School.

Dosi, G. (1982): Technological paradigms and technological trajectories. *Research Policy* 11(3), 147-162. doi: 10.1016/0048-7333(82)90016-6

Fernández, E., & Valle, S. (2018): Tecnología disruptiva: la derrota de las empresas establecidas. Innovar, 28(70), 9-22. https://doi.org/10.15446/innovar.v28n70.74 404

Finck, M. & Moscon, V. (2019): "Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0. IIC - *International Review of Intellectual Property and Competition Law*, volume 50: pp. 77–108. https://doi.org/10.1007/s40319-018-00776-8

Granados, A. (2022): NFT: *¿Qué son, para qué sirven y cómo van a cambiarlo todo?* Madrid: La esfera de los libros.

McCarthy, J. (2007): "What is artificial intelligence?", [en línea] disponible en: http://www-formal.stanford.edu/jmc/whatisai/ [consultado el 19/02/2020].

Rotolo, D.; Hicks, D. & Martin, B. (2015): What is an emerging technology? *Research Policy*, Volume 44, Issue 10, pp. 1827-1843. https://doi.org/10.1016/j.respol.2015.06.006

Schwab, K. (2016): *La cuarta revolución industrial*. World Economic Forum.

REFERENCIAS SECCIÓN 2

1982, L. 2. (01 de 07 de 2022). *Gestor Normativo*. Obtenido de Función Pública de Colombia: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=3431#:~:text=Esta%20Ley%20protege%20exclusivamente%20la,obras%20literarias%2C%20cient%C3%ADficas%20y%20art%C3%ADsticas.

2018, L. 1. (01 de 07 de 2022). *Gestor Normativo*. Obtenido de Función Pública de Colombia: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=87419

Comisión Europea. (2018). *Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre Inteligencia Artificial para Europa*. Bruselas: Unión Europea.

Comité de Expertos IA Chile. (2021). *Documento Política Nacional de Inteligencia Artificial*. Santiago: Ministerio de Ciencia, Tecnología, Conocimiento e Innovación.

Departamento Nacional de Planeación . (2019). *POLÍTICA NACIONAL PARA LA TRANSFORMACIÓN DIGITAL E INTELIGENCIA ARTIFICIAL*. Bogotá: DNP - Colombia.

DW. (11 de 10 de 2021). *Científicos utilizan inteligencia artificial para completar la Décima Sinfonía de Beethoven*. Obtenido de DW Noticias: https://www.dw.com/es/cient%C3%ADficos-utilizan-inteligencia-artificial-para-completar-la-d%C3%A9cima-sinfon%C3%ADa-de-beethoven/a-59454097

Ministerio de Ciencia, Tecnología, Conocimiento e Innovación . (01 de 07 de 2022). *Chile presenta la primera Política Nacional de Inteligencia Artificial*. Obtenido de Ministerio de Ciencia, Tecnología, Conocimiento e Innovación : https://www.minciencia.gob.cl/noticias/chile-presenta-la-primera-politica-nacional-de-inteligencia-artificial/#:~:text=Chile%20presenta%20la%20primera%20Pol%C3%ADtica,aspectos%20de%20%C3%A9tica%20y%20seguridad

MINISTERIO DE CIENCIA, TECNOLOGÍA, CONOCIMIENTO E INNOVACIÓN. (01 de 07 de 2022). *Biblioteca del Congreso Nacional de Chile*. Obtenido de DECRETO 20 APRUEBA POLÍTICA NACIONAL DE INTELIGENCIA ARTIFICIAL: https://www.bcn.cl/leychile/navegar?idNorma=1169399

Pitol, S. (13 de 10 de 2017). *La Inteligencia Artificial que pintó el último retrato de Rembrandt*. Obtenido de VICE: https://www.vice.com/es/article/qvjyxq/creators-la-inteligencia-artificial-que-pinto-el-ultimo-retrato-de-rembrandt

RAE. (01 de 07 de 2022). *Real Academia de la Lengua Española*. Obtenido de Real Academia de la Lengua Española: https://dle.rae.es/artificial

RAE. (01 de 07 de 2022). *Real Academia de la Lengua Española*. Obtenido de Real Academia de la Lengua Española: https://dle.rae.es/inteligencia#LqtyoaQ

Vázquez, L. G. (30 de 01 de 2020). *China: Un tribunal reconoce derechos a un articulo escrito por un algoritmo de inteligencia artificial desarrollado por una empresa*. Obtenido de Instituto Autor: http://www.institutoautor.com/boletines/

REFERENCIAS SECCIÓN 3

BENTLY, Lionel; SHERMAN, Brad; GANGJEE, Dev y JOHNSON, Phillip (2018). *Intellectual Property Law* (5ª edición, Oxford University Press).

CALMA, Justine (2021). 'The climate controversy swirling arounf NFTs', *The Verge*. Disponible en línea: https://www.theverge.com/2021/3/15/22328203/nft-cryptoart-ethereum-blockchain-climate-change.

DUTFIELD, Graham y SUTHERSANEN, Uma (2020). *Global Intellectual Property Law* (2ª edición, Edward Elgar).

FERRARI, Valeria (2020). 'The regulation of crypto-assets in the EU – investment and payment tokens under the radar',

Maastricht Journal of European and Comparative Law, Vol. 27, Nº3, pp. 325 – 342.

GIANNOPOULOU, Alexandra; QUINTAIS, Joao Pedro; MEZEI, Peter y BODÓ, Balázs (2021). 'The rise of non-fungible tokens (NFTs) and the role of copyright law – Part I'. En *Kluwer Copyright Blog*. Disponible en línea: http://copyrightblog.kluweriplaw.com/2021/04/14/the-rise-of-non-fungible-tokens-nfts-and-the-role-of-copyright-law-part-i/.

GUADAMUZ, Andrés (2021a). 'Non-fungible tokens (NFTs) and copyright', *WIPO Magazine*, Nº4, pp. 32 – 37. Disponible en línea: https://www.wipo.int/export/sites/www/wipo_magazine/en/pdf/2021/wipo_pub_121_2021_04.pdf.

GUADAMUZ, Andrés (2021b). 'Can copyright teach us anything about NFTs'. En *TechnoLlama*. Disponible en línea: https://www.technollama.co.uk/can-copyright-teach-us-anything-about-nfts.

GUADAMUZ, Andrés (2021c). 'Copyfraud and copyright infringement in NFTs'. En *TechnoLlama*. Disponible en línea: https://www.technollama.co.uk/copyrfraud-and-copyright-infringement-in-nfts.

LAPATOURA, Ioanna (2021). 'Copyright and NFTs of Digital Artworks'. En *The IPKat*. Disponible en línea: https://ipkitten.blogspot.com/2021/03/guest-post-copyright-nfts-of-digital.html.

MEZEI, Peter; QUINTAIS, Joao Pedro; GIANNOPOULOU, Alexandra; BODÓ, Balázs (2021). 'The rise of non-fungible tokens (NFTs) and the role of copyright law – Part II'. En *Kluwer Copyright Blog*. Disponible en línea: http://copyrightblog.kluweriplaw.com/2021/04/22/the-rise-of-non-fungible-tokens-nfts-and-the-role-of-copyright-law-part-ii/.

MUNSTER, Ben (2021). 'NFT art bubble? 2017 crypto bust could spell out the future of current bloom", *The Art News-*

paper. Disponible en línea: https://www.theartnewspaper.com/2021/03/31/nft-art-bubble-2017-crypto-bust-could-spell-out-the-future-of-current-boom.

VALIENTE, María-Cruz y TSCHORSCH, Florian (2021). 'Blockchain-based technologies', *Internet Policy Review*, Vol. 10, Nº 2. Disponible en línea: https://policyreview.info/glossary/blockchain-based-technologies.

REFRENCIAS SECCIÓN 4

Argelich Comelles, C. (2020). Smart contracts o Code is Law: soluciones legales para la robotización contractual. *Dret Revista para el análisis del Derecho*(2), 1-41. Retrieved 08 08, 2022

Best, J., Sherwood D, N., & Jones, D. (n.d.). How Crowdfund Investing Helps Solve Three Pressing Socioeconomic Challenges,,. *Crowdfund Capital Advisors*, 3-5.

Bloomen. (2020). *Blockchain for Creative Content Management*. Retrieved 08 07, 2022, from Whitepaper: http://bloomen.io/wp-content/uploads/2020/08/Bloomen-White-Paper-August-2020.pdf

Blue Room Innovation. (n.d.). *Disruptive innovation for sustainability*. Retrieved from https://www.blueroominnovation.com/blockchain-para-el-sector-cultural-y-creativo/

Bourque, S. y. (2014). A lawyer's introduction to smart contract. *Scientia Nobilitat Reviewed Legal Studies*(201), 1-24. Retrieved from https://github.com/joequant/scms/blob/master/doc/pdfs/A%20Lawyer's%20Introducti on%20to%20Sm

Bozzo Hauri, S. (2021). Contratos inteligentes en torno a su desarrollo». In A. y. coordinadores, *Inteligencia artificial y derechos, desafíos y perspectivas*. Tirant lo Blanch.

Comisión para el Mercado Financiero, CMF. (2019, 02). *White Paper*. Retrieved 08 08, 2022, from Lineamientos Gene-

rales para la Regulación del Crowdfunding y Servicios Relacionados: https://www.cmfchile.cl/portal/principal/613/articles-25860_recurso_9.pdf

Consortium, B. (2020). D2.4 *Final Bloomen overall architecture*. Retrieved 08 07, 2022, from Bloomen: http://bloomen.io/wp-content/uploads/2020/08/Bloomen-White-Paper-August-2020.pdf

Creditonline. (2022). *Crowdfunding Software*. Retrieved from https://www.creditonline.eu/crowdfunding/?gclid=Cj0KCQjwxb2XBhDBARIsAOjDZ36KNA9_0ciZBdWJ4ydJbC33XfoPFW0THS1sYHL816MFfk1WZR8qsYwaAu1SEALw_wcB

Davara Fernández De Marcos, E. (2017, 07-08 01). "Los Smart contract". *Actualidad Administrativa*(7-8).

De las Heras Ballell, R. (2013). El crowdfunding: una forma de financiación colectiva, colaborativa y participativa de proyectos. *Revista Pensar en Derecho*, 2 (3), 101-123.

Durovic, M. (2018, 06 01). Law and Autonomous Systems Series: How to Resolve Smart Contract Disputes - Smart Arbitration as a Solution. *Oxford Business Law Blog*. Retrieved from https://www.law.ox.ac.uk/business-law-blog/blog/2018/06/law-and-autono

Fetsyak, I. (2020, 12). Contratos inteligentes: análisis jurídico desde el marco legal español". *Redur*(18), 197-236.

Herrera, M. (2018, febrero 27). Codeverde. Retrieved from Comisión Nacional de Energía será la primera entidad pública en utilizar Blockchain en Chile: https://codexverde.cl/comision-nacional-energia-sera-la-primera-entidad-publica-utilizar-blockchain-chile/

Idea.me. (2021). *Idea.me*. Retrieved 08 08, 2022, from Cómo funciona: https://www.idea.me/como-funciona

Pinochet Olave, R. (2006). Aspectos especiales en la formación del contrato electrónico. *Cuadernos de Análisis Jurídico*, *Colección de Derecho Privado*(3).

Superintendencia de Industria y Comercio y Centro de Información Tecnológica y Apoyo a la Gestión de la Propiedad Industrial- CIGEP. (2018, junio). *Boletín Tecnológico*. Retrieved from Blockchain, la revolución de la confianza digital: https://www.sic.gov.co/sites/default/files/files/Propiedad%20Industrial/Boletines_Tecnologicos/Boletin_Blockchain.pdf

Szabo, N. (1994). *Smart contracts*. Retrieved 08 06, 2022, from http://www.fon.hum.uva.nl/rob/Courses/ InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Vásquez Guzmán, J. (2020). *Estatus jurídico e implementación de los contratos inteligentes (Smart contracts) en Colombia*. Retrieved from Universidad de los Andes: https://repositorio.uniandes.edu.co/handle/1992/44918

REFERENCIAS SECCIÓN 5

ACHAP. (4 de Mayo de 2022). *ACHAP*. Obtenido de achap.cl: http://revista.achap.cl/marcas-que-lanzaron-productos-en-y-para-el-metaverso/

ALFAGEME, P. (19 de enero de 2022). *El Pais*. Obtenido de elpais.com: https://smoda.elpais.com/moda/actualidad/hermes-demanda-al-creador-de-los-metabirkins-los-nft-inspirados-en-los-famosos-bolsos-de-la-marca/

Delgado García - Pomadera, J. (2022). Los desafios de regular la creatividad en el metaverso. En J. F. Rodríguez Ayuso, A. Touriño Peña, A. Ramos Gil de la Haza, M. Estévez Sanz, A. Serrano Acitores, A. López Cazalilla, . . . E. Ortega, *Nuevas Tecnologías* (pág. 123). Madrid: Tirant lo Blanch.

Dolores Garayalde, M. D., & Cano, R. (2022). El metaverso y la protección de avatares mediante la propiedad industrial.

En J. F. Rodríguez Ayuso, A. Touriño Peña, A. Ramos Gil de la Haza, M. Estévez Sanz, A. Serrano Acitores, A. López Cazalilla, . . . E. Ortega, *Nuevas Tecnologías* (pág. 85). Madrid: Tirant Lo Blanch.

Infotextil. (27 de Marzo de 2022). *Info textil*. Obtenido de infotextil.com.ar: https://www.infotextil.com.ar/metaverse-fashion-week-todo-lo-que-tenes-que-saber-para-experimentar-esta-nueva-semana-de-la-moda/

Matinero Tor, J. (2022). NFT's (Non-fungible tokens) y el metaverso. En J. F. Rodríguez Ayuso, A. Touriño Peña, A. -E.-S. Ramos Gil de la Haza, A. López Cazalilla, J. Muñoz Rodríguez, M. R. Tapia Sánchez, . . . E. Ortega, *Nuevas Tecnologías* (pág. 335). Madrid: Tirant lo Blanch.

Santaella, L. (2021). *Foro cilac*. Obtenido de forocilac.org: http://forocilac.org/wp-content/uploads/2021/04/PolicyPapers-CILAC-InteligenciaArtificialCultura-ES.pdf

TFL. (8 de julio de 2022). *The fashion law*. Obtenido de https://www.thefashionlaw.com: https://www.thefashionlaw.com/the-euipo-has-provided-guidance-on-metaverse-nft-focused-trademarks/

REFERENCIAS SECCIÓN 6

Contreras, Pablo (2020): "El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena", en *Estudios Constitucionales* (Vol. 18, N°. 2), pp. 87-120.

Kaiser, Brittany (2018): "Facebook should pay its 2bn users for their personal data", Financial Times. Disponible en: https://www.ft.com/content/7a99cb46-3b0f-11e8-bcc8-cebcb81f1f90

Remolina Angarita, Nelson. Recolección Internacional de datos personales: un reto del mundo post-internet. Agencia Española de Protección de Datos. 2015.

REFERENCIAS SECCIÓN 7

Alexandrou, A. (2022). Cybercrime and Information technology. Theory and practice: The computer network infrastructure and computer security, cybersecurity laws, Internet of Things (IoT), and mobile devices. CRC Press.

Anchugam, C. V. (2021). Essential security elements and phases of hacking attacks. In N. Y. Conteh (Ed.), Ethical hacking techniques and countermeasures for cybercrime prevention (pp. 114–143). IGI Global.

Bambauer, D., y Day, O. (2011). The hacker's aegis. Emory Law Journal, 60(5), 1051–1108.

Bedecarratz, F. (2018). Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal, en: *Revista Chilena de Derecho y Tecnología*, 7(1), 79-105.

Benias, N., y Leventopoulos, S. A. (2019). Cyber warfare: A beyond the basic approach. In N. J. Daras (Ed.), Cyber-security and information warfare (pp. 57–82). Nova.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., *et a*l. (2018) "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation". https://bit.ly/2Vz1iX9.

Chawki, M., Darwish, A., Khan, M. A., y Tyagi, S. (2015). Cybercrime, Digital Forensics and Jurisdiction. Springer.

Denardis, L. (2020). The Internet in everything. Freedom and security in a world with no off switch. Yale University Press.

Donaldson, S. E., Siegel, S. G., Williams, C. K., y Aslam, A. (2015). Enterprise cybersecurity. How to build a successfull cyberdefense program against advanced threats. Apress.

Harper, A., Ragalado, D., Linn, R., Sims, S., Spasojevic, B., Martínez, L., Baucom, M., Eagle, C., y Harris, S. (2018). Gray hat

hacking. The ethical hacker's handbook (5th ed.). McGraw-Hill Education.

Miraz, M. H., Ali, M., Excell, P. S., y Picking, R. (2015). A review on Internet of Things (loT), Internet of Everything (IoE) and Internet ofNano Things (IoNT). 2015 Internet Technologies and Applications (ITA), 219–224.

Ngo, F. T., Agarwal, A., Govindu, R., y MacDonald, C. (2020). Malicious software threats. In T. Holt y A. M. Bossler (Eds.), The Palgrave handbook of international cybercrime and cyberdeviance (pp. 793–813). Palgrave Macmillan.

Ryan, M. (2021). Ransomware revolution: The rise of a prodigious cyber threat. Springer.

Seth, R., Sharaff, A., Chatterjee, J. M., y Jhanjhi, N. (2022). Ransomware attack: Threats y different detection technique. In N. Z. Jhanjhi, K. Hussain, A. Bin Abdullah, M. Humayun, y J. M. R. S. Tavares (Eds.), Information Security Handbook (pp. 157–176). CRC Press.

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., y Wu, C. (2009). AVOIDIT: A Cyber Attack Taxonomy. CTIT Technical Reports Series, n.pag. https://www.researchgate.net/publication/229020163_AVOIDIT_A_Cyber_Attack_Taxonomy

REFERENCIAS SECCIÓN 8

Barrientos Camus, F. (2015). *Lecciones de Derecho del Consumidor.* Santiago: Thomson Reuters.

Barrientos Zamorano, M. (2013). Artículo 3 B). En I. P. De la Maza Gazmuri, La protección de los derechos de los consumidores: comentarios a la Ley de Protección a los Derechos de los Consumidores. Santiago: LegalPublishing.

Isler Soto, E. (2013). Artículo 32. En I. d. Maza Gazmuri, *La protección de los derechos de los consumidores: comentarios a*

la Ley de Protección a los Derechos de los Consumidores (1a. ed. LegalPublishing.

Isler Soto, E. (2016). Aproximación al derecho a la no discriminación arbitraria en el régimen de la Ley 19.496. *Revista de Derecho Público*, 84, p. 104.

KATSH, E. &. (2016). What we know about Online Dispute Resolution. *South Carolina Law Review*, 67(2), 329.

MARTÍNEZ-CÁRDENAS, B. (2022). Online dispute resolution y la renovación del concepto del derecho de acceso a la justicia para los consumidores. En A. MADRID PARRA, & L. ALVARADO HERRERA, *Derecho Digital y Nuevas Tecnologías*. Thomson Reuters.

OCDE. (2001). *RECOMENDACIÓN DEL CONSEJO DE LA OCDE RELATIVA A LOS LINEAMIENTOS PARA LA PROTECCIÓN AL CONSUMIDOR EN EL CONTEXTO DEL COMERCIO ELECTRÓNICO*. Obtenido de https://doi.org/10.1787/9789264065680-es

Picod, Y., & Davo, H. (2010). *Droit de la Consommation*. Paris: Dalloz.

Quirós-García, E. (2021). La huella digital y la protección de datos: su impacto en las culturas de alto contexto y alto control de incertidumbre en Latinoamérica. *InterSedes, 22*(46), 169–187. doi: 10.15517/isucr.v22i46.46254

Rodríguez Grez, P. (2015). *Derecho del Consumidor, Estudio Crítico*. Santiago: Thomson Reuters.

Salgado, D. (2016). La huella digital. *revistaindice.com*, 14-17. Obtenido de http://www.revistaindice.com/numero68/p14.pdf

Schneble, C., Elger, B., & Shaw, D. (2018). The Cambridge Analytica Affair and Internet-Mediated Research. *EMBO REPORTS*, 19(8). doi:10.15252/embr.201846579.

SERNAC. (21 de 03 de 2019). *Resolución Exenta No. 0184*. Obtenido de Aprueba Circular Interpretativa sobre Buenas Prácticas en Comercio Electrónico: https://www.sernac.cl/portal/618/articles-9195_archivo_01.pdf

SERNAC. (2022). *Circular interpretativa sobre protección a consumidores frente al uso de sistemas de Inteligencia Artificial*. Obtenido de https://www.sernac.cl/portal/618/w3-article-64740.html

SIC. (2022). *Guía para la Protección del Consumidor en el Comercio Electrónico*. Obtenido de https://www.sic.gov.co/sites/default/files/files/2021/Gu%C3%ADa%20de%20comercio%20electr%C3%B3nico%2006-12-2021.pdf

SIC. (2022). *Guía de Buenas Practicas en la Publicidad a través de Influencers*. Obtenido de https://www.sic.gov.co/sites/default/files/files/2022/GUIA%20PRACTICAS%20PUBLICIDAD%20INFLUENCIADORES%20con%20firma%20-%202.pdf

SIC. (2022). *Guía de Buenas Prácticas en la Publicidad a través de Influenciadores*. Obtenido de https://www.sic.gov.co/sites/default/files/files/2022/GUIA%20PRACTICAS%20PUBLICIDAD%20INFLUENCIADORES%20con%20firma%20-%202.pdf

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

Organização das Nações Unidas para a Educação, a Ciência e a Cultura

CERLALC

Centro Regional para el Fomento del Libro en América Latina y el Caribe
Bajo los auspicios de la UNESCO

Centro Regional para o Fomento do Livro na América Latina e o Caribe
Sob os auspícios da UNESCO

DUC IN ALTUM

UNIVERSIDAD AUTONOMA DE CHILE

MÁS UNIVERSIDAD