



Los déjà vu de las regulaciones y de los desafíos legales

COLECCIÓN

GÉNESIS DE UN FUTURO DIGITAL



Marcos Pueyrredon



Los déjà vu de las regulaciones y de los desafíos legales

Marcos Pueyrredon

Nombre original: *Los déjà vu de las regulaciones y de los desafíos legales*

Número de edición: 1ª edición. Octubre, 2025

Textos: Marcos César Pueyrredon

Editora de textos: Roxana Tanita Miguel

Diseño gráfico y maquetación: eContent LAB – Estudio de diseño Mowbrand

Diseño de Tapa: Ángela Mayquez

© de las gráficas propias y adaptaciones:
eCommerce Institute

© de los textos: Los autores

© de las fotografías: Marcos César Pueyrredon (M.C.P)

Editorial eCommerce Institute

© de la presente edición digital y PDF interactivo

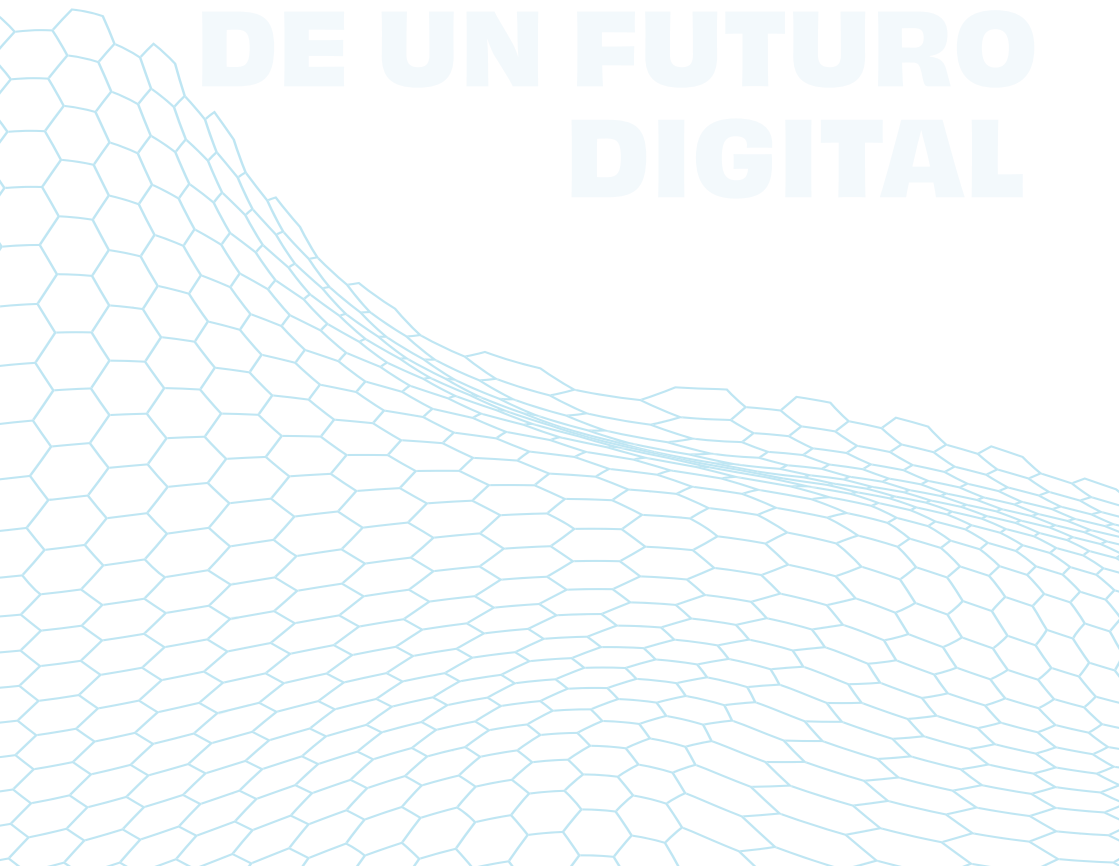
Año de publicación: 2025 ISBN: 978-631-01-2403-2

Queda hecho el depósito que previene la ley 11.723

No está permitida la reproducción total o parcial de este libro, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro u otros medios, sin el permiso previo y por escrito de los titulares del Copyright.



**Navegando por el caótico panorama normativo
que rodea al ecosistema digital.**



A mi querida esposa Teresa, mi adorada hija Carolina y a nuestro angelito Ignacio, quienes, junto con toda mi amada familia, son mi fuente inagotable de inspiración y fuerza. Han caminado a mi lado en cada paso de este fascinante viaje hacia el futuro digital. Sin su amor, paciencia y apoyo incondicional, esta obra no habría sido posible.

A mi dre@m te@m, que ha compartido conmigo la pasión por lo que hacemos, enfrentando cada desafío con determinación y creatividad.

Este libro vivo es un testimonio de nuestro esfuerzo conjunto y del impacto que hemos logrado al unir nuestras visiones para construir un ecosistema digital más robusto y dinámico.

A todos los pioneros, referentes, jedi y master jedi del ecosistema digital iberoamericano que, con su “fuerza”, aportes y testimonios, han sido fundamentales para que nuestra colección se convierta en una fascinante cadena de dominós que permite armar miles de caminos hacia el mismo objetivo. Ustedes, que se atrevieron a soñar con un futuro digital cuando aún era sólo una idea incipiente, han dejado una huella imborrable en la historia del ecosistema digital en nuestra región. Este libro es un homenaje a su valentía, innovación y compromiso inquebrantable.

Que esta obra sea un faro para las futuras generaciones, un recordatorio de que el futuro se construye con la suma de nuestras experiencias, aprendizajes y, sobre todo, con la convicción de que lo imposible sólo tarda un poco más en alcanzarse.

Con gratitud y admiración: **Obrigadíssimo!**



Índice

Prólogo	11
□ Acerca de cómo navegar esta colección de libros vivos	15
□ Características destacadas de la colección de libros vivos Génesis de un futuro digital	20
La paradoja digital: Innovar sin marco legal	25
□ El desfase entre la innovación y la regulación	28
□ Mitos regulatorios frecuentes en el ecosistema digital	29
□ Primera década del ecommerce: Crecimiento sin normas claras	37
□ El rol pasivo (y luego punitivo) del Estado	39
□ Brecha regional en materia legal digital	43
□ Lecciones aprendidas	48
Déjà vos regulatorios: Viejos problemas, nuevas caras	53
□ Del catálogo digital al marketplace: Las reglas llegan tarde	53
□ Matriz de responsabilidades en el comercio colaborativo	58
□ Publicidad digital y protección al consumidor: Una deuda sin saldar	65
□ Medios de pago y su eterna persecución legal	71
□ Desafíos locales vs. regulación global	81
□ Desafíos constantes: Opacidad, burocracia e inseguridad jurídica	90
Focos de tensión legal transversales al ecosistema digital	99
□ Protección de datos personales y privacidad	100
□ Propiedad intelectual en el entorno digital	107
□ Fiscalidad digital: ¿Dónde se genera el valor?	115

□ Derechos del consumidor digital	126
□ Publicidad y responsabilidad en redes sociales	134
□ Radar de riesgos regulatorios 0–5	143

Jurisprudencia clave y casos que sentaron precedentes 153

□ La función de la jurisprudencia en un ecosistema en mutación	154
□ Casos emblemáticos en Iberoamérica	156
■ Serie “Caso corto regulatorio”: Radiografías rápidas para aprender	157
■ Brasil: Responsabilidad de marketplaces y lucha contra la falsificación	164
■ México: Protección al consumidor digital – Profeco vs. Amazon y Mercado Libre	168
■ Colombia: Datos personales y responsabilidad de las plataformas (Linio, Rappi, Mercado Libre)	172
■ Chile: El derecho a retracto en lo digital – nuevos criterios de protección al consumidor	177
■ Argentina: Tributación digital – Mercado Libre, Netflix y el largo brazo fiscal de la AFIP	180
□ Casos transversales: La influencia del derecho comparado	184
□ Efecto cascada: Cómo impactan estos fallos en el ecosistema	190

Los desafíos del marco normativo en la era digital:

Diseñando regulaciones adaptativas y colaborativas 197

□ Del riesgo regulatorio al P&L: Risk–impact canvas regulatorio	210
■ IA-Unificada como radar regulatorio y traductor del caos normativo	218
■ Equipos legales en modo human augmented AI	228

Conclusión 255

Apéndice práctico: Operar en modo regulatory-ready 263

□ Matriz 2x2 de riesgo regulatorio (impacto vs probabilidad)	264
□ Árbol de decisión	268
□ Mapa de stakeholders regulatorios	271
□ Checklist de regulatory readiness para proyectos digitales	275
□ Preguntas que debería hacerle a tu abogada o abogado antes de lanzar	286

Agradecimientos 295

Referencias 299

Podcast y entrevistas 317

Sobre las dimensiones del libro vivo 321

Próximos Momentums 327

GÉNESIS
**DE UN FUTURO
DIGITAL**

Prólogo

GÉNESIS



Cada vez que el ecosistema digital da un paso adelante, la regulación se queda mirando desde atrás. Es una escena que se repite una y otra vez —un verdadero déjà vu— en la historia del comercio electrónico y la economía digital iberoamericana. Este libro nace precisamente de esa constatación: la brecha entre la innovación y la ley no sólo persiste sino que se reinventa con cada avance tecnológico.

Durante los últimos 25 años fuimos testigos de una transformación sin precedentes. El comercio electrónico pasó de ser una curiosidad de emprendedores visionarios a representar más del 20% de las ventas minoristas globales en 2025, con proyecciones que superan los 8 billones de dólares en volumen transaccionado para 2028.¹ Pero mientras los consumidores adoptaban nuevas plataformas, los Estados debatían cómo regularlas.

Iberoamérica no fue la excepción. La región creció a un ritmo vertiginoso —con picos del 63 % de expansión en 2020, según eMarketer—, pese a carecer de marcos legales modernos para las transacciones digitales. Esa tensión entre crecimiento e indefinición regulatoria se convirtió en uno de los grandes ejes de este volumen.

En estas páginas revisamos las lagunas normativas, los conflictos legales y las soluciones emergentes que moldearon la evolución del ecosistema digital. Analizamos desde los casos emblemáticos —como los enfrentamientos entre Uber y los reguladores municipales, o las sanciones a marketplaces por publicaciones de terceros— hasta los nuevos dilemas que plantean la IA generativa, la protección de datos y la competencia en entornos digitales.

Este libro no busca ofrecer respuestas definitivas, porque no las hay. Lo digital es, por naturaleza, un terreno en constante movimiento. Cada innovación genera nuevos desafíos éticos, legales y económicos. Lo que hoy parece una solución mañana se convierte en un nuevo problema.

Por eso, más que un compendio jurídico, este volumen pretende ser un mapa de aprendizaje colectivo: una radiografía de los errores y aciertos de una región que, con creatividad y resiliencia, ha sabido avanzar incluso cuando las reglas del juego aún no estaban escritas.

Si algo aprendimos a lo largo de la colección ***Génesis de un Futuro Digital*** es que la verdadera madurez del ecosistema no depende sólo de la tecnología

o de la ley, sino de la capacidad de diálogo entre quienes las hacen posibles: innovadores, reguladores, emprendedores y ciudadanos.

Los déjà vu regulatorios seguirán apareciendo, porque la innovación no espera. Pero cada repetición deja una lección más clara: no hay desarrollo digital sin confianza, y no hay confianza sin reglas claras, éticas y compartidas.

Este libro es un homenaje a esa búsqueda.

GÉNESIS

DE UN FUTURO DIGITAL

GÉNESIS

DE UN FUTURO DIGITAL



Acerca de cómo **navegar** esta colección de **libros vivos**

Génesis de un futuro digital es un libro vivo; es una colección de diferentes *momentums* que se presentarán en formato de libro vivo. Es la primera publicación de este tipo en la historia editorial que utiliza todos los recursos tecnológicos de los que actualmente disponemos en un solo lugar, para que no sólo puedas leerlo en formato digital **ingresando a la web oficial**, sino que también puedas interactuar con su contenido y participar con tu propio relato.

Conscientes de que estamos compartiendo mucho más que palabras y mucho más que un registro histórico, he reunido a un equipo multidisciplinario para diseñar el formato vivo, que te permite navegar el pasado, presente y futuro del ecosistema digital en Iberoamérica, pudiendo descubrir, aprender y contribuir con el reconocimiento del mismo mediante los siguientes recursos:

1. **Lectura enriquecida:** gracias a la colaboración de más de 200 expertos que fueron entrevistados y que tan gentilmente han compartido sus experiencias y conocimientos, más un detallado trabajo documental, cada uno de los libros vivos que forman parte de la colección *Génesis de un futuro digital* es una ventana que te permite explorar los hitos, testimonios

y tendencias que han moldeado al comercio digital. Puedes empezar tu recorrido por medio del libro vivo que quieras y sin la obligación de seguir una correlación. Por ser un formato vivo, algunos *momentums* pueden estar en desarrollo, en cuyo caso te invito a suscribirte para recibir una notificación o aportar contenido al mismo.

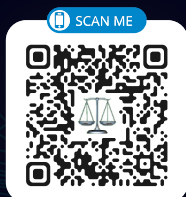
Al acceder a los libros de esta colección obtienes:

a. Contenido completo en múltiples formatos: texto, video, audio, fichas de perfil y glosario.

b. Acceso a más de 200 entrevistas a pioneros y referentes del *digital commerce* en Iberoamérica, disponibles en la playlist [eLíderes x25](#), del canal oficial del eCommerce Institute en YouTube o en [Spotify](#).

2. Escucha donde quieras: cada libro cuenta con una versión audiolibro con relatos únicos sobre el origen del ecosistema digital en Iberoamérica.

**¡Escucha ahora
el audio libro!**



ACCEDE A
eLíderesx25
PODCAST



a. Los primeros audiolibros ya están disponibles para que los escuches donde quieras y te sumerjas en el origen del ecosistema digital en Iberoamérica, contado por algunos de los protagonistas en primera persona.

3. Interactividad y actualización constante: no te limites a leer; explora un mundo de contenido multimedia que incluye videos, fichas de perfil, glosario y mucho más. Esta experiencia multimedial y multidimensional te ofrece una perspectiva completa y enriquecida.

a. Experimenta una lectura dinámica gracias al soporte de inteligencia artificial aumentada, que adapta la experiencia a tus preferencias y necesidades.

b. Por su formato de libro vivo, los contenidos se actualizan continuamente para reflejar los cambios y avances en el ecosistema digital, manteniéndote siempre informado.

4. Participación activa: tú también puedes formar parte de esta narrativa.

a. Contribuye con tu testimonio, casos, anécdotas, estudios o investigaciones, enriqueciendo así el conocimiento compartido sobre la génesis del ecosistema digital. Para hacerlo, completa el formulario que encontrarás en genesisfuturo.digital.

Hola, soy *Delphy*

Tu agente de AI en
Génesis de un futuro
digital



5. Potencia la experiencia con inteligencia artificial aumentada y generativa: ¿tienes preguntas o quieres profundizar en algún tema específico?

Interactúa con Delphy, nuestra agente de inteligencia artificial disponible para acompañarte a explorar los contenidos de esta colección de libros vivos, por medio de una experiencia de lectura generativa y aumentada. Dialoga con ella desde nuestra web <https://genesisfuturo.digital/> para acceder a la información más detallada de cada libro, pionero, temas, definiciones, empresas y acontecimientos relevantes sobre los que quieras profundizar.



Características destacadas de la colección de *libros vivos* *Génesis de un futuro digital*



Colaborativo y documentado: más de 200 expertos colaboraron para proporcionar una visión completa del ecosistema digital en Iberoamérica.



Innovador y tecnológico: utiliza inteligencia artificial generativa y aumentada para ofrecer una experiencia de lectura avanzada y dinámica, adaptada a las necesidades del lector moderno.



Multimedia y multidimensional: integra diferentes formatos de contenido como texto, video, audio, fichas de perfil y glosario, proporcionando una experiencia de lectura enriquecida.



Actualizable y dinámico: por ser un libro vivo, los contenidos se actualizan constantemente para reflejar los cambios y avances en el ecosistema digital.

Escanea el **código QR** y elige por dónde empezar a navegar esta historia que contará con **25 momentums** del ecosistema digital de Iberoamérica.

Suscríbete para enterarte antes que nadie cada vez que se publique o actualice algunos de los momentums.

Lee, escucha, participa e interactúa. Esta historia está en construcción y todos, de alguna manera, ya somos parte.



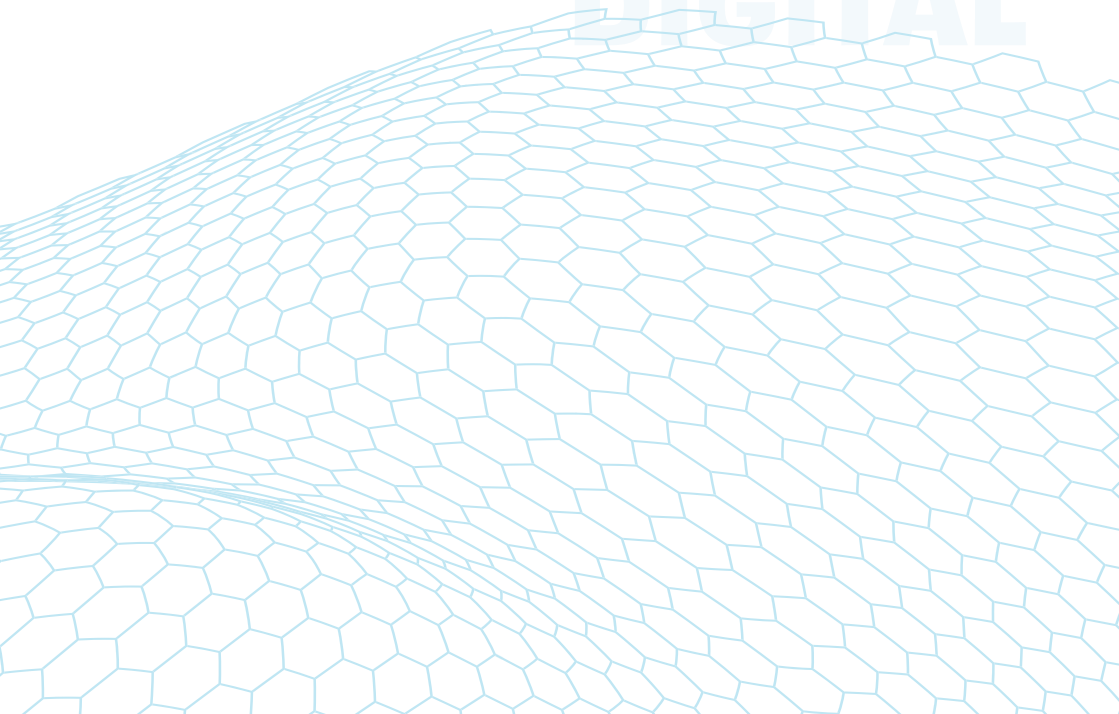
GÉNESIS

DE UN FUTURO DIGITAL



MOMENTUM

GÉNESIS 
DE UN FUTURO
DIGITAL



GÉNESIS

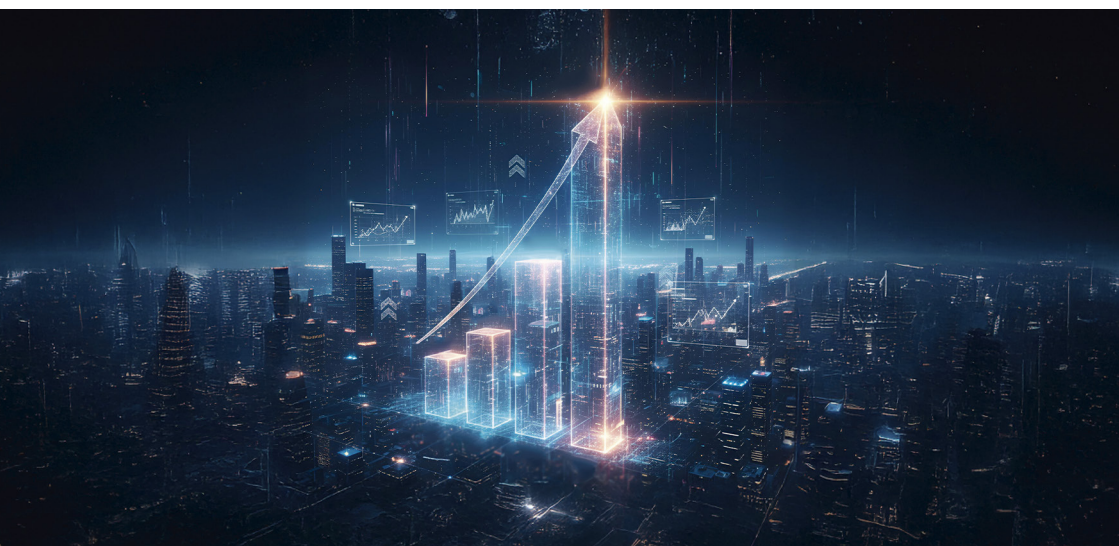
DE UN FUTURO DIGITAL





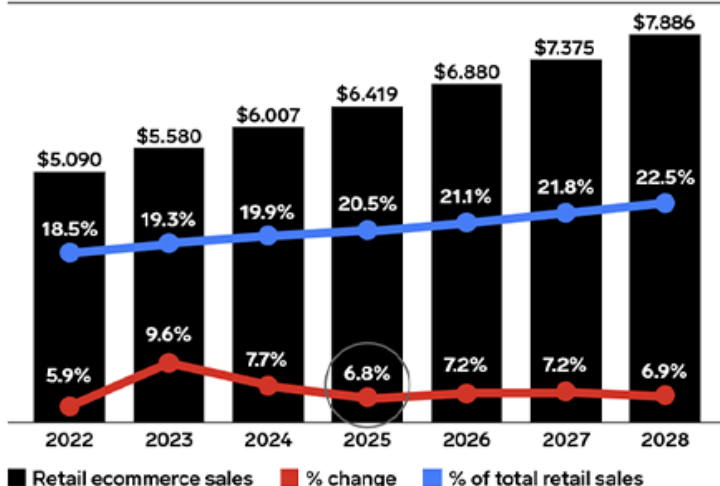
La paradoja digital: Innovar sin marco legal

La economía digital global ha experimentado un crecimiento sostenido en ventas de comercio electrónico, pasando de 5,08 billones de dólares en 2022 a 6,42 billones en 2025, y se proyecta que alcanzará 8,09 billones para 2028, según datos de eMarketer (Cramer-Flood, 2024). Este crecimiento representa un incremento promedio anual del 9,4 %, impulsado por la expansión del consumo digital en mercados emergentes y la consolidación de ecosistemas omnicanal en los países desarrollados.



Worldwide Ecommerce Sales Growth Will Dip Slightly in 2025, Mostly Due to Softness in China

trillions in retail ecommerce sales worldwide, % change, and % of total retail sales, 2022-2028



Note: Includes products or services ordered using the internet, regardless of the method of payment or fulfillment; excludes travel and event tickets, payments such as bill pay, taxes, or money transfers, restaurant sales, food services and drinking place sales, gambling and other vice goods sales

Source: EMARKETER Forecast, Feb 2025

289739

EMARKETER

Gráfico. Evolución del comercio electrónico mundial: las ventas minoristas online alcanzarán USD 7,88 billones en 2028, pese a una leve desaceleración en 2025. Fuente: eMarketer, *Worldwide Ecommerce Forecast*, febrero de 2025.

Pese a este auge, el comercio digital global convive con una paradoja estructural: la innovación tecnológica avanza más rápido que la capacidad de los marcos regulatorios para acompañarla. En Iberoamérica, esa tensión se transparentó en 2020, cuando el comercio electrónico en Latinoamérica creció un **63,3 %** para alcanzar ventas por más de 104 mil millones de dólares,

justamente en un momento en que pocas jurisdicciones contaban con leyes digitales maduras o específicas para ese escenario emergente.²

Siempre me impresionó cómo la innovación suele correr más rápido que el derecho. Lo viví desde los primeros años del ecommerce y lo sigo viendo hoy con cada nueva ola tecnológica. Uber, por ejemplo, no fue el primero ni será el último caso en demostrarlo: llegó a nuestras ciudades antes de que existieran normas que lo reconocieran o regularan. En ese vacío legal convivieron la disrupción y la incertidumbre, los usuarios fascinados por la novedad y los reguladores tratando de entender qué estaba ocurriendo. Esa tensión —entre lo posible y lo permitido— ha acompañado a todo el ecosistema digital iberoamericano desde su génesis. Éste ha sido testigo de innovaciones que florecieron en un “lejano oeste regulatorio”, seguidas por oleadas de respuestas legales tardías: un ciclo de *déjà vu* que aún hoy condiciona la madurez institucional de la economía digital.

¿Siempre ha sido así? A finales de los noventa, emprender online era navegar sin mapa legal: contratos digitales sin reconocimiento normativo, transacciones transfronterizas sin claridad impositiva y consumidores desprotegidos ante fraudes en línea. Aquella primera generación de empresas digitales innovó a ciegas, guiada más por la confianza que por las normas. Esa dinámica —innovar sin marco legal— es el punto de partida de todas las lecciones que siguen.

El desfase entre la innovación y la regulación

La brecha temporal entre el avance tecnológico y la respuesta legal ha sido una constante en la historia del comercio digital. Por un lado, la innovación opera bajo la lógica de la rapidez y la disrupción; por otro, la regulación avanza con la prudencia y lentitud propias del consenso legislativo. Este desfase se refleja en cifras elocuentes: a nivel global, más del 75% de los usuarios de Internet ya realizaba compras en línea en 2024, y se proyecta que la mitad de la población mundial mayor de 14 años será compradora digital para 2028.

Sin embargo, las políticas públicas no han logrado un acompañamiento homogéneo. Según un informe del Banco Mundial, incluso dos décadas después del auge del comercio electrónico, **sólo el 79 % de los países ha adoptado leyes sobre transacciones electrónicas, y apenas el 52 % cuenta con normativas específicas de protección al consumidor en línea**, lo que refleja los amplios vacíos que aún persisten en la tutela de los usuarios digitales a nivel global.³

Este rezago legal es más acentuado en regiones emergentes: junto a África, Latinoamérica ostenta el promedio más bajo en el índice global de preparación para el comercio electrónico B2C, reflejo tanto de desafíos infraestructurales como regulatorios. En síntesis, **mientras la economía digital escala a un ritmo de doble dígito anual en ventas y usuarios, los marcos legales luchan por salir de la etapa analógica.**

Este descompás histórico ha generado escenarios de incertidumbre jurídica. Innovaciones como las criptomonedas, la inteligencia artificial o las plataformas de economía colaborativa suelen nacer en terrenos grises, no cubiertos por la ley vigente. En Iberoamérica, los primeros años evidenciaron este patrón: las startups de finales de los 90 y principios de los 2000 operaban sin un paraguas normativo específico, por lo que creaban sus propias reglas de juego. Los emprendedores forjaron códigos de conducta voluntarios y modelos de autorregulación para suplir la ausencia de legislación, prácticas que, si bien ayudaron a construir confianza, también demostraron ser frágiles ante abusos.

La consecuencia fue una sensación de “tierra de nadie” legal, donde los derechos y obligaciones no estaban claramente delimitados. Voces expertas, como la del analista Alejandro Prince, han subrayado la necesidad de marcos jurídicos adaptativos que evolucionen al compás de la tecnología y eviten que las sociedades queden rezagadas. La alternativa es repetir el ciclo de improvisación y corrección a posteriori: *una secuencia de déjà vu que el ecosistema ya no puede permitirse.*

Mitos regulatorios frecuentes en el ecosistema digital

Cuando uno mira en retrospectiva las últimas dos décadas del ecosistema digital iberoamericano, llama la atención la cantidad de decisiones que se tomaron no sólo con poca información, sino apoyadas en **ideas equivocadas**

sobre la regulación. Más que un vacío normativo absoluto, lo que había —y muchas veces sigue habiendo— es un vacío de comprensión: mitos que se repiten en pasillos, pitches e incluso en ruedas de políticas públicas, y que terminan justificando la inacción o el atajo.

Al igual que en otros libros de la colección ["Génesis de un Futuro Digital"](#) —desde ["El boom del comercio electrónico"](#) hasta ["El ecosistema emprendedor y el impulso de las nuevas iniciativas"](#)— vale la pena detenernos a desarmar algunos de estos mitos. No para hacer teoría jurídica, sino para que quien emprende, dirige una empresa o diseña políticas públicas pueda **reconocer cuándo está decidiendo en base a relatos falsos.**

A continuación, cuatro mitos regulatorio-digitales que se repiten una y otra vez en nuestra región.

Mito 1: "Internet está fuera de la ley"

Durante años se instaló la idea de que "internet era tierra de nadie". Lo escuché en reuniones con empresarios, funcionarios y emprendedores: como no había una "Ley de Internet" o una "Ley de Ecommerce" específica, entonces el espacio digital era una especie de Far West donde casi todo estaba permitido mientras no hubiera escándalo. Este mito explica parte de la sensación de "tierra de nadie legal" que describimos en este capítulo y que reconstruimos en detalle en *El boom del comercio electrónico* con testimonios de pioneros que vendían online sin saber qué contrato estaban celebrando realmente.

En la práctica, nunca fue cierto que internet estuviera fuera de la ley. Aunque los códigos civiles, comerciales y de consumo no hubieran sido escritos pensando en plataformas, criptomonedas o IA generativa, **según vigentes**: habían normas sobre responsabilidad contractual y extracontractual, deber de información, vicios de la cosa, prácticas abusivas, publicidad engañosa, protección de la persona, e incluso principios constitucionales. Lo que sí faltaba era **claridad y adaptación**: jueces y reguladores tuvieron que reinterpretar normas viejas en contextos nuevos, con toda la inseguridad jurídica que ello implicó.

La consecuencia práctica de creer este mito fue doble. Para muchas empresas, sirvió de excusa para “hacer primero y preguntar después”; para muchos reguladores, justificó una pasividad cómoda (“total, esto es otro mundo”). El resultado lo conocemos: conflictos que podrían haberse evitado con lecturas mínimas de normas ya existentes, consumidores desprotegidos y un retraso innecesario en la creación de marcos específicos. El mensaje para la próxima ola —IA, identidad digital, tokenización— es claro: aunque todavía no haya una “Ley de IA” con nombre y apellido, **los principios jurídicos básicos ya existen y se aplican**.

Mito 2: “Si mi startup es chica, nadie me va a mirar”

Otro relato recurrente en el ecosistema emprendedor es que los reguladores sólo persiguen a los gigantes. Bajo esta premisa, startups y scale-ups se sienten autorizadas a postergar indefinidamente cualquier conversación seria sobre regulación, datos o cumplimiento: “cuando seamos grandes vemos”, “primero crezcamos, después nos ordenamos”, “la autoridad ni sabe que existimos”.

Como mostramos en *El ecosistema emprendedor y el impulso de las nuevas iniciativas*, esta lógica suele funcionar hasta cierto punto... hasta que deja de funcionar. En el momento en que una startup entra en un mercado sensible (fintech, salud, educación, logística, transporte, medios de pago, datos personales) o se vuelve visible por el tipo de servicio que presta, **deja de ser invisible**. A veces la primera llamada no viene del regulador, sino de un banco que no quiere trabajar con un actor informal, de un corporativo que exige ciertos estándares para firmar un acuerdo, o de un fondo que pide claridad regulatoria antes de invertir.

Además, hay un aspecto político: muchos organismos de control **eligen casos ejemplificadores**. Una empresa relativamente pequeña pero simbólica puede convertirse en “caso testigo” para marcar un criterio, mostrar autoridad o enviar un mensaje a todo el sector. El tamaño no es un salvavidas absoluto; de hecho, a veces es lo contrario: el regulador sabe que un actor todavía no sistémico es más fácil de sancionar sin generar efecto dominó.

La enseñanza que se desprende de este libro y de la colección es simple: **no existe etapa de la vida de un emprendimiento en la que pensar el marco regulatorio esté de más**. Lo que cambia es el nivel de profundidad. En la fase inicial, bastan buenas prácticas mínimas y entender los grandes riesgos. A medida que se escala —especialmente cuando se entra en modelos de unified & collaborative commerce o de retail media que describimos en otros momentums—, la sofisticación regulatoria deja de ser opcional.

Mito 3: “Cumplir algo parecido al GDPR en Latam es overkill”

Con la entrada en vigor del GDPR en Europa y, más tarde, de la LGPD en Brasil y de reformas profundas en otros países, empezó a escucharse otro mantra: “eso allá, acá es imposible”, “adaptarnos a estándares europeos nos va a matar la innovación”, “en Latinoamérica la gente no se preocupa tanto por la privacidad, lo que quiere es precio y entrega”.

En [“La revolución de los datos en la era del big data”](#), mostramos cómo esta mirada subestima tres cosas:

1. La velocidad con la que la conciencia sobre datos se globalizó.
2. El peso que tienen los marcos extraterritoriales (como el propio GDPR) sobre empresas que operan cross-border.
3. El rol de la confianza en los modelos de datos que sostienen el Data Trust Flywheel.

Cumplir con estándares altos de privacidad y protección de datos no es sólo una carga; es **una condición para poder jugar ciertos juegos**. Una fintech latinoamericana que quiera operar con correspondientes europeos, una plataforma que procese pagos internacionales, un retailer que use servicios de nube globales, terminan expuestos —de manera directa o indirecta— a esos marcos. Aun cuando el propio país no tenga una ley tan avanzada,

los socios, proveedores o inversores pueden exigir ese estándar como precondition.

Además, la idea de que la gente “no se preocupa por sus datos” es cada vez menos cierta. Los escándalos de filtraciones masivas, doxing, estafas y usos indebidos han instalado la sensación de vulnerabilidad digital. El ciudadano que en [“El boom del comercio electrónico”](#) estaba preocupado sobre todo por si el producto llegaba o no, hoy también pregunta qué pasa con la información que deja en cada click.

El punto no es “copiar el GDPR” acríticamente, sino **entender que la vara global se movió**. Para muchos proyectos, diseñar desde el inicio con un estándar alto de privacidad —incluso si la ley local todavía no lo exige— es, paradójicamente, una manera de competir mejor y de evitar dolores de cabeza futuros cuando el país inevitablemente actualice su marco.

Mito 4: “Si soy plataforma, no tengo ninguna responsabilidad”

Este ha sido uno de los mitos más costosos para el ecosistema. La idea de que la plataforma es “mera intermediaria tecnológica” y que, por tanto, sólo facilita el encuentro entre terceros sin asumir responsabilidades, se sostuvo durante años y ayudó a escalar modelos muy potentes... pero también generó tensiones crecientes con reguladores, consumidores y otros actores. En [“La implementación de los modelos unified & collaborative commerce”](#) analizamos cómo esa visión choca con

la realidad de plataformas que fijan reglas, ordenan la oferta, procesan pagos, gestionan reputación y muchas veces controlan logística.

Lo que muestra la jurisprudencia y los casos que recorreremos en este libro es que **la responsabilidad de las plataformas es graduada, pero real**. No es lo mismo ser un tablón de anuncios totalmente pasivo que una superapp que controla cada paso de la experiencia. Aun en los modelos más abiertos, los tribunales y autoridades han ido marcando ciertos mínimos: deber de colaboración, de información, de implementar mecanismos razonables para prevenir fraudes, falsificaciones o contenidos ilícitos, de responder cuando se notifica un incumplimiento evidente.

Crear en el mito de la “no responsabilidad” llevó a algunas plataformas a desentenderse de problemas que, con el tiempo, terminaron dañando su propia licencia social para operar: productos falsos, estafas recurrentes, contenidos violentos o discriminatorios que se mantenían en línea sin reacción. En contraste, en [“El boom del comercio electrónico”](#) y en [“El desarrollo del Retail Media Network”](#) vemos casos donde las compañías entendieron temprano que, aun sin obligación legal explícita, **valía la pena asumir un rol más activo**: códigos de conducta, acuerdos con cámaras, sistemas de detección de abuso, programas de protección de marcas y consumidores.

La pregunta ya no es si la plataforma tiene responsabilidad, sino **cómo la asume inteligentemente**, sin matar la innovación ni asfixiar a los sellers, pero

tampoco escondiéndose detrás de un discurso de neutralidad que nadie cree. La matriz de responsabilidades que planteamos en este libro —plataforma, merchant, usuario, Estado— es una herramienta concreta para salir de este mito y diseñar acuerdos más claros y sostenibles.

Al desmontar estos mitos, este libro busca algo más que precisión conceptual: pretende que **las próximas decisiones** —sobre IA, identidad digital, tokenización, comercio colaborativo, retail media— no se construyan sobre creencias heredadas de la primera ola del ecommerce, sino sobre **aprendizajes conscientes**. El resto de la colección ["Génesis de un Futuro Digital"](#) puede leerse como un diálogo continuo con estos mitos: cómo se generaron, cómo nos condicionaron y cómo podemos superarlos para que regulación e innovación se dejen de ver como enemigos y pasen a ser socios en el diseño de un futuro digital más justo y sostenible.



Primera década del ecommerce:

Crecimiento sin normas claras

La primera década del comercio electrónico en Iberoamérica (aprox. 1995–2005) fue un período de crecimiento silvestre, donde el entusiasmo empresarial y la adopción tecnológica superaron con creces la capacidad regulatoria de los Estados.

En esos años iniciales, la penetración de internet en la región aún era baja – un 70% de conectividad recién para 2020 en América Latina,⁴ muy por debajo de los países desarrollados en los 2000 –, pero el comercio electrónico despegaba de manera constante. Plataformas pioneras como Mercado Libre, que nació en 1999, o Submarino en Brasil aprovecharon la ausencia de barreras legales específicas para escalar rápidamente sus modelos de negocio.

Esta libertad, si bien permitió la proliferación de innovaciones, significó que no existían reglas claras sobre aspectos críticos: contratación por medios electrónicos, validez de firmas digitales, privacidad de datos de usuarios o responsabilidades de las plataformas ante fraudes. Las empresas operaban con la única guía de códigos civiles/comerciales pensados para el mundo offline, lo que obligaba a una interpretación creativa de normas generales para aplicarlas a situaciones inéditas.

En esta etapa, el papel del Estado fue mayormente observador. Pocas iniciativas legislativas vieron la luz en

los primeros años. Una excepción notable fue la temprana aprobación de leyes de firma digital y mensajes de datos en algunos países influenciados por la ley modelo de UNCITRAL.⁵ Por ejemplo, Colombia adoptó la Ley 527 de 1999, que reconoce la equivalencia jurídica de los documentos electrónicos y habilita la infraestructura de certificación digital. Para [Eugenio Sánchez, Jefe de Oficina en Positiva Compañía de Seguros](#).⁶



“Con este paso (impulsado por la aparición de una ley modelo), se logró la democratización de Internet en el país”.



Eugenio
Sánchez

Hay que decir que, además, sentó las bases para la masificación del comercio electrónico. Colombia entendió que primero debía cerrar la brecha de conectividad para luego pensar en comercio electrónico; así, al inicio de los 2000, promulgó marcos para ampliar el acceso a las TIC y abrió camino a la inclusión digital. No obstante, tales ejemplos fueron la minoría. En la mayoría de los países latinoamericanos, la década del 2000 transcurrió con un ecommerce en crecimiento exponencial pero sin una legislación dedicada que le diera soporte o certezas.

Paradójicamente, esta “edad dorada” desregulada del ecommerce trajo consigo tanto éxitos sorprendentes como problemas latentes. Por un lado, emprendimientos digitales pudieron florecer sin las cargas burocráticas

habituales, y la innovación de modelos de negocio –tiendas en línea, subastas digitales, marketplaces regionales– avanzó sin cortapisas. Los consumidores comenzaron a familiarizarse con las compras en línea aprovechando la conveniencia y precios competitivos. Pero por otro lado, la falta de normas claras derivó en notorias fallas de mercado: fraudes impunes (estafas piramidales y sitios fantasma que cobraban sin entregar), abuso de datos personales sin consentimiento, ausencia de políticas de devoluciones o garantías, y una enorme desconfianza del público hacia lo digital.

A mediados de la década, encuestas de la época mostraban que la principal barrera para el comprador latinoamericano era el temor a ser engañado o que sus datos financieros fuesen robados, sentimiento exacerbado por la falta de un paraguas legal protector. Esta primera ola de crecimiento *“a la buena de Dios”* dejó una enseñanza clave: el mercado por sí solo no siempre corrige estas fallas, y que el crecimiento sin normas claras no es sostenible en el tiempo sin erosionar la confianza de usuarios e inversores.

El rol pasivo (y luego punitivo) **del Estado**

Si durante los inicios del comercio electrónico el Estado actuó con pasividad –ya fuera por desconocimiento, lentitud procedimental o por priorizar otras agendas–, con el pasar del tiempo, su postura viró hacia la reacción punitiva ante el surgimiento de conflictos y presiones sociales.

En la segunda década (2010–2020), los gobiernos empezaron a despertar ante el impacto del comercio digital, muchas veces motivados por crisis o escándalos. Un ejemplo paradigmático fue la llegada de Uber y las plataformas de transporte compartido a la región a partir de 2013. Inicialmente, Uber operó en un limbo legal en prácticamente todas las urbes latinoamericanas. Para 2016, ninguna contaba con un marco legal para Uber, excepto la Ciudad de México, que ese año se convirtió en la primera en regular su servicio. En el resto de las metrópolis, el vacío normativo derivó en conflictos abiertos: protestas masivas de taxistas, denuncias por competencia desleal, bloqueos y violencia en las calles de Bogotá, Buenos Aires, São Paulo, Santiago, entre otras.

La reacción gubernamental, al sentirse desbordados, fue frecuentemente prohibir o sancionar a la plataforma y sus conductores. Jueces locales dictaron órdenes de cese (muchas veces revertidas poco después) y se impusieron multas, mientras se trabajaba apresuradamente en legislación de emergencia. En Chile, por ejemplo, recién en 2023 se promulgó la **“Ley Uber” (N°21.553)**,⁷ un marco integral para regular las aplicaciones de ride-hailing después de casi una década de operaciones de Uber y Cabify en la *alegalidad*. Este patrón –de tolerancia inicial seguida de mano dura repentina– se repitió en numerosos países con Uber, Airbnb y otras plataformas disruptivas.

El caso de Airbnb refleja dinámicas similares en el sector turístico-inmobiliario. Durante años, la plataforma de alquileres vacacionales creció en Latinoamérica sin

regulación específica, aprovechando un vacío que le permitía no tributar impuestos hoteleros ni cumplir normativas urbanas. Esto originó que muchas ciudades finalmente optaran por frenar y regular su actividad ante las quejas del sector hotelero y de comunidades locales. Hacia 2023, ciudades como Buenos Aires habían impuesto registros obligatorios y límites de días de alquiler, mientras Bogotá aplicaba una tasa parafiscal a las estancias cortas.

A nivel global, Nueva York y otras urbes directamente prohibieron los alquileres menores a 30 días sin residente presente, y penalizó su incumplimiento con multas de miles de dólares. Detrás de estas medidas punitivas subyace el reconocimiento de que Airbnb operaba “libre de impuestos” y con ventajas competitivas desiguales, en una distorsión del mercado convencional de hospedaje. Las autoridades voltearon la mirada a esta actividad antes no regulada al notar la merma de impuestos y el clamor de la industria hotelera, lo que llevó a una oleada regulatoria global y regional contra Airbnb y sus similares. Nuevamente, el Estado respondió tarde y en modo correctivo: tras años de inacción, vinieron restricciones severas para contener los efectos negativos acumulados.

No todos los ejemplos de intervención estatal fueron estrictamente coercitivos; algunos surgieron de la cooperación público-privada ante problemas evidentes. Un hito significativo en Brasil ilustró cómo la autorregulación incentivada por el Estado pudo llenar vacíos normativos. En la Black Friday de 2012, miles de consumidores brasileños denunciaron “*maquiagem de*

preço” (subir precios antes para fingir descuentos),⁸ lo que generó un escándalo en redes y en el sitio ReclameAqui.

Tras recibir 8.000 quejas en un solo día, la Cámara Brasileña de Comercio Electrónico (camara-e.net) tomó cartas en el asunto con el apoyo gubernamental: en 2013 lanzó un Código de Ética para Black Friday, al que las tiendas podían adherirse voluntariamente bajo la supervisión de la cámara.⁹

Ludovino Lopes, Founder Partner de Ludovino Lopes Sociedade de Advogados, y presidente de camara-e.net en ese entonces, lideró la iniciativa. Sobre ella, enfatizó que:¹⁰



“Los participantes debían obedecer la legislación vigente, en especial el Código de Defensa del Consumidor, el estatuto de camara-e.net y el nuevo Código de Ética”.



Ludovino
Lopes

Las tiendas que violaran las reglas enfrentarían sanciones como la suspensión del uso del sello de confianza “Black Friday Legal” o la expulsión de eventos futuros. Este esfuerzo de autorregulación, reconocido por las autoridades, buscó restaurar la confianza de los compradores sin necesidad (por el momento) de una ley nueva, actuando más rápido que el proceso legislativo.

El caso brasileño demuestra que el Estado, aun partiendo de un rol pasivo inicial, puede pivotar hacia facilitador de soluciones colaborativas cuando el mercado da señales de alarma. Con todo, a nivel regional, la constante fue similar: primero, dejar hacer; luego, intentar componer. Esa reacción tardía a menudo implicó medidas drásticas, ajustes apresurados a leyes existentes o creación de regulaciones emergentes que, si bien resolvieron la crisis puntual, evidenciaron la falta de previsión estratégica.



Brecha regional en materia legal digital

En Iberoamérica, la evolución de los marcos normativos digitales ha sido desigual, lo que ha creado una brecha regional entre países adelantados y rezagados en regulación. Brasil suele citarse como modelo de avances:

no sólo promulgó tempranamente normativa específica para comercio electrónico (ej., el Decreto 7.962/2013 que reguló la contratación online y protección al consumidor en ventas a distancia),¹¹ sino que consagró derechos digitales de vanguardia mediante el Marco Civil de Internet (2014) – una ley pionera que garantiza la neutralidad de la red, la libertad de expresión en línea y la responsabilidad de intermediarios¹²– y posteriormente adoptó una Ley General de Protección de Datos Personales (LGPD, 2018), equiparable al estándar europeo GDPR.

Brasil, impulsado tanto por el sector público como por una fuerte representación gremial (camara-e.net), consiguió un ecosistema normativo integral para 2020, que abarca desde transacciones electrónicas seguras hasta privacidad y cibercrimen.

En contraste, otras naciones sudamericanas llegaron mucho más tarde – o aún no han llegado – a ese grado de madurez legal. Por ejemplo, Bolivia no cuenta hasta 2025 con una ley específica de comercio electrónico ni de protección integral de datos personales. El comercio digital boliviano ha operado apoyándose en normativas generales (como una ley de telecomunicaciones de 2011) y apenas un par de resoluciones administrativas sobre impuestos al comercio en línea, lo que deja al país con uno de los entornos legales menos desarrollados en la materia dentro de la región.

Entre ambos extremos existen casos intermedios. Paraguay, por ejemplo, promulgó la Ley de Comercio Electrónico (Nº 4868) en 2013 – relativamente temprano

–, que regula la contratación por medios digitales y las firmas electrónicas,¹³ incluso adherido a acuerdos regionales como el Acuerdo de Comercio Electrónico del Mercosur (incorporado en 2023). No obstante, Paraguay apenas en años recientes es cuando debate una ley robusta de datos personales y por ahora sólo tiene normativas parciales (como una ley de 2020 enfocada en datos crediticios).

México y Argentina son ejemplos de países con cierta delantera en aspectos puntuales pero rezagos en otros: México modificó su Código de Comercio desde 2000 para dar validez a actos de comercio electrónico e implementó una norma oficial (NOM-151) sobre conservación de mensajes de datos, además de poseer una ley federal de protección de datos desde 2010;¹⁴ sin embargo, carece de una ley unificada de economía digital y ha optado por reglamentaciones sectoriales.

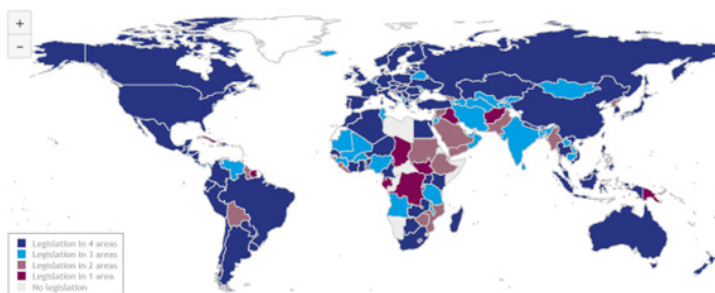
Argentina, por su parte, fue pionera regional en protección de datos con la Ley 25.326 de 2000 (incluso reconocida por la UE como adecuada en su momento)¹⁵ y en 2001 sancionó la Ley de Firma Digital,¹⁶ pero no llegó a dictar una ley específica de ecommerce – su regulación se da mediante disposiciones dispersas en la Ley de Defensa del Consumidor y en decretos sobre venta domiciliaria –, y hasta 2023 no había actualizado su ley de datos para alinearla con estándares modernos. Estas diferencias se traducen en entornos dispares para negocios y usuarios: emprender una startup fintech o de retail digital en São Paulo ofrece mucha más certeza jurídica que hacerlo en La Paz o Asunción, por ejemplo.

Para visualizar comparativamente el estado de los marcos regulatorios digitales en países seleccionados al año 2025, presento a continuación un cuadro sinóptico:

País	Legislación de comercio electrónico	Protección de datos personales	Otros marcos relevantes
Brasil	Decreto 7.962/2013 (ventas online), Marco Civil de Internet 2014	Ley 13.709/2018 (LGPD, vigente 2020)	Código de Defensa del Consumidor (1988, aplica a ecommerce); Ley de Cibercrimen 2012
México	Reformas Código de Comercio 2000 (e-contracting); NOM-151 y NOM-CO-34 (reglas ecommerce)	Ley Federal de Protección de Datos Personales 2010	Ley Fintech 2018; Regulación tributaria IVA digital 2020
Colombia	Ley 527/1999 (comercio electrónico y firma digital); Estatuto del Consumidor 2011 (incluye ventas por medios electrónicos)	Ley 1581/2012 (habeas data)	Decreto 886/2014 (comercio minorista electrónico); Ley 1273/2009 (delitos informáticos)
Argentina	Sin ley específica integral (ecommerce regulado por Ley de Defensa del Consumidor y Código Civil-Comercial)	Ley 25.326/2000 (protección de datos), Decreto 1559/2001 reglamentario	Ley 25.506/2001 (firma digital); Ley 26.388/2008 (delitos informáticos)
Paraguay	Ley 4868/2013 de comercio electrónico (reglamentada 2014)	Sin ley general aún (Ley 6534/2020 de datos crediticios; proyecto de ley integral en debate)	Ley 4.568/2011 (firma digital); Ley 7102/2023 (acuerdo Mercosur de ecommerce)
Bolivia	Sin ley específica (se aplica ley 164/2011 de telecomunicaciones)	Sin ley general (protección de datos pendiente, sólo disposiciones sectoriales)	RND 10-0016-15 y 10-0025-14 (resols. imp. sobre ecommerce); código de comercio 1977 (obsoleto)

Tabla. Contraste de marcos regulatorios digitales en Iberoamérica (al 2025). Países como Brasil y México han desarrollado legislaciones integrales o sectoriales que brindan certidumbre al comercio electrónico y la economía digital. Otros, como Bolivia, aún carecen de leyes específicas, con lo que operan con vacíos importantes en la protección al consumidor y datos personales. (Fuente: elaboración propia con datos públicos de cada país)

Como evidencia la tabla, la región exhibe un mosaico normativo heterogéneo. A nivel global, América Latina y el Caribe han avanzado en la última década en cerrar algunas brechas: para 2021, aproximadamente el 71% de los países de la región tenía una ley de protección de datos, y el 80%, alguna normativa de cibercrimen, con lo que se acercaba a los promedios mundiales.¹⁷



Mapa global de la adopción de marcos legales sobre comercio electrónico, protección de datos, privacidad y ciberseguridad. Fuente: *Global Cyberlaw Tracker*, UNCTAD (2024).

Sin embargo, subsisten rezagos en materia de protección al consumidor en línea, actualización de normas de propiedad intelectual para entornos digitales, y armonización regional. La Unión Europea, por comparación, contó desde el año 2000 con la Directiva de Comercio Electrónico y hoy tiene reglamentos como el Digital Services Act (2022),¹⁸ que impone obligaciones claras a las plataformas; esa anticipación ha sido escasa en Latinoamérica. Recién en años recientes, organismos como ELAC (Agenda Digital para América Latina y el Caribe) y convenios subregionales (e.g., Mercosur Digital) han fomentado la convergencia de estándares legales.

No obstante, las disparidades internas aún generan “paraísos” y “zonas grises” regulatorias: empresas que operan panregionalmente tienden a establecerse donde el marco es más favorable o definido (por ejemplo, tech startups eligen Ciudad de México o São Paulo sobre plazas con más incertidumbre). Esto plantea un desafío futuro: sin esfuerzos coordinados, la brecha legal podría traducirse en brecha de innovación, lo que profundiza las

diferencias económicas entre países líderes y rezagados en el entorno digital.

Lecciones aprendidas

Tras este recorrido de 25 años – del auge inicial desregulado, pasando por choques y ajustes, hasta la situación actual – emergen lecciones valiosas para el futuro del ecosistema digital iberoamericano. La primera –y fundamental– es que la confianza es el cimiento del comercio electrónico: construirla requiere tanto innovación tecnológica como certeza jurídica. Cada ola de abusos o escándalos (fraudes, brechas de datos, conflictos con industrias tradicionales) minó la confianza de los usuarios y obligó a reacciones correctivas de gobiernos y empresas.

Por ello, hoy existe consenso en que prevenir es mejor que curar: es preferible desarrollar marcos normativos proactivos y flexibles que anticipen los potenciales conflictos, en vez de lidiar con sus consecuencias cuando el daño ya está hecho. Esto implica dotar de mayor agilidad a los procesos legislativos y regulatorios, abrir canales permanentes de diálogo entre reguladores e innovadores, y adoptar principios regulatorios “adaptativos”.

Al respecto, el experto [Alejandro Prince, Director de Prince Consulting y miembro de la Comisión Directora Fundadora de la Cámara Argentina de Comercio Electrónico \(CACE\)](#),¹⁹ sostiene que:



“Las leyes en la era digital deben ser leyes vivas, susceptibles de actualización constante a medida que surgen nuevas tecnologías, para evitar quedar obsoletas al poco de nacer. La adaptabilidad normativa es clave para no repetir el déjà vu de un Estado siempre corriendo detrás de la tecnología”.



Alejandro
Prince

Otra lección aprendida es la importancia de la autorregulación y la cooperación público-privada como complemento a la ley. La experiencia de la Cámara de Comercio Electrónico en Brasil con el Código de Ética, o los diversos sellos de confianza y estándares voluntarios creados por cámaras sectoriales (como los programas de “Compra Segura” de distintas asociaciones en la región), han demostrado que el sector privado puede –y debe– asumir responsabilidad en elevar las prácticas de la industria. Estas iniciativas funcionan mejor cuando están alineadas o reconocidas por políticas públicas, lo que genera una corregulación eficaz.

Asimismo, los casos exitosos señalan la necesidad de educación digital de todos los actores: los legisladores y jueces de las nuevas generaciones están más familiarizados con la tecnología que sus predecesores, lo que reduce la brecha de entendimiento que tantas veces dificultó actualizar las leyes. La capacitación de pymes y usuarios en derechos y deberes digitales también se ha vuelto esencial para empoderar a la ciudadanía digital y

que esta exija –en tiempo y forma– mejores prácticas a las empresas y acción a sus gobernantes.

Finalmente, la historia del ecommerce regional deja una mirada de legado y de futuro. Como participante de esta travesía desde sus albores, recuerdo que a fines de los 90 debíamos evangelizar sobre las bondades del comercio electrónico ante funcionarios escépticos; hoy, en cambio, nadie cuestiona la importancia estratégica de la economía digital, pero quedan pendientes debates éticos y jurídicos mucho más complejos (desde la inteligencia artificial hasta el derecho al olvido, pasando por la fiscalidad de los gigantes digitales).

Si algo hemos aprendido, es que innovación y regulación no deben ser fuerzas opuestas sino complementarias en un mismo ecosistema. El ideal es un círculo virtuoso: un marco legal claro y justo genera confianza, la confianza impulsa la adopción tecnológica, y esa adopción exitosa retroalimenta la prosperidad económica y la demanda de seguir innovando. Para lograrlo, Iberoamérica cuenta con la ventaja de poder observar experiencias previas (propias y ajenas) y no tropezar dos veces con la misma piedra. Los déjà vu de las regulaciones pueden romperse si incorporamos la visión sistémica: entendiendo el comercio digital como un fenómeno transversal que involucra a múltiples sectores y naciones, y abordándolo con políticas integrales y coordinadas.

En conclusión, el ecosistema digital de nuestra región ha madurado entre aciertos y tropiezos, y deja como legado una convicción compartida: el futuro digital

requiere tanto de la audacia para innovar como de la sabiduría para regular. Ninguna revolución tecnológica perdura sin un andamiaje institucional que la sostenga. A 25 años del génesis del ecommerce iberoamericano, nos encontramos ante una nueva encrucijada histórica – con tecnologías emergentes como la IA generativa, el metaverso o la Web3 llamando a la puerta –, que nos invita a aplicar estas lecciones con humildad y determinación.

Es responsabilidad de nuestra generación de líderes digitales, legisladores, académicos y emprendedores trabajar juntos para crear “leyes con visión de futuro”, capaces de adaptarse al cambio continuo sin perder de vista la protección de los valores fundamentales. Sólo así transformaremos los *déjà vu* del pasado en oportunidades de crecimiento sostenible, para asegurar que la brecha entre innovación y regulación se acorte, y que el futuro digital iberoamericano se construya sobre cimientos de confianza, inclusión y desarrollo compartido.

Este recorrido ha sido más que un ciclo de desafíos legales: ha sido una escuela de aprendizaje colectivo. Cada obstáculo enfrentado nos hizo más resilientes y creativos: desde improvisar soluciones legales en tiempos donde no existían, hasta reformar instituciones enteras para abrazar la digitalización. Que las próximas generaciones tomen este legado y lo amplíen. Como me gusta decir, “lo imposible sólo tarda un poco más”, y con la experiencia ganada, ese “poco más” ahora puede ser tiempo ganado y no tiempo perdido. El desafío está servido; el futuro digital de Iberoamérica nos espera, y esta vez, sin dudas, llegaremos preparados.

GÉNESIS

DE UN FUTURO DIGITAL



ACCEDE A LAS
DIMENSIONES



Déjà vus regulatorios: Viejos problemas, nuevas caras

Es curioso cómo, tras más de dos décadas involucrado en el comercio digital iberoamericano, sigo experimentando la sensación de *déjà vu* ante muchos desafíos legales. Continuamente se repiten viejos problemas con nuevas máscaras.

A continuación, recorro estos “*déjà vu*” regulatorios en cinco secciones, contrastando experiencias pasadas con datos recientes de 2024-2025, y con voces expertas de nuestro ecosistema digital.

Del catálogo digital al marketplace: Las reglas llegan tarde

A principios de los 2000, cuando comenzamos a publicar catálogos de productos en línea, el terreno normativo era prácticamente una hoja en blanco. Recuerdo catálogos

digitales pioneros –sitios modestos que mostraban productos como si fueran vitrinas virtuales– operando en un limbo legal. Las mismas dudas que enfrentaron aquellos catálogos resurgen años después con los marketplaces: *¿Qué responsabilidades tiene la plataforma intermediaria? ¿Quién responde si algo sale mal en una transacción entre terceros?* En aquellos primeros años, muchos reguladores ni siquiera comprendían el modelo de negocio; las reglas siempre llegaban tarde, cuando el modelo ya había evolucionado.

Como responsable legal de Mercado Libre en sus inicios, **Jacobo Cohen Imach, Senior Vice President y General Counsel de Mercado Libre**,²⁰ vivió de primera mano esa necesidad de *inventar* marcos legales sobre la marcha. Jacobo recuerda que en Argentina la discusión sobre responsabilidades surgió muy temprano, pero se encaró de forma constructiva:



“Pasó de no regular y de no proteger los datos personales a una norma que ponía el tema sobre la mesa, lo enfrentaba de manera lógica y constructiva”.



**Jacobo
Cohen Imach**

Aquella primera ley de protección de datos de 2000 fue pionera en la región, y se logró “*sentar a los jugadores en la mesa*” para consensuar protecciones sin frenar la innovación. Sin embargo, fuera del tema datos personales, otros aspectos del comercio digital quedaron

sin respuesta clara por años. La figura del “**intermediario**” en plataformas generaba resquemor: tradicionalmente, las leyes asignaban la responsabilidad al vendedor o al fabricante, pero ¿qué hacer cuando un sitio conecta a miles de vendedores con millones de compradores?

En ausencia de regulación específica, en Mercado Libre optaron por la autorregulación como salida audaz. Como describe Jacobo Cohen Imach (eLíderes Podcast x25, 2025):



“Establecimos una manera: si alguien sentía que su derecho de propiedad intelectual estaba siendo lesionado, nos avisaba y dábamos de baja la publicación. Y eso se convirtió en el estándar de la industria”.



Jacobo
Cohen Imach

Así nació el programa de protección de propiedad intelectual (*notice-and-takedown*), mucho antes de que la ley lo exigiera. Fue un parche necesario ante un vacío legal: no podíamos esperar años para que el Congreso entendiera la economía de plataformas. Esta autorregulación proactiva mitigó riesgos, aunque no eliminó la incertidumbre jurídica.

Esa incertidumbre se manifestó en casos concretos. En **Argentina**, a medida que Mercado Libre crecía, no faltaron intentos de responsabilizarla por las acciones de

sus usuarios. Un ejemplo son las sanciones por ventas de bienes prohibidos o infracciones tributarias de terceros en la plataforma. Recientemente, la Aduana argentina imputó a Mercado Libre por supuestas irregularidades en importaciones de dispositivos, acusándola de subdeclarar mercancías para evadir impuestos.²¹

Si bien este caso de 2022 trata sobre bienes propios (terminales de pago), ilustra la creciente atención de los entes fiscalizadores: perciben a la plataforma como un actor central, casi como si fuera un importador o minorista tradicional, y le exigen cuentas cuando algo no cuadra. Del mismo modo, la Secretaría de Comercio Interior llegó a imputar a Mercado Libre por presunta competencia desleal, bajo el argumento de que algunos vendedores eludían requisitos formales (por ejemplo, no emitían facturas) aprovechando el modelo de marketplace.

En **Brasil** se dio una situación análoga: asociaciones de comercio reclamaron que Mercado Livre exigiera a todos sus vendedores la emisión de la *nota fiscal* (comprobante tributario obligatorio), pues temían que vendedores informales obtuvieran ventajas indebidas en la plataforma. Es paradójico –y aquí el *déjà vu*– ver cómo se repite la historia: lo mismo que se objetaba a sitios de subastas en los 2000 (facilitar ventas “sin controles”) resurge ahora con marketplaces modernos.

En **México**, las autoridades también han puesto la mira en las plataformas. La Procuraduría Federal del Consumidor (Profeco) en 2023 estableció una mesa de

trabajo permanente con Mercado Libre para mejorar la transparencia hacia usuarios, tras detectar problemas en ofertas de terceros (productos incumpliendo normas, publicidad engañosa, etc.). Y en materia de competencia, la COFECE (Comisión Federal de Competencia Económica) inició una investigación por posibles prácticas anticompetitivas en comercio electrónico. Finalmente, Amazon y Mercado Libre evitaron multas en México luego de dicha investigación, pero el simple hecho de ser indagadas muestra que los organismos ya no tratan a las plataformas con guante de seda.

Lo que aprendimos de estos episodios es que las **reglas llegaron tarde** y, cuando lo hicieron, a veces intentaron encajar modelos nuevos en categorías viejas. Durante años, ni la ley de defensa del consumidor ni las normativas comerciales contemplaban explícitamente a un *intermediario digital*. Hubo que interpretarlas creativamente. Hoy, varios países están actualizando sus leyes para definir **responsabilidades claras** de las plataformas frente a fraudes, productos defectuosos o abusos cometidos por vendedores terceros.

Aún así, persiste el debate sobre *hasta dónde* debe responder el marketplace. ¿Debe ser solidariamente responsable ante un comprador si un vendedor incumple? ¿O sólo debe actuar diligentemente cuando detecta una infracción? En Europa, la discusión llevó a la **Digital Services Act**; en Latinoamérica, estamos dando recién los primeros pasos, entre autorregulación sectorial y pinceladas regulatorias locales.

Confieso que a veces me frustra ver cómo se repiten estos patrones. Los catálogos digitales de ayer enfrentaron la sospecha de legisladores que no entendían Internet; los marketplaces de hoy enfrentan la de reguladores que aún no comprenden del todo la economía de plataformas. En ambos casos, la innovación va tres pasos adelante de la ley. Sin embargo, también soy testigo de cómo hemos avanzado: lo que antes era un vacío total, hoy son mesas de diálogo público-privadas.

Si en 2000 costaba explicar qué era vender online, en 2025 al menos logramos que las autoridades vean a las plataformas como aliados potenciales en la formalización y la protección al consumidor. Falta camino por recorrer, pero el simple hecho de que estemos discutiendo impuestos, defensa del consumidor y competencia en marketplaces muestra que las reglas, aunque tarde, **están llegando**.

Matriz de responsabilidades **en el comercio colaborativo**

Buena parte del conflicto regulatorio que rodea a los marketplaces y al comercio colaborativo nace de una pregunta básica que casi nadie responde igual: **¿quién tiene que hacerse cargo de qué?** ¿Es la plataforma, el vendedor, el medio de pago, el regulador o todos a la vez? En la práctica, cada incidente —un producto defectuoso, un pago fraudulento, un dato mal usado, un contenido engañoso— se convierte en una pulseada para ver quién paga la cuenta económica, legal y reputacional.

En los libros vivos [“El boom del comercio electrónico”](#) y [“La implementación de los modelos unified & collaborative commerce”](#) mostramos cómo, del catálogo digital al marketplace y de ahí a las plataformas de servicios, el ecosistema pasó de relaciones bilaterales simples (retailer–proveedor, tienda–consumidor) a una **trama de múltiples actores interdependientes**. Aquí damos un paso más: vestimos esa arquitectura colaborativa con su capa de responsabilidades legales y regulatorias, para que nadie se esconda detrás del “yo sólo pongo la tecnología” ni caigamos en el extremo opuesto de pretender que la plataforma responde por todo.

Para ordenar el mapa, proponemos una **matriz de responsabilidades plataforma–merchant–usuario–Estado**, que cruza cuatro grandes actores con seis ámbitos críticos:

□ **Actores (filas):**

- Plataforma (marketplace, superapp, app de delivery, plataforma de servicios).
- Merchant / proveedor (marca, retailer, seller third party, profesional que presta el servicio).
- Usuario / consumidor (comprador, destinatario, usuario final).
- Estado / regulador (autoridades de datos, consumo, competencia, fiscalidad, banca central, etc.).

□ **Ámbitos (columnas):**

- Datos personales y privacidad.
- Contenidos e información (listados, reseñas,

claims, publicidad).

- Producto / servicio (seguridad, calidad, aptitud para el uso).
- Pagos, fraude y prevención de lavado. Impuestos y obligaciones fiscales.
- Publicidad, influencers y uso comercial de datos.

La lógica no es buscar al “culpable único”, sino **visualizar dónde hay responsabilidad principal, dónde responsabilidad compartida y dónde responsabilidad residual** (secundaria, pero real). Una matriz típica, en un marketplace generalista B2C, podría verse así:

- En **datos personales**, la plataforma suele tener **responsabilidad principal** como controladora o corresponsable del tratamiento (define fines y medios del procesamiento), mientras que el merchant asume una **responsabilidad compartida** cuando descarga y reutiliza esos datos para su propio fulfillment o marketing. El usuario tiene una responsabilidad residual en el uso que hace de su propia información (por ejemplo, compartir credenciales), y el regulador fija reglas y fiscaliza su cumplimiento. Esta lectura dialoga directamente con lo que desarrollamos en [“El arribo de las tecnologías exponenciales y la transformación del ecosistema”](#), cuando hablamos de **data trust flywheel** y de la necesidad de una gobernanza explícita del dato para que el flywheel pueda girar.
- En **contenidos e información**, la **responsabilidad principal** por la veracidad de las descripciones,

claims y reseñas sobre un producto recae en el merchant o proveedor; la plataforma asume una **responsabilidad compartida** al diseñar el sistema de publicación, moderación y ranking (qué incentiva, qué tolera, qué detecta y qué remueve). El usuario soporta responsabilidad directa sobre las reseñas que publica y el Estado interviene a través de normas de publicidad, defensa del consumidor y, en algunos casos, responsabilidad por contenidos dañinos. Este cruce se conecta con ["El desarrollo del retail media network"](#): allí mostramos cómo la plataforma pasa de ser "estantería" a ser **medio de comunicación y segmentación publicitaria**; aquí hacemos explícito que ese rol también viene con responsabilidades adicionales.

- En **producto / servicio**, la **responsabilidad principal** suele estar en el merchant: es quien fabrica, importa o provee, y quien responde por la seguridad, la calidad y la conformidad. La plataforma toma responsabilidades específicas (por ejemplo, cuando concentra logística, fulfillment, empaquetado o cuando conoce y tolera patrones de incumplimiento reiterados de ciertos sellers). El usuario tiene deberes de uso adecuado, y el Estado fija estándares de seguridad, etiquetado, garantías, etc. Esta distribución conecta con los casos y aprendizajes que contamos en ["El boom del comercio electrónico"](#), donde muchos conflictos no nacían en la tecnología sino en **prácticas comerciales heredadas del mundo físico que no se actualizaron al nuevo contexto digital**.
- En **pagos, fraude y prevención de lavado**, la matriz cambia de forma: los medios de pago, adquirentes, emisores y billeteras —a veces integrados a la

plataforma, a veces terceros— comparten con la plataforma y el merchant una combinación de responsabilidades. Aquí el Estado (banco central, unidad de inteligencia financiera, regulador financiero) juega un rol protagónico. Según la configuración del modelo —como mostramos en [“La implementación de los modelos Unified & Collaborative Commerce”](#)— la plataforma puede limitarse a ser “pasarela” o convertirse en **agregador de pagos, emisor de saldo o incluso proveedor de crédito**, asumiendo obligaciones mucho más pesadas.

- En **impuestos y obligaciones fiscales**, el merchant tiene responsabilidad principal sobre facturación, declaración y pago de tributos derivados de las operaciones; la plataforma puede actuar como **agente de retención o percepción**, y en algunos países ya tiene obligaciones directas de información y recaudación sobre las operaciones de terceros. El usuario tiene deberes como contribuyente según el tipo de operación, y el Estado define el diseño fiscal (o su ausencia) que veremos repetidamente como déjà vu a lo largo de este libro.
- En **publicidad, influencers y uso comercial de datos**, la responsabilidad se distribuye entre:
 - El merchant o marca que contrata la campaña y define el mensaje.
 - La plataforma y la red de retail media que decide cómo, a quién y con qué datos impactar.
 - El influencer o creador que ejecuta la pieza.

- El regulador que fija reglas de transparencia, etiquetado y protección de audiencias. Los conflictos que analizamos aquí conversan con los casos y modelos expuestos en [“El desarrollo del retail media network”](#), donde el gran desafío no es sólo monetizar la atención, sino hacerlo **sin quemar el capital de confianza** construido con consumidores y reguladores.

Llevar esta matriz a una tabla concreta —plataforma, merchant, usuario y Estado en filas; ámbitos en columnas; y casillas marcadas con “P” (principal), “C” (compartida) o “R” (residual)— ayuda a desmontar dos mitos peligrosos:

1. El mito de que “la plataforma sólo pone la tecnología y no responde por nada”.
2. El mito opuesto de que “la plataforma es responsable de absolutamente todo lo que ocurre en su ecosistema, sin matices ni graduaciones”.

En la práctica, la clave está en **cómo se diseñan y gobiernan las interacciones**. En [“La implementación de los modelos unified & collaborative commerce”](#) veíamos que un mismo actor puede jugar como retailer, marketplace, proveedor logístico y medio de pago dentro de un mismo ecosistema. Esta matriz permite preguntarse, para cada sombrero que se pone la plataforma, **qué responsabilidades adicionales activa** y qué acuerdos contractuales y de cumplimiento necesita construir con sus merchants y partners.

Esta lógica no es sólo teórica. A lo largo del capítulo siguiente, cuando revisemos **jurisprudencia clave y casos que sentaron precedentes**, veremos cómo muchos fallos se pueden “mapear” sobre esta matriz: qué tribunales reforzaron la responsabilidad principal del merchant, cuándo consideraron que la plataforma debía responder solidariamente, en qué contextos el regulador fue detrás del medio de pago o del intermediario logístico, y cómo el comportamiento del usuario también entra en juego.

Nuestra recomendación —en línea con la cultura de **human augmented AI** que recorre toda la colección *Génesis de un Futuro Digital*— es que cada organización construya su propia versión de esta matriz, apoyándose en IA-Unificada para:

- ☐ Relevar contratos y T&Cs existentes.
- ☐ Identificar lagunas o contradicciones entre “lo que hacemos” y “lo que decimos que hacemos”.
- ☐ Simular qué cambia si se modifica una regulación o si un caso emblemático sienta un nuevo estándar.

Así, la matriz deja de ser un cuadro estático en un libro y se convierte en una **herramienta viva de conversación** entre negocio, legal, compliance, producto y partners del ecosistema.

Publicidad digital y protección al consumidor:

Una deuda sin saldar

La publicidad es otro terreno que experimentó un *déjà vu* constante. Vuelvo mentalmente a mis días diseñando banners y popups en los albores de la web comercial, cuando intentábamos aplicar las normas de publicidad tradicional a los nuevos formatos digitales. Ya entonces era difícil encajar los viejos marcos en las nuevas prácticas, y hoy esa dificultad persiste ampliada. Las leyes de *lealtad comercial* o *publicidad engañosa* datan de la era de la televisión y el papel impreso; al trasladarlas al ecosistema digital, quedan grietas enormes.

Un ejemplo evidente es el fenómeno de los **influencers** y el marketing en redes sociales. Las regulaciones tradicionales exigen que la publicidad se identifique como tal –uno ve en la TV el rótulo de “PNT” o en una revista la palabra “Publicidad”–, pero ¿qué pasa cuando un influencer de Instagram recomienda un producto? Durante mucho tiempo, en nuestra región esto ocurrió en tierra de nadie: miles de influencers promoviendo marcas sin aclararlo, mezclando contenido orgánico con pautas pagas, ante consumidores que difícilmente distinguen.

Yerka Yukich, Secretaria Ejecutiva del Centro de Economía Digital de la Cámara de Comercio de Santiago,

lo señaló en una entrevista: Chile, por ejemplo, vio crecer su comercio electrónico un 8% en 2024 y “*está retomando los ritmos de crecimiento previos a la pandemia*”, con una

proyección de tasas de dos dígitos para 2025. Ese boom digital incluye el auge del influencer marketing, pero la regulación publicitaria no ha acompañado el ritmo.

Los datos actuales muestran la magnitud del fenómeno: En Latinoamérica, **hasta un 64 % de los consumidores** afirma que sus decisiones de compra están influenciadas por creadores de contenido.²² La inversión global en marketing de influencers alcanzó los **USD 32.55 mil millones** en 2025, con un retorno de inversión (ROI) promedio de **5.78x**.²³ En América Latina, el marketing de influencers continúa consolidándose como una estrategia clave para las marcas, impulsada por la confianza en su capacidad para aumentar ventas y engagement.²⁴ En México, el marketing de influencers ha alcanzado una etapa de madurez y sofisticación, con una inversión creciente y procesos más profesionales, lo que ha resultado en un impacto tangible en los resultados de negocio.²⁵

A pesar de este crecimiento, la mayoría de los países iberoamericanos aún carece de una normativa clara sobre publicidad digital encubierta, lo que representa un desafío para la regulación del sector.

En Estados Unidos, la **Comisión Federal de Comercio (FTC)** mantiene guías actualizadas para regular la publicidad realizada por influencers y creadores de contenido. Las *Endorsement Guides*, revisadas en 2023,²⁶ establecen criterios claros sobre cómo los anunciantes y los influencers deben divulgar cualquier relación comercial para garantizar transparencia y proteger a los consumidores de prácticas engañosas. Además, la

FTC ofrece recursos específicos como *Disclosures 101 for Social Media Influencers*,²⁷ que orientan sobre cuándo y cómo comunicar adecuadamente la existencia de compensaciones o patrocinios en publicaciones en redes sociales, como una forma de adaptarse a la dinámica cambiante del marketing digital y para reforzar la confianza del consumidor.

Pero en nuestra región, ¿qué tenemos? Predominan esfuerzos aislados y recientes.

México fue pionero en 2023 al publicar la *Guía de Publicidad para Influencers*, vía Profeco.²⁸ Dicho documento –inspirado en gran medida por las guías de la FTC– estipula que el influencer debe revelar vínculos materiales con anunciantes (usando hashtags como #Publicidad o #Ad, por ejemplo) y ser veraz en lo que comunica. Es un avance, sin duda, pero cabe aclarar que se trata de lineamientos administrativos, no de una ley en sentido estricto.

En otros países, la situación es incluso más precaria: en Argentina o Colombia, por ejemplo, la “publicidad digital” sigue regida por los mismos principios generales de siempre (veracidad, no inducción a error) pero sin reglas concretas para influencers, publicaciones en redes o videos de YouTube. Apenas algunas autorregulaciones: códigos de ética publicitaria voluntarios y recomendaciones de cámaras de la industria. En síntesis, la deuda regulatoria persiste –seguimos sin saldarla– en cuanto a brindar **protección al consumidor** frente a las nuevas formas de publicidad online.

Otra área nebulosa es la del **retargeting, las cookies y el uso de datos personales en campañas digitales**. Aquí confluyen la normativa de privacidad con la de publicidad. Europa marcó el camino con su *ePrivacy Directive* y, más recientemente, con estrictas reglas de consentimiento para cookies bajo el GDPR.

Latinoamérica, de nuevo, va rezagada. Varios países cuentan con leyes de protección de datos personales (Argentina desde 2000, México en 2010, Brasil y su LGPD de 2018, Chile con una nueva ley en 2024, etc.), pero ninguna aborda de forma detallada la publicidad comportamental o el seguimiento online. El resultado: hasta hace poco, prácticamente cualquier sitio podía rastrear a los usuarios con cookies de terceros y perfilar sus hábitos sin mayor restricción, más allá de la aceptación tácita de términos y condiciones eternos que nadie leía. Recién ahora empezamos a ver un cambio.

Brasil, por ejemplo, con la LGPD estableció bases legales para el tratamiento de datos y creó una autoridad de protección de datos; en 2023 se aplicaron las primeras multas a empresas por violaciones a la LGPD, lo que inauguró una fase de enforcement efectiva.

Chile, tras años de debate, aprobó su Ley 21.719 de Protección de Datos Personales en diciembre de 2024, que creó también una agencia reguladora e impuso 24 meses para adaptarse. Estos marcos generales obligarán a las empresas a ser más transparentes en el uso de datos para publicidad, pero sigue sin haber lineamientos específicos sobre, por ejemplo, **publicidad basada en cookies o retargeting**.

Para entender lo rezagados que estamos, basta comparar con Estados Unidos: allí, incluso sin ley federal de privacidad, ya hubo sanciones ejemplares a prácticas de seguimiento opacas.

Un caso ilustrativo es el de *Sephora* en California (2022): la fiscalía estatal multó con USD 1,2 millones a la cadena por no respetar el derecho de los usuarios a excluirse de la venta de sus datos. Sephora permitía cookies de terceros y píxeles que recolectaban información para publicidad dirigida sin informar adecuadamente ni honrar las preferencias de *opt-out* del consumidor. Ese caso mandó un mensaje claro al retail estadounidense: incluso sin una ley federal, los reguladores locales harán valer los nuevos derechos digitales de los ciudadanos.

En Iberoamérica, ¿hemos visto algo similar? Por ahora no. Ningún país de la región ha multado (que se sepa públicamente) a una empresa por usar cookies de seguimiento sin consentimiento. En la práctica, muchos sitios latinoamericanos implementaron banners de cookies *por presión global* (para cumplir con usuarios europeos o buenas prácticas internacionales), no porque sus leyes locales lo exigieran contundentemente.

Entonces, ¿qué tenemos? Una **brecha normativa** donde el consumidor queda desprotegido ante ciertas prácticas digitales. Influencers que publicitan sin avisar, anuncios hipersegmentados cuyos criterios nadie explica, recolección de datos de navegación sin transparencia... Todo esto ocurre mientras las agencias de protección

al consumidor locales tratan de aplicar, con calzador, normas pensadas para otro contexto.

Las guías de la FTC en EE.UU. no tienen equivalentes claros en la mayoría de los países iberoamericanos, aunque, como vimos, México dio un paso y otros podrían seguir. Algunos actores privados han propuesto autorregulaciones: por ejemplo, en Colombia, la ANDA (Asociación Nacional de Anunciantes) lanzó recomendaciones para marketing de influencers; y en España –fuera de nuestra región pero relevante por idioma–, se aprobó en 2021 un Código de Conducta sobre el Uso de Influencers en Publicidad, que sirve de referencia. Sin embargo, estas iniciativas carecen de dientes legales.

Cierro esta sección reconociendo que tenemos aún **una deuda pendiente**. Así como en su momento hubo que reglamentar la publicidad en radio y TV, hoy debemos hacerlo en Instagram, YouTube, TikTok y el entorno web. No para coartar la creatividad de influencers o marcas, sino para **proteger al consumidor** y darle las mismas garantías que espera en medios tradicionales. La buena noticia es que el ecosistema mismo está madurando: muchas marcas ya prefieren ser transparentes (por temor a crisis reputacionales si se descubren engaños), y algunos influencers han profesionalizado su conducta adoptando las mejores prácticas internacionales. Falta que la regulación alcance ese nivel de madurez.

Medios de pago y su eterna persecución legal

En la historia del comercio electrónico latinoamericano, los métodos de pago digitales han sido la vanguardia que siempre lleva ventaja sobre los marcos legales y tributarios. Primero fueron las tarjetas de crédito usadas tímidamente en línea; luego, las *billeteras virtuales*, los pagos contra entrega, las fintech ofreciendo cuentas prepagas, y más recientemente, las **criptomonedas** y transferencias *peer-to-peer*. Cada innovación nació “fuera” o “más allá” del esquema regulatorio existente, lo que obligó una persecución constante por parte de legisladores y entes de control para no quedarse atrás.

En los primeros años, la cuestión principal era la falta de inclusión financiera: poca gente tenía tarjeta o cuenta bancaria, así que la innovación venía de la mano de métodos alternativos (pagos en efectivo en puntos de conveniencia, giros postales, etc.). Recuerdo cómo **Brasil** desarrolló su propio ecosistema de pagos en línea (con Boleto Bancário, transferencias locales), mientras que en **Argentina** surgían plataformas como Dinero Mail y luego Mercado Pago para facilitar transacciones.

Aquellas billeteras nacientes operaban casi sin regulación específica: eran sociedades ofreciendo un servicio tecnológico de pagos, no bancos. Así esquivaban muchas exigencias (encajes, seguros de depósito, reportes prudenciales) que sí tenían las entidades financieras tradicionales. Esta situación ventajosa les permitió crecer

rápido, pero eventualmente atrajo la mirada de los bancos centrales y reguladores fiscales.

Hoy, la **ola fintech** en Latinoamérica es impresionante: entre 2017 y 2024, el número de empresas fintech en la región creció un 340%. Este boom ha empujado la inclusión financiera: según el Banco Mundial, el porcentaje de adultos con cuenta bancaria en la región pasó de aproximadamente un 45% en 2011 a un 73% en 2021,²⁹ lo que significa decenas de millones de nuevos usuarios financieros. Las billeteras digitales y bancos digitales han sumado usuarios que antes operaban sólo en efectivo.

Por ejemplo, **Colombia** logró catalizar la adopción de pagos móviles a través de iniciativas privadas y públicas: servicios como **Nequi** y **Daviplata** incorporaron a millones de colombianos al sistema financiero formal, muchos de ellos jóvenes o habitantes de zonas rurales que nunca antes tuvieron un producto bancario. Hoy en Colombia es común que un puesto de mercado campesino o un taxi en Medellín no acepten tarjeta pero sí pagos vía Nequi; el dinero móvil se ha **normalizado** y ha sido un “*caballo de Troya*” para la inclusión.

Esta expansión vertiginosa de los medios de pago digitales, sin embargo, ha planteado **dilemas regulatorios** complejos. Un eje de tensión ha sido cómo encuadrar legalmente a las billeteras virtuales, fintech de préstamos, criptoactivos y demás jugadores nuevos. *¿Deben someterse a la misma regulación que los bancos? ¿Creamos licencias específicas?* Inicialmente, muchos países aplicaron el criterio “mismo riesgo, misma

regulación”, pero eso no siempre es claro: ¿una billetera que custodia saldos pequeños de usuarios representa el mismo riesgo sistémico que un banco tradicional? Probablemente no, y regular igual podría sofocar la innovación. Por otro lado, dejarlas operar sin supervisión podría abrir la puerta a fraudes o usos ilícitos (piénsese en lavado de dinero a través de billeteras no vigiladas).

La **persecución legal** se observa en decisiones recientes de los entes reguladores. En **Argentina**, durante años Mercado Pago, Ualá y otras fintech operaron como *PSP* (proveedores de servicios de pago) con menor carga regulatoria que un banco. Al ver su masividad, el Banco Central empezó a ajustar las tuercas. En 2022-2023 impuso que las billeteras digitales inmovilicen parte de sus fondos en cuentas bancarias (algo parecido a un encaje), y finalmente en 2023, anunció la creación de **categorías de licencias** según el tamaño de las fintech, lo que insinuaba que las más grandes deberían transformarse en entidades financieras formales.

El mensaje fue que los *unicorns* locales de pagos ya juegan en las grandes ligas y tendrán que someterse a reglas de bancos. De hecho, varias han tomado la delantera: **Ualá** adquirió un banco (Wilobank, rebautizado Uilo) en 2022 para obtener licencia; **Mercado Pago** inició trámites para conseguir licencia bancaria en Argentina; el gigante brasileño **Nubank**, que en Brasil ya es banco, buscó en 2023 comprar una entidad en Argentina (Brubank).

En México, Nubank obtuvo en 2022 licencia de institución de banca múltiple para poder captar depósitos. En otras

palabras, las fintech más exitosas se están “**convirtiendo en bancos**” porque la figura de PSP o de emisor de dinero electrónico les quedó chica y porque la regulación las empuja a ello.

¿Por qué las empuja? Porque los reguladores temen arbitrajes regulatorios. Imaginemos un banco tradicional que debe cumplir mil normas vs. una fintech grande que ofrece servicios similares sin tanto requisito: existe un riesgo de competencia desigual y también de acumulación de riesgos ocultos fuera del perímetro regulatorio. Así, los bancos centrales y superintendencias están constantemente actualizando normas para alcanzar a las fintech.

Es una carrera de gato y ratón: las fintech innovan (por ejemplo, ofrecen **rendimientos por saldo en cuenta** invirtiendo en fondos comunes, como hicieron Mercado Pago y Nubank en Brasil) y el regulador reacciona (limitando esos rendimientos o pidiendo más divulgación). Un caso concreto: en Argentina, Mercado Pago ofrecía rendimientos diarios por el dinero en cuenta de usuarios invirtiéndolo en un fondo money market; en 2023, el regulador le exigió recalibrar esa comunicación y luego, con la perspectiva de ser banco, esas prácticas estarán bajo supervisión más estricta.

En materia **tributaria**, los medios de pago digitales también han ido un paso adelante de las administraciones fiscales, y han generado áreas grises. Las transferencias *peer-to-peer*, por ejemplo, permiten movimientos de dinero entre personas sin pasar por

bancos tradicionales, lo cual desafía los esquemas de retención de impuestos.

En varios países, los físicos han debido crear mecanismos para gravar actividades dentro de plataformas digitales: **México** nuevamente fue pionero al implementar en junio de 2020 un régimen donde las plataformas retenían el IVA (16%)³⁰ y el impuesto sobre la renta a sus vendedores independientes. Desde entonces, cualquier venta en Mercado Libre México o Amazon México incluye IVA, y los vendedores pagan impuestos sobre sus ingresos con retenciones escalonadas. Esto formalizó miles de transacciones que antes podían estar en la informalidad fiscal.

Brasil, por su parte, ya en 2019 había dictado una norma tributaria (Instrucción Normativa RFB 1888) que obligaba a las exchanges de criptomonedas a reportar transacciones de sus clientes, un paso audaz que pocos países habían dado entonces. **Colombia** y **Argentina** están discutiendo marcos para criptoactivos –Colombia con proyectos de ley para exchanges desde 2021, Argentina con propuestas en el Congreso– pero aún sin ley específica, lo que crea incertidumbre sobre cómo se declaran o gravan las ganancias en crypto.

El tema de las **criptomonedas** merece mención especial en este contexto de “persecución legal”. Las crypto nacieron globales, descentralizadas, sin fronteras... y los reguladores nacionales corren detrás tratando de encajarlas en alguna categoría existente (*¿activo intangible? ¿valor financiero? ¿moneda extranjera?*).

La mayoría de los países iberoamericanos hoy trata las criptos como **activos intangibles**: por tanto, las ganancias se gravan como renta de capital y los saldos se incluyen en impuestos al patrimonio. Pero no deja de haber un vacío en protección al inversionista y estabilidad: si quiebra una plataforma cripto local, no hay seguro de depósitos que valga.

Algunos países como **España** han optado por exigir registro a proveedores de servicios cripto y aplicar normas de prevención de lavado; en nuestra región, Brasil también discute la implementación de un régimen de *sandbox* regulatorio para proyectos blockchain. Así, poco a poco, ese “lejano oeste” de las cripto empieza a ser abordado, aunque fragmentariamente.

Volviendo a las **billeteras virtuales y pagos móviles**, hay un dilema político-regulatorio de fondo: ¿cómo equilibrar la **inclusión financiera** y la **competencia** con la **seguridad financiera** y la estabilidad? Las fintech han traído competencia a sectores dominados por oligopolios bancarios, han bajado costos y democratizado servicios. Por ejemplo, gracias a fintechs de pago en países como Argentina o Perú, hoy personas sin cuenta bancaria pueden pagar servicios o comprar online usando efectivo convertido a digital en agencias. Esto es positivo para la economía digital. Pero a la vez, algunas fintech han crecido tanto que levantan sus propias preocupaciones de competencia (¿monopolios fintech en camino?) e inquietudes de estabilidad (¿qué pasa si quiebra una fintech grande con millones de usuarios no bancarizados?). Los reguladores se debaten entre fomentar la innovación y controlarla.

La **eternidad** de esta “persecución legal” se manifiesta en que nunca se termina: cada vez que parece que la normativa alcanzó al mercado, surge algo nuevo. Les comparto un caso reciente: el surgimiento de los pagos en tiempo real interbancarios como **Pix** en Brasil, un sistema impulsado por el Banco Central que descolocó tanto a bancos como a fintech privadas.

Pix fue lanzado en 2020 y rápidamente se volvió el método más popular de pago electrónico en Brasil, al punto de que hoy representa el 22% de los pagos online en Latinoamérica (y eso que sólo existe en Brasil por ahora).³¹ Su éxito es tal que América Latina en conjunto es la región de mayor crecimiento proyectado en pagos cuenta a cuenta (A2A), con un 29% CAGR 2022-2027.

Pues bien, ahora otros países quieren replicar Pix, y las fintech privadas aplauden la interoperabilidad pero se preocupan por cómo competir con un sistema gratuito del banco central. Este es un ejemplo de regulación (o innovación pública) que se puso adelante del mercado, una excepción notable en la tendencia general. Aun así, genera nuevas preguntas para el marco legal: ¿cómo garantizar la seguridad de Pix internacional? ¿Cómo prevenir fraudes masivos en sistemas instantáneos? Los legisladores tendrán que atender también eso.

Para visualizar la evolución actual de los pagos en la región, veamos la composición de métodos de pago online:

En 2024, los **pagos digitales** (transferencias A2A y billeteras electrónicas) ya constituyen el 46% del volumen

de comercio electrónico en Latinoamérica, mientras que las tarjetas de crédito –históricamente dominantes– han caído al 42% de participación (en 2019 eran el 56%). El efectivo en puntos de pago y otras modalidades tradicionales retroceden. Esto muestra cómo la adopción tecnológica avanza más rápido de lo que nuestros códigos comerciales pueden asimilar.³²

Ante este panorama, vuelvo a las voces expertas. **Eugenio Sánchez, Jefe de Oficina en Positiva Compañía de Seguros**, ha advertido sobre el riesgo de ciertas sobrerregulaciones propuestas en su país (eLíderes Podcast x25, 2024):



Una iniciativa legislativa buscaba restringir la información crediticia disponible, lo cual, según él, “acabaría con el crédito digital, el cual ha sido un motor de inclusión financiera” para poblaciones tradicionalmente excluidas.



**Eugenio
Sánchez**

En sus palabras resuena un principio clave: si regulamos mal o con miedo, podemos matar beneficios que la tecnología ya está trayendo en materia de acceso e inclusión. **Jacobo Cohen Imach** reflejó una preocupación similar en el contexto regional más amplio (eLíderes Podcast x25, 2025):



“Se prohíben cosas o se ponen límites cuando la gente comparte mucho más de lo que el regulador cree”, dice sobre ciertos intentos regulatorios desconectados de la realidad del consumidor digital. Y advierte: “Regular mal no sólo frena la innovación sino que expulsa talento y oportunidades. La tecnología no es como ensamblar autos. Si no lo hacés acá, lo hacen en otro lado. Pero se va todo el ecosistema”.



Jacobo
Cohen Imach

Esa frase me quedó grabada. En efecto, si asfixiamos a las fintech con normas concebidas para otra era, los emprendedores y capitales simplemente migrarán a jurisdicciones más amigables y nos dejarán atrás.

En esta eterna pugna entre innovación y regulación, soy optimista en que encontraremos gradualmente el equilibrio. Ya vemos aproximaciones más sofisticadas: *sandboxes* regulatorios en México, Colombia y Brasil, donde fintechs prueban modelos con supervisión flexible; mesas de innovación financiera en bancos centrales; regulación colaborativa. Hace 10 años, muchos banqueros tradicionales veían a las fintech como “tierra de nadie” que debía prohibirse o encorsetarse.

Hoy, en cambio, entienden que la clave es integrar innovación con garantías mínimas. **La persecución legal continuará**, sin duda, porque la tecnología de pagos

seguirá sorprendiéndonos (pienso en DeFi, en monedas digitales de bancos centrales, en pagos invisibles IoT). Pero confío en que esa persecución será más estratégica y menos reactiva. En última instancia, todos (industria, reguladores, usuarios) queremos lo mismo: sistemas de pago que sean seguros, eficientes e inclusivos. Aprenderemos de los tropiezos y, ojalá, la próxima generación vea menos “gato y ratón” y más convivencia armoniosa entre innovación financiera y marco legal.



Desafíos locales vs. regulación global

El comercio digital borra fronteras por naturaleza, mientras que las regulaciones siguen siendo en su mayoría nacionales. Este descompás produce un *déjà vu* constante: legislaciones locales intentando ponerle vallas a modelos de negocio globales, lo que genera fricciones e inconsistencias. Lo vivimos ya en la época de las “punto-com” y se recrudece ahora con las Big Tech y las plataformas transnacionales de todo tipo. En nuestra región, cada país ha reaccionado por su lado –impuestos digitales aquí, restricciones allá–, muchas veces sin contemplar que el servicio o plataforma opera desde fuera de su jurisdicción o en múltiples mercados a la vez.

Un frente claro de conflicto son los **impuestos digitales**. Con el auge de servicios como Netflix, Spotify, Amazon Prime, Uber, Airbnb, etc., los fiscos nacionales vieron una base imponible escapándose de sus manos: consumo local de servicios extranjeros tradicionalmente no gravados. La respuesta fue fragmentada. **Argentina** avanzó temprano: desde 2018 aplicó el IVA del 21% a los servicios digitales de no residentes (cobrados vía tarjetas) y luego sumó el llamado *impuesto PAIS* y percepciones adicionales, que llegaron a encarecer estos servicios cerca de un 74% sobre su precio original.

Para 2023, un argentino pagando Netflix o Spotify estaba abonando casi el doble por la cascada de impuestos. Recién a fines de 2024, el gobierno anunció la reducción

del impuesto PAIS para plataformas de streaming del 8% al 0% –lo cual implicó una caída inmediata de aproximadamente un 8% en las tarifas finales de esos servicios– en un intento de aliviar el bolsillo y equiparar condiciones con otros países. Aun así, durante años se dio la paradoja de que Netflix costaba mucho más en Argentina que en Chile o Brasil por esa carga fiscal extra, lo que empujó a algunos usuarios a *trampearlas* (por ejemplo, pagando con tarjetas emitidas en el exterior).

México, por su parte, implementó en 2020 un modelo bastante ordenado de impuesto digital: exigió a los proveedores extranjeros de servicios (desde streaming hasta apps de transporte) registrarse ante el SAT y cobrar el 16% de IVA a sus usuarios mexicanos. Adicionalmente, impuso obligaciones a plataformas de intermediación (Uber, Mercado Libre, Airbnb) para retener impuestos a sus conductores/vendedores/anfitriones independientes. Esto fue notable porque implicó coordinación con las empresas globales, muchas de las cuales inicialmente recelaban actuar como recaudadoras de impuestos para un país. Finalmente, todas cedieron: hoy es normal que Netflix te cobre IVA en México, que Uber retenga impuestos a sus choferes y los entere al fisco mexicano, etc.

Colombia y Chile siguieron un camino similar con el IVA digital en 2019-2020 (del 19% en ambos casos). Chile incluso implementó un mecanismo sencillo: las tarjetas de crédito automáticamente cargan el IVA a los pagos hacia proveedores designados como digitales extranjeros, lo que simplifica la recaudación. El resultado es que, al menos en materia de IVA, la región tendió a homogeneizar

el trato: consumir un servicio digital extranjero se grava como si fuera un servicio local.

No obstante, surgen fricciones interesantes. **Plataformas globales vs. normas locales:** un clásico ejemplo fue cuando algunos países exigieron que servicios como Netflix incluyeran contenido nacional (cuotas de pantalla) o invirtieran en producción local. Brasil y México discutieron sobre imponer cuotas de contenido nacional en streaming, inspirados en la normativa europea, lo que generó cabildeo intenso de las plataformas.

En general, esas exigencias no prosperaron de forma rígida, pero reflejan el choque de un modelo global (un único catálogo para todo el mundo) contra políticas culturales locales. Otro caso: leyes locales de protección al consumidor que chocan con términos de servicio globales. En España, Amazon fue llevada a tribunales por cláusulas que violaban la ley local; en Latinoamérica, Amazon, Alibaba y otros han debido adaptarse a leyes nacionales de devoluciones y garantías que varían país por país.

Un tema candente es el de la **tributación de las grandes multinacionales digitales** más allá del IVA. Aquí entramos en la compleja esfera de la *tributación corporativa internacional*: empresas como Google, Facebook (Meta), Amazon o Airbnb generaban ingresos en nuestros países sin presencia legal fuerte, y pagaban impuestos mínimos al canalizar ganancias a través de jurisdicciones de baja tributación. La reacción local tomó a veces formas polémicas.

España implementó su *tasa Google* (impuesto a ciertos ingresos digitales) en 2021; en Latinoamérica hubo proyectos similares en Chile y Uruguay, aunque pocos se materializaron, a la espera de una solución global coordinada vía OCDE (el famoso Pilar 1 para distribuir derechos de imposición sobre multinacionales digitales). Mientras tanto, algunos optaron por mecanismos ingeniosos: aplicar percepciones de impuesto a las ganancias sobre los pagos al exterior hechos a estas empresas, presumiendo que parte es ganancia. A nivel de retención en la fuente se trató de gravarlas indirectamente. Esto, por supuesto, complejiza la operatoria y a veces encarece al usuario final sin garantía de una justicia tributaria real.

Otro frente de choque es el de las **normas aduaneras y de comercio local vs. operaciones globales**. El comercio electrónico transfronterizo (que un consumidor compre en AliExpress, por ejemplo, y reciba vía correo) explotó en los últimos años. Las regulaciones nacionales, sin embargo, no estaban preparadas: procedimientos aduaneros pensados para importaciones comerciales tradicionales, con montañas de papeleo, de pronto debían lidiar con millones de pequeños paquetes para personas físicas. La respuesta también varió.

Colombia estableció en 2019 un umbral de USD 200 debajo del cual los envíos personales están exentos de aranceles (similar al *de minimis* de EE.UU.), para facilitar las compras en el exterior de bajo valor. **Argentina** fue en sentido contrario por mucho tiempo: mantuvo un importe *de minimis* bajísimo (USD 50 anual por persona,

luego algo más flexible) y exigió trámites engorrosos, lo que enfrió las compras transfronterizas. Apenas en 2022-2023 se empezó a simplificar un poco el *courier* para envíos pequeños.

Esta fragmentación normativa dificulta el ecommerce regional: idealmente, podríamos avanzar hacia acuerdos en Mercosur, Alianza del Pacífico o a nivel CELAC para unificar criterios; por ejemplo, establecer un umbral **de minimis regional elevado**, que permita envíos sin tanto papeleo. No es sencillo políticamente (cada aduana cuida su terreno), pero ese sueño de armonización facilitaría muchísimo la vida a pymes y consumidores digitales.

También está el **conflicto fiscal-local** cuando operaciones digitales globales no tienen establecimiento en el país. Un caso reciente: provincias argentinas intentando cobrar Ingresos Brutos (impuesto local) a Netflix y similares, aun sin sede física allí, mediante convenios con tarjetas. O municipios que pretenden tasar a Uber aunque la empresa no esté domiciliada localmente, responsabilizando a los conductores. Estas creatividades legales generan litigios sobre si hay o no “nexo” suficiente para gravar. De nuevo, un déjà vu: replican disputas de hace décadas sobre mail orders o servicios transfronterizos, ahora con plataformas.

En cuanto a **fricciones específicas con empresas**: Mercado Libre ha tenido que negociar con gobiernos sobre cómo manejar la importación directa de mercancías vendidas en su plataforma (*Mercado Libre Global Shipping*), para no chocar con normas de importadores oficiales. Amazon fue cuestionada en Brasil por prácticas

de logística y tratamiento fiscal de vendedores terceros extranjeros. Spotify y Netflix han debido cumplir con cuotas de música local en algunos mercados (Brasil tiene cuotas de música brasileña en radios, que se extienden a radios online). Cada país empuja sus intereses, y las empresas globales tratan de estandarizar operaciones, así que hay roces inevitables.

Un desarrollo interesante es que algunos países están mirando experiencias extranjeras para diseñar una regulación **con alcance global**. **Chile** y **Brasil**, por ejemplo, han hablado de crear regulaciones para “plataformas digitales dominantes” inspiradas en la **Digital Markets Act (DMA)** de la UE.³³

La DMA europea impone obligaciones ex ante a los grandes “guardianes” (gatekeepers) como Google, Meta, Amazon, para asegurar equidad (ej., prohibir que favorezcan sus propios productos en el marketplace en detrimento de terceros). En Latam aún no hay nada equivalente, pero el solo debate indica que nuestros reguladores ya piensan más allá de sus fronteras: entienden que si Europa logra doblegar ciertas prácticas de Big Tech, Latinoamérica podría beneficiarse o seguir ese camino para proteger su mercado. Ahora bien, aplicar localmente algo así tendría escollos: ¿de qué serviría que un país declare dominante a X empresa y le dicte obligaciones, si la empresa puede argumentar que sólo cumple en sedes principales? Quizá podría hacerse mediante requisitos para operar en el territorio (tal como se hace con telecomunicaciones). Es un tema a seguir de cerca.

Al final del día, el **conflicto local vs. global** en regulación digital nos enseña humildad: ningún país por sí solo puede abarcar la totalidad de un fenómeno transnacional. La cooperación internacional es clave. Celebré cuando, en 2021, más de 130 países acordaron en la OCDE el esquema global de impuesto mínimo corporativo, que afectará a las Big Tech entre otras multinacionales; eso promete reducir la elusión fiscal global. O cuando varias naciones se unieron en acciones antitrust coordinadas (como ciertas investigaciones conjuntas de EE.UU. y UE sobre empresas tech). Latinoamérica necesita alzar su voz en esos foros para asegurarse de no quedar como mera espectadora.

Mientras tanto, en casa, debemos evitar el proteccionismo miope o las soluciones unilaterales que sólo ahuyentan la innovación. He visto de cerca cómo emprendedores digitales sufrían cuando de pronto un gobierno local bloqueaba Uber o Binance sin un plan alternativo, o imponía impuestos desproporcionados que hacían inviable un servicio. Esa **inseguridad jurídica** global-local termina perjudicando al usuario local, que se queda sin el servicio o lo paga más caro.

Mi propuesta –y la de muchos colegas– es **buscar puntos medios**: por un lado, exigir que las plataformas globales contribuyan y respeten las reglas locales (paguen impuestos, cumplan normas de defensa del consumidor, compitan lealmente); por otro, simplificar las normativas para admitir la naturaleza transfronteriza (facilitar registro de empresas extranjeras para que operen formalmente, homologar estándares con otros países, aprovechar la

economía digital sin tratar de *encajonarla* en regulaciones pensadas para lo físico). Es un equilibrio difícil, sí, pero necesario.

Imaginemos un futuro cercano: un emprendedor chileno vende vía marketplaces a toda la región; paga IVA en cada destino con mecanismos automatizados, despacha con un régimen aduanero simplificado de minimis regional, tributa ganancias donde corresponda según un acuerdo multilateral, y los consumidores de distintos países reciben sus productos rápidamente sin trabas burocráticas. Esa visión requerirá **armonización regional** en varios frentes. Algunos organismos como la CAF y la GSMA han abogado por políticas integrales para la economía digital latinoamericana, conscientes de que fragmentados avanzaremos más lento.

En resumen, el choque entre lo local y lo global es otro déjà vu persistente. Así como en los 2000 las empresas .com globales desafiaron regulaciones nacionales (pienso en casos como Napster vs. leyes de copyright nacionales, o eBay desembarcando sin oficina local), hoy vivimos algo similar con plataformas de todo tipo. La ventaja es que ahora tenemos más experiencia: ya no vemos lo global con ingenuidad; sabemos que hay que negociar términos. Y también las empresas globales aprendieron a dialogar localmente (muchas tienen equipos de asuntos públicos en cada país).

Creo firmemente que el camino no es erigir muros digitales sino **tender puentes legales**: actualizar nuestras normas para ser compatibles con la economía digital

internacional, mientras defendemos nuestros intereses (recaudación, cultura, consumidores). Si logramos eso, quizás este déjà vu termine siendo una experiencia de aprendizaje y no un eterno retorno al desencuentro.



Desafíos constantes: Opacidad, burocracia e inseguridad jurídica

Después de 25 años de desarrollo del comercio electrónico en Iberoamérica, uno podría suponer que las barreras iniciales han desaparecido. En parte es cierto: hoy es mucho más fácil montar un negocio en línea que en 2000. Pero muchas **barreras burocráticas** e **incertidumbres legales** persisten, lo que provoca esa incómoda sensación de *“hemos estado aquí antes”*. Son desafíos constantes que atraviesan toda la era digital: trámites engorrosos, regulación ambigua, falta de diálogo entre innovadores y autoridades. Como emprendedor y ejecutivo, me he topado con ellos una y otra vez.

Un primer escollo es la **burocracia para constituir y operar empresas digitales**. Pese a avances como la creación de figuras societarias simplificadas (la SAS en Argentina, Colombia y otros; la SpA en Chile), todavía iniciar un emprendimiento tecnológico puede implicar meses de trámites en ciertos países. El *Índice de Burocracia* de 2025³⁴ reveló que fundar una empresa mediana en Latinoamérica lleva en promedio más de 40 días, y puede demandar hasta once procedimientos administrativos, dependiendo del país. Si bien esto ha mejorado respecto a décadas pasadas, aún estamos por detrás de regiones más ágiles.

Muchos emprendedores optan por constituir su holding en **Delaware o en las Islas Caimán** para atraer inversión,

dado que los fondos internacionales a menudo lo exigen por seguridad jurídica. Esta práctica –el famoso *Delaware tostada* o *Cayman sandwich*, donde la startup latina tiene doble estructura local y offshore– refleja que nuestros sistemas legales domésticos no dan suficiente confianza o flexibilidad para escalamiento global.

Es decir, las **reglas locales excesivas o confusas** empujan a los fundadores a “empaquetar” sus emprendimientos fuera. Una y otra vez, escucho a inversores decir: “Nos encanta tu startup, pero para invertir, debes estar constituido bajo ley de Delaware”. Es frustrante, porque implica tiempo y costos, pero lo hacen para esquivar las inseguridades de nuestras jurisdicciones.

¿Qué inseguridades? Por ejemplo, la **ambigüedad normativa** en áreas clave para negocios digitales. Un caso crítico es la falta de un marco claro para **stock options** (opciones sobre acciones para empleados) en muchos países. Las startups tecnológicas dependen de atraer talento ofreciendo participación societaria futura, pero nuestras leyes laborales y societarias a veces no contemplan bien esa figura. En Colombia recién se discuten ajustes; en Argentina se hizo una reforma parcial en 2017 pero aún con vacíos. Esto limita la capacidad de las empresas locales de retener talento, comparado con Silicon Valley, donde el *employee stock option pool* es estándar.

Hasta hace pocos años, en Argentina no estaba claro si una tienda online debía o no ofrecer el mismo precio que en tienda física (por leyes de lealtad comercial pensadas

para catálogos en papel). Muchos comercios dudaban sobre sus estrategias omnicanal por temor a multas de la Secretaría de Comercio. Eventualmente se aclaró vía interpretaciones, pero mientras tanto, reinó la inseguridad. Ejemplo distinto: en México, los modelos de economía colaborativa (tipo Uber, Airbnb) pasaron años en zona gris, con choferes y hosts sin saber si su actividad era legal; la regulación llegó estado por estado, lo que creó un mosaico engorroso. Todo esto hace que emprender en digital aún implique navegar **aguas turbulentas legales**, a diferencia de entornos más estables.

Otro desafío constante es la **falta de instancias de consulta y diálogo** entre el ecosistema digital y los reguladores. En industrias tradicionales existen a menudo entidades regulatorias especializadas (una superintendencia bancaria, un ente de transporte) con las que las empresas dialogan. En cambio, la industria digital es tan transversal que carece de “su” regulador dedicado. Eso ha comenzado a cambiar: varios países crearon recientemente secretarías o unidades de economía digital, o comités público-privados para la transformación digital.

Pero en mis primeros 15-20 años de carrera, era difícil saber ante quién plantear un problema regulatorio del ecommerce. ¿Ante el ministerio de economía? ¿El de comercio? ¿Las telecomunicaciones? ¿Defensa del consumidor? Esa fragmentación persistente dificulta que el sector digital haga oír su voz antes de que salgan leyes. Recién ahora vemos un mayor involucramiento: cámaras de fintech, de economía digital, etc.,

participando en congresos y consultorios. Aun así, muchas normas se siguen dictando **sin suficiente consulta previa** y repiten errores.

¿Ejemplos? La “Ley de Góndolas” en Argentina (pensada para supermercados) tuvo artículos que afectaban a los marketplaces online sin que estos fueran consultados, lo que generó confusión sobre si aplicaban o no. En Colombia, la Ley de Protección de Datos (2012) impuso obligaciones a responsables de bases de datos, que agarraron desprevenidas a cientos de startups que ni supieron de la ley hasta tener el requerimiento encima. Estas situaciones me reafirman la importancia de institucionalizar el diálogo.

Cuando **Jacobo Cohen Imach** rememoró la implementación de la factura electrónica en Argentina, destacó que se hizo bien porque *“el regulador nos invitó, nos dijo ‘vengan, díganme cómo esto se puede implementar’ y juntos lo logramos”*. Esa cocreación temprana evitó un choque y permitió que Argentina fuera pionera en sistemas como la firma digital (aunque Jacobo reconoce que *“a nivel de implementación, fue un desastre”*, la intención colaborativa estuvo). Necesitamos más de ese espíritu de **escucha mutua**.

Por último, un desafío permanente es la **cultura jurídica y burocrática tradicional**, que a veces mira con recelo las novedades digitales. Aunque suene anecdótico, todavía en 2025 me encuentro con trámites que requieren documentación en papel, firmas manuales, sello de escribano, incluso para empresas 100% en línea. La

pandemia de 2020 forzó la digitalización administrativa en muchos ámbitos, es cierto, pero no erradicó cierta mentalidad formalista. Constituir una empresa digital en algunos países sigue implicando procesos presenciales y tiempos prolongados que no se condicen con la rapidez del negocio digital.

Además, la capacitación de funcionarios en temas tech es dispar: unos pocos, muy avanzados, pero muchos con poca comprensión de modelos como *SaaS*, *big data*, *IA*, *blockchain*. Esto redundaba en interpretaciones erráticas de la norma. Recuerdo el caso de una startup de cloud en Perú que me contaba cómo un inspector tributario pretendía aplicarle impuesto de alojamiento hotelero porque “alquilaba espacio en la nube”; obviamente un absurdo, corregido luego, pero ilustra la brecha de entendimiento.

A pesar de todo, quiero señalar que no todo es inmovilidad. En estos años también he visto mejoras sostenidas: leyes de firma digital y comercio electrónico que dan validez legal a contratos online (pioneras: Argentina en 2001, Colombia en 1999, actualizadas en muchos países), marcos de protección al consumidor en comercio electrónico (por ejemplo, normativas específicas en Perú y Colombia que obligaban a cierto formato de información en sitios web), simplificación de registros de nombre de dominio, etc.

Y destaco iniciativas gubernamentales proactivas: programas *Startup Chile* o *Colombia Crea Digital*, que buscan apoyar emprendimientos y hasta revisar trabas regulatorias. En **Colombia**, la Ley de Emprendimiento de

2020 introdujo cláusulas para facilitar trámites a nuevos negocios y extendió beneficios tributarios. En **Brasil**, se aprobó en 2021 el *Marco Legal das Startups*, que, entre otras cosas, estableció un ambiente regulatorio experimental (*sandbox*) y simplificó contrataciones públicas con startups. Son pasos en la dirección correcta, señal de que la temática está en la agenda.

Sin embargo, la sensación general entre mis colegas emprendedores es que persisten la **opacidad, la excesiva burocracia y la inseguridad jurídica** como sombras en el ecosistema. Para que la economía digital alcance su pleno potencial, debemos despejar esas sombras. ¿Cómo? Simplificando y digitalizando trámites (¿por qué no un *one-stop shop* regional para registrar startups?), armonizando regulaciones internamente y con vecinos, y creando espacios de interlocución permanente entre reguladores y la industria.

Un emprendedor debería poder preguntar sin temor: “¿Puedo lanzar este producto digital? ¿Qué regulación aplica?”, y obtener respuesta clara. Hoy muchos optan por el camino de “lanzar y ver”, rezando que nada caiga fuera de la ley; otros, más conservadores, directamente no lanzan ciertas innovaciones por la niebla legal.

Quiero cerrar con una nota positiva, recordando palabras de Jacobo Cohen Imach que me inspiran. Él afirma que la mejor fórmula es la **transparencia y la construcción de confianza**, más que la sobrerregulación. “Voy a honrar la confianza de que me dejes tus datos. Eso es lo que tenemos que comunicar y garantizar”, dice sobre la relación

usuario-plataforma. Esa filosofía puede extenderse a todos los aspectos: honrar la confianza del emprendedor brindándole un entorno claro, honrar la confianza del regulador cumpliendo el espíritu y letra de las normas, y honrar la del consumidor siendo honestos. Si todos los actores actuamos con buena fe y foco en resolver problemas –en vez de entramparnos en formalismos–, podremos sortear estos desafíos constantes.

Llevo más de dos décadas en este viaje digital y, a pesar de los *déjà vu* regulatorios, soy testigo del enorme progreso. Donde antes había desierto normativo hoy hay cimientos sobre los que construir mejores reglas. Los retos de opacidad, burocracia e inseguridad no desaparecerán mágicamente, pero estoy convencido de que, trabajando juntos, podemos transformarlos. En vez de un *déjà vu* estancado, que sean lecciones aprendidas. En lugar de navegar a ciegas por aguas legales inciertas, que tracemos mapas claros para el futuro. La **economía digital iberoamericana** late con fuerza y talento; es hora de que sus marcos normativos latan al mismo ritmo, acompañando sin ahogar. Sólo así dejaremos de repetir la historia y empezaremos verdaderamente a escribir capítulos nuevos, con final feliz, en la génesis de este futuro digital.



GÉNESIS

DE UN FUTURO DIGITAL





Focos de tensión legal transversales al ecosistema digital

En la evolución del ecosistema digital iberoamericano, han emergido **focos de tensión legal transversales** que recuerdan debates ya vividos en el pasado; de ahí la noción de *déjà vu* en las regulaciones. Tal como se ha narrado en otros libros de la colección *Génesis de un Futuro Digital*, los inicios del comercio electrónico se desarrollaron en un entorno normativo incipiente. Años después, muchas de aquellas cuestiones vuelven al centro de la escena regulatoria, ahora amplificadas por la escala y velocidad de la economía digital actual.

A continuación, profundizaremos en cinco de estos focos de tensión: **protección de datos personales, propiedad intelectual digital, fiscalidad digital, derechos del consumidor digital, y publicidad en redes sociales**, analizando su situación en Latinoamérica hacia 2024–2025.

Protección de datos personales y privacidad

La protección de los datos personales se ha convertido en un pilar fundamental para el desarrollo sostenible del ecosistema digital. En los últimos años, Latinoamérica vivió una aceleración normativa influenciada en gran medida por el Reglamento General de Protección de Datos europeo (GDPR, por sus siglas en inglés). La “ola GDPR” se sintió con fuerza en la región: *en 2024, los países latinoamericanos intensificaron la actualización de sus leyes de datos siguiendo la tendencia internacional marcada por Europa.*³⁵ Esto ha resultado en un mosaico normativo donde conviven marcos modernos inspirados en GDPR con legislaciones más rezagadas, lo que creó desafíos de cumplimiento para empresas que operan en múltiples jurisdicciones.

Influencia del GDPR en América Latina. Varios países han alineado sus normativas con estándares europeos. Por ejemplo, **Brasil** promulgó su Lei Geral de Proteção de Dados (LGPD) en 2018 (vigente desde 2020), claramente modelada a partir del GDPR. En 2024, introdujo mejoras a la LGPD: aprobó cláusulas contractuales tipo para transferencias internacionales, otorgó a los titulares más control sobre sus datos y endureció sanciones por incumplimiento (Crowell, 2025).

Chile, que desde 1999 contaba con una ley de protección de datos desactualizada, aprobó en agosto de 2024 un proyecto de ley integral que moderniza su marco

y lo *alinea con el GDPR*, incluyendo principios como minimización, derechos ARCO robustos y reconocimiento expreso de la anonimización (Crowell, 2025).

Colombia también emprendió en 2023–2024 la reforma de su Ley 1581/2012 para acercarla a estándares internacionales, incorporando nuevas bases legales de tratamiento, requisitos de consentimiento para menores, plazos de notificación de brechas y hasta límites al *profiling* y decisiones automatizadas. Estos esfuerzos muestran cómo el GDPR sirvió de **referente** para elevar la vara de la privacidad en la región (Crowell, 2025).

Brechas normativas locales. A pesar de los avances, persisten importantes **brechas entre países**. **Argentina** fue pionera con su Ley 25.326 de 2000 (incluso obteniendo la adecuación de la UE en 2003), pero durante muchos años no actualizó su ley a la par del GDPR. Recién en junio de 2024 dio un paso significativo con la resolución 126/2024 de la Agencia de Acceso a la Información Pública, que estableció una nueva clasificación de sanciones para infracciones a la ley de datos personales, y unificó además el registro de infractores (Crowell, 2025). Sin embargo, Argentina aún tiene pendiente la sanción de una ley nueva (un anteproyecto inspirado en el GDPR estuvo en debate en 2022–2023).

Bolivia, por su parte, todavía *carece de una ley integral de protección de datos* –existen proyectos en el Congreso, pero nada definitivo–. **Paraguay** tampoco contaba con ley general (tiene normas sectoriales, por ejemplo, en información crediticia); un proyecto de ley de datos

personales lleva años sin aprobarse. Incluso en países con leyes modernas, la aplicación práctica enfrenta retos: el cumplimiento efectivo requiere autoridades de control sólidas y cultura corporativa de privacidad.

En palabras de [Jacobo Cohen Imach](#) (eLíderes Podcast x25, 2025):



“Por años hicimos negocios en países cuya regulación no estaba pensada para internet ni para el ecommerce; tuvimos que desarrollar ‘cuero duro’ para gestionar esos riesgos”.



Jacobo
Cohen Imach

La reflexión del vicepresidente legal de Mercado Libre ilustra cómo históricamente las empresas digitales operaron en vacíos legales que recién ahora comienzan a llenarse. Hoy nos encontramos con un **paisaje normativo heterogéneo**: algunas jurisdicciones con esquemas tipo GDPR (Brasil, Chile, Uruguay, etc.), otras con leyes más antiguas o parciales (México con su Ley Federal de 2010; Perú con Ley 29.733 de 2011; Colombia con prereforma), y otras recién elaborando marcos (Bolivia, Paraguay). Esta disparidad genera desafíos para la expansión regional de servicios digitales, que deben navegar por distintas definiciones de consentimiento, responsabilidades del encargado, obligaciones de notificación de brechas, etc.

Sanciones y desafíos regulatorios recientes. A medida que maduran las normas, aumentan las acciones de

control y las sanciones, lo que evidencia tensiones entre empresas, usuarios y reguladores. En **Brasil**, la Autoridad Nacional de Protección de Datos (ANPD) comenzó a ejercer su poder sancionador tras la entrada en vigor plena de la LGPD en 2021, aplicando multas importantes a empresas locales y multinacionales por fallas de seguridad o uso ilegítimo de datos.

Europa ha impuesto más de €5.600 millones en multas acumuladas bajo GDPR hasta fines de 2024,³⁶ presión que se siente globalmente. Si bien en Latinoamérica las multas aún no alcanzan esas magnitudes, la tendencia es a incrementarlas.

Argentina, con su nueva escala sancionatoria de 2024, unificó criterios para penalizar infracciones tanto a datos personales como a “No llame” (Crowell, 2025). **México** ha tenido casos sonados de vulneraciones (p.ej., fugas de bases de datos) que enfrentaron a su INAI con empresas, aunque las multas están topeadas por ley y su agencia atraviesa desafíos institucionales.

Un desafío común es la **aplicación extraterritorial**: muchas empresas globales de tecnología operan servicios en la región sin presencia legal local, lo que dificulta a las autoridades latinas hacer valer la ley más allá de sus fronteras. También surgen tensiones alrededor de tecnologías emergentes: por ejemplo, la reciente ola de sistemas de **inteligencia artificial generativa** plantea preguntas sobre recolección masiva de datos para entrenar modelos, posible sesgo o decisiones automatizadas. Colombia explícitamente incorporó

consideraciones sobre **IA** en la reforma de su ley de datos (Crowell, 2025), anticipando la necesidad de regular algoritmos con impacto en las personas.

Otra fuente de debate es la **seguridad pública vs. privacidad**: en Paraguay se aprobó en 2024 una ley que obliga a recolectar datos biométricos (incluyendo reconocimiento facial) de todos los asistentes a eventos deportivos, con la finalidad de prevenir violencia en los estadios (Crowell, 2025). Si bien busca un fin legítimo, los críticos señalan que esa recolección masiva indiscriminada vulnera la privacidad de miles de ciudadanos inocentes. Este tipo de casos evidencia la delgada línea que los reguladores deben caminar para equilibrar derechos fundamentales en conflicto.

En este contexto dinámico, *las voces expertas subrayan la importancia de la autorregulación y la cooperación público-privada*. [Yerka Yukich](#), directora de eCommerce de la Cámara de Comercio de Santiago, destaca que la protección de los datos personales no es sólo una carga legal sino un factor de confianza del consumidor.³⁷



“Una adecuada gestión de datos “fortalece la confianza, lo que es fundamental para seguir superando expectativas” en el comercio digital.



Yerka
Yukich

Por su parte, [Ludovino Lopes](#) (elÍderes Podcast x25, 2025) sostiene que las leyes deben adaptarse al ritmo de la innovación, pero sin sofocar el desarrollo de nuevos negocios. Lopes aboga por *criterios unificados en la región*, inspirados en marcos globales como GDPR, pero tomando en cuenta las realidades locales; además, enfatiza la educación y compliance corporativo como claves para cerrar la brecha entre la letra de la ley y su cumplimiento efectivo.

En suma, la protección de datos personales en Latinoamérica avanza con paso firme pero dispar: la influencia europea es innegable, las brechas entre jurisdicciones aún generan incertidumbre, y los casos recientes ponen a prueba la capacidad de enforcement de nuestras autoridades. El reto hacia el futuro próximo es lograr **armonía normativa** (idealmente mediante convergencia a estándares altos), sin descuidar la innovación y competitividad digital de la región. La privacidad, antes vista por muchos como un obstáculo burocrático, hoy se entiende como **condición habilitante de la economía digital** basada en la confianza.



Legislación de protección de datos en algunos países de Latinoamérica

País	Ley de protección de datos (año)	¿Enfoque GDPR?
Argentina	Ley 25.326 de 2000 (Adecuación UE 2003). Reforma pendiente al 2024.	Parcial (ley vigente inspirada en directiva 95/46/CE; proyecto nuevo al estilo GDPR en trámite).
Brasil	Lei Geral de Proteção de Dados – LGPD (2018, vigente 2020). Enmiendas 2023–24.	Sí (amplio alineamiento con GDPR, incluyendo bases legales, derechos titulares, DPO, sanciones).
Chile	Ley 19.628 de 1999 (obsoleta). Nuevo proyecto aprobado en 2024 (ley 21.459, en revisión constitucional).	Sí (nuevo marco 2024 equiparable a GDPR: autoridad independiente, deber de consentimiento expreso, etc.).
Colombia	Ley 1581 de 2012 (en reforma desde 2023). Decretos reglamentarios vigentes.	Parcial (ley actual inspirada en estándares OCDE; reforma busca alineación plena con GDPR).
México	Ley Federal de Protección de Datos Personales en Posesión de Particulares – LFPDPPP (2010).	Parcial (basada en principios similares a 95/46/CE; sin algunos derechos GDPR como portabilidad).
Uruguay	Ley 18.331 de 2008 (modif. 2010). Adecuación UE reconocida en 2012.	Parcial (nivel adecuado según UE; aún no incorpora todas las novedades de GDPR 2018).
Bolivia	Sin ley general (proyectos en debate al 2025).	N/A
Paraguay	Sin ley general (proyecto de Ley de PDP pendiente). Ley sectorial de información crediticia (2024).	N/A

Fuente: eContentLAB

Fuente: Adaptado de [Crowell \(2025\)](#) y revisión de legislación nacional.

Propiedad intelectual en el entorno digital

La economía digital ha ampliado exponencialmente las oportunidades de creación y distribución de contenidos, pero también ha exacerbado problemas clásicos de **propiedad intelectual (PI)** bajo nuevas formas. Temas como la venta de falsificaciones en marketplaces, la piratería de contenido en redes sociales y las políticas de *takedown* (retiro de contenidos ilegales) han cobrado relevancia transversal en la región. Estos desafíos no son enteramente nuevos –ya en los albores del comercio electrónico se debatía la responsabilidad de plataformas tipo eBay en la venta de bienes falsificados–, pero hoy el volumen y velocidad de las transacciones digitales plantean un escenario de **“déjà vu” intensificado**.

Falsificaciones y marketplaces. La venta de productos falsificados (*counterfeits*) en plataformas de ecommerce es quizás la arista más crítica de PI en Latam. Mercado Libre, Amazon, AliExpress y otros marketplaces se ven inundados de listados de artículos que infringen marcas registradas (textiles con logos apócrifos, electrónica de imitación, etc.), y desafían tanto a dueños de marcas como a consumidores.

Según un informe del FMI, *las pérdidas globales por fraude en ecommerce –incluyendo la venta de productos falsos– superaron los 48 mil millones de dólares en 2023, y más del 65% provino de transacciones transfronterizas.*³⁸ Latinoamérica aporta su cuota a

este problema: la región es un mercado atractivo para falsificadores por la alta demanda de ciertos bienes de consumo y, hasta hace poco, por marcos regulatorios débiles en fiscalización online.

Las plataformas líderes han respondido reforzando sus sistemas de detección y políticas internas. Un ejemplo contundente es **Mercado Libre** –el gigante regional del ecommerce–, que en su informe de transparencia del 2º trimestre de 2023, reveló haber moderado *5,4 millones de publicaciones* que violaban sus términos (el 0,84% del total de listados), de las cuales la **principal causa** de remoción fueron *productos falsificados*.³⁹

En México, Argentina, Brasil y Uruguay, las publicaciones de artículos apócrifos ocuparon el primer lugar entre las infracciones en la plataforma. Además, *el 97% de las bajas de listados fue detectado proactivamente por los sistemas y equipos de Mercado Libre*; sólo un 3% provino de denuncias de usuarios o autoridades. Estas cifras reflejan una inversión creciente en **tecnología antifalsificación**: mediante algoritmos de inteligencia artificial entrenados para identificar listados sospechosos, Mercado Libre y otros actores logran bajar la gran mayoría de las ofertas ilícitas antes siquiera de una denuncia.⁴⁰

Jacobo Cohen Imach, quien lidera el equipo legal de Mercado Libre, ha señalado que la compañía tiene “*tolerancia cero*” con la infracción y ha desarrollado herramientas como su **Programa de Protección de Marca (Brand Protection Program)**, para colaborar con los titulares de PI.⁴¹ Ese programa unificado permite a las

marcas denunciar productos en cualquiera de los 18 países donde operan, a través de un sistema único, con lo que estandarizan el proceso pese a diferencias legales locales. La estandarización ha sido clave porque –como destaca Cohen Imach– las leyes de la región carecían hasta hace poco de procedimientos claros *notice-and-takedown*, lo que forzaba a las plataformas a autorregularse y ofrecer una experiencia uniforme a los denunciantes.

La estrategia combinada de **KYC estricto de vendedores** (Mercado Libre bloqueó más de 3 millones de cuentas sospechosas al 2021 e impidió su registro), **detección automatizada** (IA filtrando más del 99% de listados fraudulentos)⁴² y **sanciones escalonadas** a infractores reincidentes está rindiendo frutos: por ejemplo, Amazon reportó en 2023 que gracias a medidas similares, redujo en un 35% las notificaciones de infracción de PI recibidas.

No obstante, el problema dista de estar resuelto: organizaciones internacionales como la OCDE y la EUIPO estiman que el comercio de falsificaciones representa todavía cerca del 2,5% del comercio mundial, y en sectores como indumentaria o juguetes, una porción significativa de lo vendido online en Latam podría ser falsificado.

La **presión regulatoria** va en aumento: EE.UU. incluye a ciertos marketplaces en su lista de “*Notorious markets*” si se percibe laxitud contra la piratería; la Unión Europea, con su nueva **Digital Services Act**, exigirá a grandes marketplaces medidas proactivas de control de vendedores y origen de mercancías, estándar que podría eventualmente influir en nuestra región.

En suma, la venta de falsificaciones en línea requiere un *enfoque multiactor*: las plataformas implementando tecnología y colaborando con dueños de marcas; los gobiernos modernizando leyes para responsabilizar a vendedores ilegales (e incluso debatir la responsabilidad subsidiaria de las plataformas en caso de inacción); y los consumidores con una mayor educación para identificar ofertas sospechosamente baratas o de origen desconocido.

Uso indebido de contenido en redes. Otra dimensión crítica de la PI digital es la circulación masiva de obras protegidas por derecho de autor en redes sociales y sitios de streaming no autorizados. La cultura del *share* ha llevado a que diariamente se suban a plataformas como Facebook, YouTube, TikTok o Twitter fragmentos de videos, música, imágenes y texto que muchas veces infringen los derechos de sus creadores originales. Un caso común es la publicación de videos con música de fondo sin licencia o la retransmisión no autorizada de eventos deportivos vía streaming pirata.

Las grandes plataformas se han amparado en regímenes de **puerto seguro** (*safe harbor*), donde no son responsables directos si actúan diligentemente bajando contenido infractor tras ser notificados. Sin embargo, en Latinoamérica los marcos de limitación de responsabilidad de intermediarios no siempre están claramente definidos por ley, lo que ha generado incertidumbre.

Por ejemplo, Argentina y Brasil no cuentan con una ley específica tipo DMCA; la jurisprudencia argentina (caso

“Belén Rodríguez c/ Google”, CSJN 2014) estableció lineamientos de responsabilidad subjetiva, pero aún se debate la conveniencia de legislar el *notice-and-takedown*. En este vacío, empresas como YouTube implementan sus propios sistemas de gestión de derechos (content ID), que identifican y monetizan contenidos protegidos subidos por usuarios. Aun así, persisten abusos: transmisiones en vivo en Facebook de partidos de fútbol de pago, canciones viralizadas en TikTok sin pagar regalías a artistas, memes que reutilizan ilustraciones sin atribución, etc. [Ludovino Lopes](#), desde su experiencia en la Cámara-e.net de Brasil, ha enfatizado la necesidad de actualizar las leyes de *copyright* para la era de las redes sociales, combinando la autorregulación tecnológica con directrices legales claras.

Propone que los países latinoamericanos se inspiren en iniciativas como el artículo 17 de la directiva europea de derechos de autor (que obliga a plataformas a acordar licencias con titulares o asegurar la indisponibilidad de obras infractoras), y las adapten a nuestra realidad. No obstante, Lopes también advierte que una regulación excesivamente rígida podría sofocar la creatividad y la libertad de expresión en Internet, por lo que aboga por un equilibrio: *“ni barra libre a la piratería digital, ni exigencias técnicas imposibles que ahoguen a emprendedores locales”*.

Políticas de “takedown” y rol de las plataformas. Un punto central en este foco legal es cómo se instrumentan las **políticas de retirada de contenidos ilícitos**. Las plataformas globales operan términos de servicio que

prohíben publicar material que viole derechos de autor o marcas, y disponen canales para denuncias (*report abuse*).

En Latinoamérica, muchas empresas han firmado acuerdos de cooperación con entidades sectoriales: por ejemplo, Mercado Libre trabaja con la Cámara Argentina de la Indumentaria para identificar falsificaciones de ropa; Facebook colabora con organismos antipiratería en México para dar de baja grupos que comparten enlaces a películas pirateadas. Sin embargo, los titulares de derechos a veces critican demoras o inconsistencias en la respuesta.

Jacobo Cohen Imach reconoció este desafío al señalar que **unificar criterios** en 18 países con legislaciones distintas no ha sido trivial, pero que Mercado Libre logró *“estandarizar políticas de cumplimiento y penalización de reincidentes con los mismos criterios en todos nuestros sitios”*, lo cual sugiere que las empresas están tomando la delantera donde las leyes son difusas.

En la práctica, cuando una marca denuncia una publicación infractora, la plataforma no sólo la baja sino que analiza el comportamiento del vendedor para decidir sanciones mayores (suspensión o expulsión) si halla patrón de reincidencia.

Asimismo, se esfuerzan en **educar a los vendedores**: Mercado Libre, por ejemplo, desarrolló tutoriales, guías y hasta webinars sobre cómo evitar infringir derechos de terceros al publicar. Esto es crucial porque muchos

pequeños comerciantes pueden infringir sin plena conciencia (por ejemplo, usando imágenes “bajadas de Google” para sus catálogos o vendiendo réplicas creyendo que es lícito).

Pese a los progresos, subsisten **zonas grises legales**. Un tema candente es la **responsabilidad de las plataformas en sí mismas**: si a pesar de mecanismos razonables, se les cuela una venta de falsificación o un usuario sube una película completa a su perfil, ¿deben las plataformas responder legalmente?

En la actualidad, la mayoría de los países latinos no tiene un régimen expreso de responsabilidad de intermediarios; esto se dirime caso a caso. Hay presión desde sectores industriales para que las plataformas “*hagan más*”. Por ejemplo, asociaciones de la industria musical en Chile y Perú han abogado porque las redes implementen filtros preventivos de contenido (lo que para otros es censura previa y técnicamente complejo).

La llegada de la **Web3** y la tokenización suma nuevas preguntas sobre PI (pensemos en los NFTs de obras digitales y las disputas sobre propiedad de arte digital). Una vez más, *la historia y el futuro convergen*: así como hace dos décadas Napster sacudió la industria discográfica y llevó a repensar modelos de negocio, hoy el streaming ilícito y la reproducción viral obligan a innovar en soluciones legales.

Un aprendizaje clave es que la **cooperación internacional** resulta vital: los delitos de PI online suelen cruzar

fronteras (servidores en un país, usuarios en otro), por lo que iniciativas como la **ACE (Alliance for Creativity and Entertainment)** o convenios entre aduanas para detener envíos de mercancía falsificada son piezas del rompecabezas. Latinoamérica, como bloque, podría beneficiarse de mayor coordinación regional para combatir la piratería digital, compartiendo mejores prácticas y alzando una voz unificada en foros globales.

En síntesis, la propiedad intelectual en el entorno digital plantea a nuestra región un **desafío doble**: adoptar marcos legales actualizados que protejan la innovación y la inversión en creación de contenido, y a la vez implementar soluciones prácticas (tecnológicas, de autorregulación y de enforcement) que equilibren los derechos de todos los actores. La experiencia muestra que *ni la inacción ni las posiciones extremas son la respuesta*: se requiere flexibilidad, diálogo continuo entre empresas tecnológicas, titulares de derechos, usuarios y Estados; e incluso una buena dosis de creatividad jurídica para adaptar conceptos de PI del siglo XX a realidades del siglo XXI.

Como bien lo resume [Jacobo Cohen Imach](#), el objetivo debe ser **“habilitar el negocio”** de forma responsable;⁴³ es decir, permitir que el ecosistema digital prospere, pero dentro de reglas de juego claras que fomenten la confianza y el respeto a la ley.



Fiscalidad digital: ¿Dónde se genera el valor?

La pregunta **“¿dónde se genera el valor?”** en la economía digital encapsula uno de los debates fiscales más profundos de nuestra era. Tradicionalmente, los sistemas tributarios asignan la potestad de gravar ingresos en función de la presencia física de empresas o la realización de actividades en un territorio. Pero en el mundo digital, los gigantes tecnológicos pueden prestar servicios en un país sin tener oficinas ni empleados allí, mientras generan ingresos considerables.

Esto ha llevado a que muchos países se pregunten cómo asegurar que esas empresas *contribuyan* fiscalmente donde obtienen sus ganancias. En Latinoamérica, la discusión sobre la **fiscalidad digital** pasó de teórica a práctica en la última década: hoy casi toda la región ha implementado impuestos a los servicios digitales, especialmente indirectos (IVA), ante el crecimiento del comercio electrónico, los servicios de streaming, las apps de transporte y demás plataformas globales. Veamos la evolución, los desafíos de implementación y el contexto internacional de este tema.

Impuestos digitales en Latam: expansión unilateral. En paralelo a las negociaciones lideradas por la OCDE para un acuerdo global (los famosos *Pilar Uno* y *Pilar Dos* de BEPS), los países latinoamericanos avanzaron *por cuenta propia* con medidas para gravar la economía digital. *Al 2025, la mayoría de las jurisdicciones de la región ha adoptado impuestos digitales de algún tipo, sin esperar el consenso global que sigue demorado.*⁴⁴

Hace apenas 10 años, gran parte de los servicios digitales transfronterizos escapaba al fisco local –si acaso se gravaban vía mecanismos engorrosos de retención en pagos B2B, y los consumos de personas quedaban fuera–. Hoy, en cambio, **México, Argentina, Chile, Colombia, Perú, Uruguay, Costa Rica, Ecuador** y otros países aplican IVA (u otros impuestos) a servicios digitales internacionales.

Esta proliferación de normas ha sido calificada por expertos como una “ola pragmática”: los gobiernos, urgidos de recaudar en economías golpeadas y

conscientes del auge digital, diseñaron soluciones **ingeniosas para capturar la base imponible digital**. Un factor común es que ampliaron el alcance del IVA (impuesto al consumo) para cubrir servicios electrónicos prestados por proveedores no residentes a clientes locales (B2C), algo inicialmente no contemplado en las leyes tributarias tradicionales.

¿Cómo gravan los países los servicios digitales?

Mayormente vía **IVA digital** (impuesto indirecto). Por ejemplo, **México**, desde junio de 2020, exige a las plataformas extranjeras registrarse ante el SAT y cobrar un 16% de IVA a sus usuarios en el país. Además, innovaron incorporando una cláusula de **“kill switch”**: la autoridad puede bloquear el acceso a plataformas que no se registren o cumplan, mientras amenazan con literalmente apagar a los infractores. Aunque ese “botón rojo” no se ha aplicado todavía, ha sido un poderoso incentivo para que gigantes digitales acaten las reglas.

Argentina, por su parte, desde 2018 grava con IVA del 21% (incluso el 27% en algunos servicios) el uso local de servicios digitales extranjeros; en vez de registrar cada plataforma, implementó un sistema de retención por medio de tarjetas de crédito locales –cuando un usuario paga Netflix, su tarjeta automáticamente agrega el IVA y lo envía al fisco argentino–. Este enfoque evita cargar al proveedor extranjero con trámites, trasladando la responsabilidad a los intermediarios financieros nacionales.

Chile optó por obligar a las plataformas extranjeras a inscribirse en el Servicio de Impuestos Internos y abonar

un 19% del IVA; además, faculta a los emisores de tarjetas a retener el impuesto en pagos a no inscritos.

Colombia aplicó un modelo mixto muy completo: desde 2019 impone IVA del 19% similar a Chile, y adicionalmente, en 2021, creó un régimen de **Presencia Económica Significativa (SES)** para cobrar impuesto sobre la renta a plataformas extranjeras que tengan cierto volumen de ingresos o usuarios en el país. Estas empresas pueden elegir entre inscribirse y pagar un **3% sobre ingresos brutos locales** (con anticipos bimestrales del 2%), o bien aceptar una retención del **10%** en cada pago de sus clientes colombianos. Este mecanismo de impuesto directo es pionero en la región (inspirado en India e Israel), y de facto constituye un *digital services tax (DST)* al estilo europeo pero vía sistema interno.

Perú, desde 2020, grava el 18% del IVA a servicios digitales B2C y prevé también retención bancaria (aunque aún no implementada). **Uruguay** fue de los primeros (2018) en aplicar IVA del 22% a servicios digitales y también un impuesto a la renta para proveedores no residentes. Incluso **Brasil**, la mayor economía, que se había rezagado por temas federales, aprobó en 2023 una ley (con vigencia a partir de 2027) que impondrá un 28% de IVA/ISS combinado a servicios digitales prestados desde el exterior (Meza & Durán, 2025), lo que sería la tasa efectiva más alta de la región.

La siguiente tabla resume algunos casos:

Impuestos a servicios digitales en países de Latinoamérica

País	Impuesto aplicado (año vigencia)	Detalles clave
México	IVA 16% (2020)	Plataformas extranjeras deben registrarse ante SAT. Incumplimiento: posible bloqueo (“kill switch”). Retenciones de ISR a ciertos servicios de transporte/hospedaje P2P.
Argentina	IVA 21% (2018) + percepciones locales	Tarjetas locales retienen IVA al consumo digital. No registro de proveedores. Algunos servicios pagan una alícuota del 27%. Adicional impuesto País del 8% para pagos al exterior (desde 2020).
Chile	IVA 19% (2020)	Proveedores no residentes deben inscribirse y declarar. Faculta retención por emisores. Desde 2025: reporte anual de transacciones por plataformas, residentes y extranjeras.
Colombia	IVA 19% (2019) + régimen SES (2021)	Doble vía: IVA con registro similar a Chile e impuesto renta digital (el 3% sobre ingresos locales o un 10% de retención) para empresas con presencia económica significativa. Obligación de reporte de operaciones por plataformas (2025) siguiendo el estándar OCDE.
Perú	IVA 18% (2020)	Registro de proveedores, similar a Chile/Col. Previsto mecanismo de retención (no implementado).
Brasil	IVA ~28% proyectado (2027)	Incluirá servicios digitales en IVA/ISS combinados, tasa elevada. Plan de exigir registro de plataformas. Debate sobre un eventual impuesto sobre ingresos también en curso.
Uruguay	IVA 22% + impuesto renta 12% (2018)	Regla de fuente ampliada: servicios digitales a usuarios locales gravados. Se designan agentes de retención (tarjetas) para IVA e IRNR.
Costa Rica	IVA 13% (2020)	Catálogo de servicios digitales gravados, con retención bancaria similar a Argentina.

Fuente: eContentLAB

Doble imposición y el rol de la OCDE. La proliferación de impuestos “DIY” en Latam, si bien efectiva para recaudar, ha generado preocupación por la posible **doble imposición** y tensiones internacionales. En ausencia de un acuerdo multilateral (el Pilar 1 de la OCDE busca precisamente reasignar parte de las ganancias de las multinacionales digitales a los países de mercado), las medidas unilaterales podrían resultar en que una empresa pague impuestos en origen y en destino sobre el mismo ingreso, o que distintos países reclamen la misma porción de la renta digital. Hasta ahora, muchos impuestos digitales latinos se estructuraron como IVA –que conceptualmente recae en el consumidor final–, con lo que han evitado la confrontación directa con tratados de doble imposición (que cubren más la renta empresarial).

No obstante, **Estados Unidos** ha criticado DSTs en otras regiones por considerarlos discriminatorios hacia sus empresas tecnológicas, y ha llegado a amenazar con represalias comerciales (aranceles) en casos como el de Francia. En Latam no ha habido choques mayores con EE.UU. aún, quizá porque la mayoría optó por IVA en lugar de un DST puro sobre ingresos (Colombia es de las pocas con componente directo).

Aun así, *si la OCDE logra un consenso en 2025-2026*, los países tendrán que ajustar o remover sus impuestos locales para alinearse al acuerdo global, lo que abre interrogantes: ¿renunciarán a una fuente de recaudación ya instalada? ¿Recibirán a cambio una parte suficiente de la “cantidad A” (porción de utilidades redistribuidas) bajo el Pilar 1? Son preguntas abiertas. Por ahora, la OCDE

insta a evitar nuevas medidas mientras negocia, pero la **realpolitik fiscal** se impone: la necesidad de recursos tras la pandemia y la justicia percibida de gravar a las Big Tech donde obtienen ingresos llevaron a los gobiernos a actuar primero.

Un informe de 2024 de Baker McKenzie resaltó que *Latinoamérica tomó un rol proactivo* y que *“lejos de esperar respuestas coordinadas, los países están moldeando sus propios marcos robustos”* para la tributación digital (Meza & Durán, 2025).

Desafíos de tributación a plataformas globales.

Implementar estos impuestos no ha sido trivial. Primero, hubo que **identificar el universo de servicios digitales**: streaming de video/música, apps de ride-hailing, marketplaces, software en la nube, publicidad digital, etc. Luego, establecer mecanismos de cobranza.

Algunos países publican periódicamente listas de proveedores sujetos al IVA digital –Chile ha listado decenas, de Netflix a Spotify, pasando por servicios B2B en la nube– (Meza & Durán, 2025). Otros confiaron en los intermediarios financieros (Arg/C.Rica). México tuvo que montar todo un sistema para inscribir y recibir declaraciones de sujetos no residentes, lo cual implicó también un **cambio cultural** en las empresas globales, ahora obligadas a interactuar con múltiples fiscos locales.

Sorprendentemente, la mayoría de las grandes plataformas ha cumplido sin mayores resistencias, pues prefieren ello a ser bloqueadas o perder mercado. El

cumplimiento es alto: por ejemplo, a menos de un año de vigencia, México ya tenía más de 100 plataformas registradas y recaudó sumas significativas de IVA digital.

Un reto particular es **evitar la evasión** y **garantizar la efectividad**. Colombia, Chile y México complementaron la carga tributaria con **deberes de información estrictos**: desde 2025, Chile exige a *todas* las plataformas (chilenas o extranjeras) reportar anualmente las transacciones realizadas en el país, alineado a las *reglas modelo de la OCDE para plataformas digitales*.

Colombia impone desde 2025 que plataformas con presencia en el país informen operaciones de sus usuarios (alquileres, transporte, ventas de bienes) para facilitar el cruce de datos. Estas medidas recuerdan que la **economía colaborativa** (Uber, Airbnb, marketplaces de segunda mano) también entra en la mira fiscal, no sólo los servicios streaming tradicionales.

Argentina, en cambio, adoptó un enfoque práctico pero quizá menos transparente: no pide reportes a las plataformas, sino que se asegura la recaudación vía los bancos emisores locales. Esto simplifica las cosas para la empresa extranjera, pero podría limitar la información disponible para fiscalización.

La **agresividad en la cobranza** también marca la tendencia. “*Los fiscales latinos se han vuelto más creativos y agresivos en la era digital*”, comenta [Verónica Pinazo, Board Member de YPO Argentina](#). Ella destaca que al mismo tiempo que las empresas digitalizan pagos y flujos

(deep payments), los Estados digitalizan la recaudación; por ejemplo, integrando sistemas de fiscalización en línea en tiempo real.⁴⁵

Colombia ha intensificado auditorías, incluyendo **visitas e incluso señalamientos públicos** a incumplidores (como publicar nombres en boletines de deudores). México, con la figura del **“apagón digital”** (kill switch), impuso respeto aun sin usarla: ninguna plataforma grande quiere arriesgarse a ser dada de baja públicamente. Esta presión ha llevado a un cumplimiento generalizado; el riesgo es que en ausencia de coordinación global, surja una **sobrecarga administrativa** para las empresas, que deben navegar distintos sistemas en cada país; por ejemplo, diferencias en umbrales de registro, en bases gravables (algunos gravan también los *marketplace fees*; otros, sólo el servicio final), en si aplica a ventas de bienes importados de bajo valor (algunos países, como Argentina, gravan con IVA también las compras pequeñas online vía tarjetas).

¿Dónde se genera el valor? Retomando la pregunta inicial, los países de la región han dado una respuesta implícita: *el valor también se genera donde están los usuarios/consumidores*, no sólo donde la empresa tiene su sede. Por eso reclaman una porción de los ingresos digitales. La OCDE, a través del Pilar 1, reconoce ese principio al proponer asignar una parte de las utilidades residuales de las multinacionales a los países de mercado. Sin embargo, como ese acuerdo sigue pendiente, Latinoamérica ha cobrado mientras tanto vía IVA (que es más una carga al consumidor, aunque en la práctica las empresas digitales ajustan sus precios o márgenes).

Un riesgo de esta situación es la **doble carga** al consumidor –por ejemplo, un usuario argentino de Netflix paga un 21% más que uno de EE.UU. por el mismo servicio debido al IVA digital (e impuesto País), y la empresa, a su vez, podría enfrentar impuestos corporativos locales sobre ingresos si se implementan. Hasta ahora, las cantidades recaudadas no parecen haber encarecido dramáticamente los servicios ni frenado la adopción digital; la elasticidad ha sido baja porque la demanda de servicios digitales sigue en ascenso. Pero habrá que monitorear si, de sumarse impuestos sobre renta (un DST al estilo europeo en más países), ello repercute en precios finales o disponibilidad de servicios.

Papel de la OCDE y futuro. La OCDE ha llamado a retirar los DST unilaterales una vez se implemente Pilar 1, a cambio de dar a los países cierta garantía de ingresos mínimos. En octubre de 2023, se anunció un posible inicio de Pilar 1 para 2025, pero con adhesión voluntaria inicialmente. Algunos países de la región han suscrito el Marco Inclusivo de la OCDE, pero otros podrían sentirse más cómodos con sus propias soluciones. Es un delicado juego diplomático: por un lado, evitar *conflictos comerciales* (EE.UU. ya elogió a Brasil por no precipitar un DST y esperar a la OCDE, por ejemplo), y por otro, no resignar soberanía fiscal.

Un punto complementario es el Pilar 2 (impuesto mínimo global del 15% a multinacionales): este afecta menos a las dotcom puras (que suelen ya tributar por encima del 15% efectivo), pero algunos países latinos lo están adoptando para atraer recaudación adicional de filiales locales de tech giants.

En conclusión, Latinoamérica ha demostrado *ingenio* y *determinación* para gravar la economía digital, y ha respondido a la pregunta de dónde se genera valor con acciones concretas: “el mercado también agrega valor; por ende, debe aportar”. Esto ha implicado adaptaciones legales importantes en poco tiempo, con resultados positivos en la ampliación de la base tributaria. [Verónica Pinazo](#) lo resume así:



“Aprender a surfear en mares movedizos es la clave para hacer negocios”.



Verónica
Pinazo

Ella se refiere a cómo, tanto empresas como Estados, deben adaptarse rápidamente. En materia fiscal, los mares movedizos son la tecnología y la globalización; Latinoamérica está demostrando que puede surfearlos, aunque la tabla (el sistema impositivo) deba recalibrarse constantemente. Habrá que ver cómo convergen eventualmente nuestras soluciones locales con la arquitectura global que se termine definiendo: el objetivo último sería un sistema más *justo* y *sencillo*, donde las empresas paguen lo razonable donde obtienen sus beneficios, y eviten doble imposición y competencias desleales. Hasta entonces, el laboratorio latinoamericano de impuestos digitales seguirá siendo referente para otras regiones emergentes que enfrentan similares dilemas de la era digital.

Derechos del **consumidor digital**

El consumidor digital latinoamericano de 2025 es más exigente, informado y empoderado que nunca, pero también enfrenta desafíos particulares en la economía online. La protección al consumidor en el comercio electrónico se ha vuelto un **terreno de tensiones** entre las promesas de las marcas, las prácticas de las plataformas y la capacidad de los reguladores para hacer cumplir las normas. Aspectos como la **logística inversa** (devoluciones), la atención posventa, los derechos de cancelación, la publicidad veraz en promociones masivas y la resolución efectiva de reclamos, están en el centro de la escena.

En muchos sentidos, son temas tradicionales de defensa del consumidor, pero potenciados por la escala digital: un error de atención al cliente que antes afectaba a decenas ahora afecta a miles; un anuncio engañoso en un *Hot Sale* puede viralizarse y dañar la confianza de todo un mercado. Veamos los focos principales:

Logística inversa, devoluciones y cancelaciones. Uno de los derechos fundamentales en ventas a distancia es el **derecho a devolver o cancelar** una compra (*cooling-off period*). En varios países de la región ya se reconoce legalmente: por ejemplo, Argentina tiene un plazo de 10 días para revocar compras online; Chile, 10 días en la Ley Pro Consumidor 2021; Colombia, 5 días; Perú, 10 días; Brasil, 7 días, entre otros. Sin embargo, la **implementación práctica** de estas devoluciones es compleja: requiere sistemas logísticos eficientes (recoger el producto del

domicilio del cliente o habilitar puntos de entrega), políticas claras de reembolso rápido y absorber costos.

Muchas empresas han tratado la logística inversa como un costo operativo alto; no obstante, hoy es *parte inseparable de la experiencia del cliente digital*. Durante eventos masivos (CyberDays, Hot Sale, Black Friday), los volúmenes de ventas se disparan y, proporcionalmente, también las devoluciones.

Yerka Yukich destaca que tras eventos como CyberDay, el foco no sólo está en las ventas récord sino en *“cumplir con los plazos ofrecidos al consumidor”* y manejar eficientemente las devoluciones, porque una baja tasa de reclamos fortalece la confianza en el ecosistema (eLíderes Podcast x25, 2025). De hecho, el CyberDay 2025 en Chile registró ventas por US\$520 millones en tres días y una tasa de reclamos bajísima (0,013%),⁴⁶ lo que Yukich atribuyó a mejoras en profesionalismo logístico y atención al cliente. Esto implica que las empresas han invertido en **capacitación interna** y diversificación de proveedores logísticos para responder a contingencias.

La logística inversa se ha vuelto un nicho específico: startups especializadas en devoluciones eficientes, puntos de retiro que también aceptan retornos de múltiples retailers, etc. No obstante, aún hay brechas: muchos consumidores se quejan de *trámites engorrosos* para devolver (impresión de etiquetas, espera de courier) o de restricciones (por ejemplo, productos que no admiten devolución pese a ser comprados online, lo cual va contra la ley en ciertos casos).

Aquí los entes reguladores han empezado a fiscalizar más: en Argentina, la Dirección de Defensa del Consumidor ha multado a empresas por no acatar el derecho de arrepentimiento (por ej., casos donde obligaban al cliente a conservar un crédito en tienda en lugar de reembolso). En Perú y Colombia, recientemente se emitieron guías para retailers sobre cómo informar claramente este derecho en sus sitios web.

Un desafío adicional es el **estado del producto devuelto**: los comerciantes alegan que a veces reciben de vuelta bienes dañados o utilizados, lo que genera pérdidas. La normativa suele permitir exigir que el bien esté en condiciones similares a las del recibo, pero la interpretación varía y es fuente de roces. Algunas cadenas han optado por políticas más generosas (*free returns sin preguntas*), confiando en que esa satisfacción del cliente fideliza lo suficiente para compensar abusos eventuales.

Atención al cliente digital. En la venta online, la relación con el consumidor no termina al clicar “Comprar”, sino que se extiende a la entrega y el servicio posventa. Sin embargo, muchos usuarios reportan dificultades para obtener atención humana o rápida ante problemas (producto dañado, entrega tardía, cobros indebidos, etc.).

La automatización a veces juega en contra: chatbots poco efectivos, formularios web que nadie responde. Este tema ha derivado en **sanciones por falta de atención adecuada**.

México incluyó en su [NMX-COE-001-SCFI-2018](#) sobre comercio electrónico la obligación de proveer confirmaciones electrónicas y mecanismos claros de seguimiento de quejas. Una tendencia positiva es que varias empresas han integrado sus sistemas de atención con mensajería instantánea (WhatsApp, Facebook Messenger), para estar donde el cliente ya está. Aun así, durante eventos masivos, la demanda colapsa: es usual ver en Twitter a usuarios frustrados etiquetando a las marcas porque no les responden.

Jacobo Cohen Imach comentaba que Mercado Libre debió crear incluso un **equipo específico de resolución de disputas**, consciente de que en ecommerce, *“la resolución de controversias es crítica, pues el modelo depende de clientes satisfechos”* (Wirth, 2020). La empresa implementó sistemas de mediación en línea para conflictos entre vendedores y compradores, devoluciones simplificadas con reembolso inmediato en Mercado Pago, y programas de garantía al cliente. Muchas de estas prácticas luego fueron adoptadas por competidores, y se elevó el estándar de la industria. De cara al futuro, la incorporación de **IA generativa** en atención al cliente podría mejorar la capacidad de respuesta personalizada, aunque no reemplaza la necesidad de políticas empresariales centradas genuinamente en el consumidor.

Publicidad engañosa y ofertas en eventos masivos. Los grandes eventos de comercio electrónico tipo Hot Sale, Cyber Monday y Black Friday han impulsado ventas récord año a año en Latam, pero también trajeron la problemática de las **ofertas engañosas**. Un caso icónico:

durante un Hot Sale, una conocida cadena publicó descuentos que en realidad no lo eran, inflando el “precio anterior” para simular una rebaja. Este “falso descuento” llevó a la justicia argentina a confirmar una multa contra Walmart en 2022, al comprobarse que el precio “antes” exhibido era mayor al real previo al evento, lo que inducía al error al consumidor respecto a un descuento inexistente. El fallo señaló que **“está prohibido realizar publicidad que mediante inexactitudes u ocultamientos pueda inducir a error, engaño o confusión respecto del precio”**, con lo que reafirmó principios básicos de la defensa del consumidor.⁴⁷

Lamentablemente, esta práctica se ha repetido en diversos países y ediciones: es tan común que coloquialmente se habla del “efecto *precio inflado* antes del cyber”. Las autoridades han tomado nota. En Argentina, tras inspecciones, se sancionó a varias empresas por publicidad engañosa en ofertas, incluyendo una multa en 2024 a una cadena de electrodomésticos por anunciar rebajas sobre precios ficticios.⁴⁸

En México, PROFECO cada Hot Sale monitorea los precios y públicamente exhibe a las compañías con más quejas. En Hot Sale 2023, por ejemplo, reportó que Walmart acumuló 6 quejas (el 88% conciliadas); Amazon, 4; (el 75% conciliadas) y otras tiendas algunas más.⁴⁹ Adicionalmente, Profeco impuso multas que sumaron 3.5 millones de pesos por incumplimientos ese año (León, 2024).

Si bien el número de quejas formales en proporción a millones de transacciones es bajo, **el impacto**

reputacional de ser señalado por prácticas engañosas es alto. Las cámaras de ecommerce han reforzado sus **códigos de buenas prácticas** e instado a anunciar descuentos reales y cumplir con el stock y condiciones. En Chile, desde 2022, el SERNAC implementa un “monitor de ciberoferas”⁵⁰ para verificar que los precios rebajados lo estén efectivamente respecto a semanas anteriores, y ha logrado que la mayoría de los retailers ajuste sus estrategias para evitar sanciones.

Otro punto crítico es la **letra chica y condiciones restrictivas** en ventas digitales. Por ejemplo, limitaciones arbitrarias en cambios (ropa interior sin cambio aunque no se haya usado), garantías más cortas de lo legal, cargos ocultos (seguros añadidos por defecto). Estas prácticas han sido objeto de acciones colectivas en algunos países. En Colombia, la Superintendencia multó a una empresa de tiquetes aéreos online por preseleccionar seguros sin consentimiento expreso del cliente en el carrito de compra. En Perú, Indecopi sancionó a webs de cupones por imponer vencimientos no claros. Todo apunta a la necesidad de **transparencia total** en la información al consumidor digital: mostrar el precio final *desde el inicio*, detallar costos de envío, políticas de cambio, y no modificar condiciones tras la compra.

Casos recientes y fallos relevantes. Además del mencionado caso Walmart en Argentina, podemos citar otros ejemplos ilustrativos: En 2021, la justicia brasileña falló contra una tienda virtual que canceló unilateralmente compras hechas durante una promoción alegando error

de precio. El tribunal obligó a honrar las ventas, lo que sentó precedente sobre la *oferta vinculante online*.

En Uruguay, se gestionaron reclamos masivos cuando en un Cyberlunes 2023, una plataforma de viajes ofreció paquetes con un 50% off pero luego no pudo confirmarlos: la autoridad de consumo intervino logrando reubicación de clientes o devoluciones integrales. Estas situaciones muestran que, si bien la **explosión de las ventas online** ha sido bienvenida, también requiere una **madurez en la responsabilidad empresarial** equivalente. Yerka Yukich acota que eventos como el Cyber Day han ido **“contribuyendo al profesionalismo del comercio electrónico”**, al obligar a las marcas a implementar mejores prácticas para cumplir lo prometido y a robustecer sus sitios para soportar la demanda (Pino, 2025). Sus palabras reflejan que de los errores y reclamos se aprende: las ediciones tempranas de estos eventos tuvieron más tropiezos que las actuales, en las que las empresas chilenas al menos han logrado minimizar problemas.

Por su lado, *Jacobo Cohen Imach* suele remarcar la importancia de la **autorregulación y las garantías voluntarias** como complemento a la ley: Mercado Libre, por ejemplo, ofrece protección al comprador hasta cierto monto en casos de fraude o producto distinto al anunciado, incluso más allá de lo exigido legalmente, para brindar tranquilidad. Este tipo de iniciativas marca la pauta y se convierte en estándar cuando los competidores las adoptan.

Atención en eventos masivos (Hot Sale, Cyber Monday, etc.). Vale la pena destacar que los organismos estatales han organizado operativos especiales durante estos eventos. PROFECO en México instala “cuartos de guerra” para atender denuncias en vivo; en Argentina, la Secretaría de Comercio hace fiscalizaciones online y mantiene guardias para reclamos rápidos; en Chile, el SERNAC habilita formularios exprés durante el Cyber. Todo esto mejora la capacidad de reacción ante abusos. A la par, los propios eventos organizados por las cámaras incluyen en sus términos la cooperación con autoridades y protocolos de buenas prácticas (p.ej., penalizar a empresas que reciban muchas quejas excluyéndolas de futuras ediciones, algo que la AMVO de México y la CACE de Argentina han considerado).

En síntesis, los derechos del consumidor digital se fortalecen en el papel pero requieren vigilancia constante en la práctica. La región ha avanzado en modernizar marcos (por ejemplo, varias leyes ahora incluyen comercio electrónico explícitamente) y en mecanismos de resolución en línea de disputas. Sin embargo, el aumento del volumen de transacciones y la diversidad de actores (marketplaces con miles de vendedores) generan *nuevas formas de fricción*.

El camino hacia adelante demandará: mayor **educación digital** para consumidores (saber sus derechos y ejercerlos); inversión continua de las empresas en **customer experience** (logística, atención omnicanal, transparencia); y **reguladores innovadores**, que utilicen herramientas tecnológicas para monitorear el mercado

en tiempo real. Al final del día, como señala Yukich, “*un consumidor informado y confiado es el mejor indicador de un ecosistema ecommerce saludable*”, por lo que todos –industria y autoridades– comparten el objetivo de mejorar la **confianza digital**. Cuando los consumidores sienten que sus derechos en línea están tan protegidos como en el mundo físico, se animan a comprar más y a participar plenamente de la economía digital, lo que cierra así un círculo virtuoso de crecimiento con protección.

Publicidad y responsabilidad en redes sociales

El auge de las **redes sociales** y de las figuras de los **influencers** ha revolucionado el marketing, pero también ha abierto un frente regulatorio poco explorado: ¿cómo asegurar la **veracidad y transparencia** de la publicidad en estas plataformas? En Latinoamérica, la línea entre contenido espontáneo y publicidad pagada muchas veces se difumina, con influencers promoviendo productos sin aclararlo, recomendaciones engañosas, o falta de lineamientos claros sobre la responsabilidad por lo que se comunica en redes.

Este foco de tensión combina elementos de publicidad tradicional (engaño, omisiones) con un nuevo formato de voceros (creadores de contenido, microinfluencers) y canales (Instagram, YouTube, TikTok, Twitch, Facebook, Twitter/X). En comparación, mercados como Estados Unidos llevan la delantera con guías exhaustivas –las **Endorsement Guides** de la FTC–, mientras que en nuestra

región aún predomina un vacío normativo cubierto parcialmente por autorregulación.

Influencers y publicidad encubierta. Los influencers se han convertido en actores clave: desde celebridades hasta personas comunes que acumulan seguidores fieles. Su “naturalidad” y cercanía dan gran poder de recomendación, lo que las marcas aprovechan para publicitar de forma menos convencional. El problema surge cuando esas recomendaciones pagadas no se identifican como tales, lo que induce al engaño a la audiencia que cree en la objetividad del influencer.

Un estudio sobre la **regulación en América Latina** revela que desde aproximadamente 2017, algunos países empezaron a trazar lineamientos pero con enfoques dispares.⁵¹ Por un lado están los **códigos de autorregulación publicitaria** promovidos por la industria: por ejemplo, CONAR en Brasil emitió en 2020 guías para influencers, al igual que el Consejo de Autorregulación Publicitaria de Argentina (CONARP) en 2021 recomendó usar hashtags como #Publicidad o #Ad. Sin embargo, al ser voluntarios, su cumplimiento es variable.

Por otro lado, algunos **entes estatales** han incursionado en el tema: la Secretaría de Comunicaciones de México elaboró en 2018 un proyecto de lineamientos (tras un escándalo de influencers políticos), aunque no se volvió vinculante; en Colombia, la SIC ha sancionado algunos casos de publicidad engañosa con influencers bajo normas generales; en Chile, SERNAC inició en 2023 un estudio sobre “influencers y protección del consumidor”.

Globalmente, España recientemente aprobó en 2024 un Real Decreto que regula a los “usuarios de especial relevancia pública en redes” (influencers) y los equipara a medios en ciertas obligaciones, lo cual marca un precedente interesante.

Actualmente, la falta de claridad es la norma: la mayoría de los influencers latinos no están seguros de cómo deben revelar colaboraciones pagadas, y muchos no lo hacen en absoluto. Esto genera situaciones de engaño: promociones de productos milagro (ej., suplementos “detox” por influencers de fitness), sin base científica, recomendaciones de inversiones riesgosas por youtubers sin advertir que están patrocinados, o simplemente lifestyle bloggers mostrando marcas constantemente regaladas sin informar el patrocinio. [Ludovino Lopes](#), director del capítulo Brasil del eCommerce Institute, opina que:



“Esta falta de regulación clara deja tanto a influencers como a consumidores en una zona gris peligrosa”.



**Ludovino
Lopes**

Hizo énfasis en la necesidad de orientar a los creadores de contenido sobre qué se puede o no hacer, antes de que ocurran fraudes mayores o se socave la confianza en la publicidad digital. Según él, la autorregulación puede ser un primer paso –por ejemplo, acuerdos entre agencias de marketing de influenciadores para seguir ciertos

estándares–, pero probablemente serán necesarias **normas específicas** dado el crecimiento del fenómeno.

Comparativa con guías de la FTC (EE.UU.). Al mirar el modelo estadounidense, vemos un camino posible. La **Federal Trade Commission (FTC)** actualizó en 2023 sus guías de endorsements precisamente para los nuevos medios, y dejó claro que *cualquier conexión material entre un influencer y la marca debe ser divulgada de forma “clara y visible”*.⁵² Esto incluye pagos, regalos, vínculos laborales o familiares. Las directrices de la FTC detallan cómo hacerlo según la plataforma: por ejemplo, en Instagram o TikTok, se recomienda usar hashtags obvios como **#Publicidad**, **#Ad**, **#Patrocinado** al inicio del texto, o herramientas de etiquetado de pago cuando existan.

Prohíben cosas como esconder la divulgación entre muchos hashtags, solo mencionarla en la descripción y no en el video, o suponer que “mis seguidores ya saben que colaboro con tal marca” (Talip Pinarbasi, 2025). Además, la FTC ha tomado acciones contra casos flagrantes; por ejemplo, multó a una empresa de té dietéticos (caso Teami, 2020) por hacer que influencers famosos promocionaran beneficios de salud falsos sin revelar que eran pagados (FTC, 2023). Si bien la realidad legal de EE.UU. difiere, estas guías sirven de **referente internacional**.

Por ahora, algunos influencers latinos que trabajan con marcas globales ya incorporan **#Ad** en sus posts por requerimiento contractual (sobre todo los que también tienen audiencia en EE.UU. o Europa). Pero son la minoría;

la mayor parte de la publicidad con influencers en nuestra región sigue ocurriendo de forma **informal**. La ausencia de sanciones visibles locales quizás ha prolongado esa situación, pero también empiezan a darse los primeros precedentes: en 2021, la autoridad de competencia en Argentina (CNDC) investigó a influencers del rubro financiero por publicitar esquemas de inversión sin mencionar riesgos, y aunque la vía fue competencia leal, envió un mensaje. En Brasil, en 2019 CONAR llamó la atención a una celebridad por no indicar que su elogio a un hotel era patrocinado, y la obligó a borrar el post; si bien no fue multa estatal, mostró la presión social.

Responsabilidad en redes sociales. Más allá de la publicidad está el tema de la **responsabilidad por el contenido** que circula en redes, especialmente cuando puede causar daño o confusión en consumidores. Un ejemplo: recomendaciones médicas o nutricionales por personas no calificadas en TikTok (riesgo a la salud), publicidad de productos financieros complejos en YouTube (riesgo económico) o casos extremos de desafíos virales peligrosos. Las redes sociales hasta ahora han adoptado enfoques de *autorregulación moderada* (removiendo contenido claramente nocivo que viole sus términos), pero la cuestión de si los *influencers mismos* tienen alguna responsabilidad legal frente a sus seguidores es novedosa.

En publicidad tradicional, un anuncio falso recae en el anunciante y a veces en el medio por difundirlo. En el ámbito influencer, el “medio” es a la vez el vocero. Algunos juristas plantean que un influencer que recomienda, por ejemplo, un suplemento alimenticio diciendo que cura

enfermedades podría enfrentar acciones por publicidad engañosa o incluso por ejercicio ilegal de profesión. Sin embargo, no hay casi casos judiciales al respecto aún en Latam.

Una línea de acción probable es que se adapte el marco de **publicidad comercial** para incluir a comunicadores digitales. Varias leyes de defensa del consumidor ya establecen que *“quien, usando cualquier medio de difusión, realice recomendaciones comerciales engañosas será responsable”*. Esto podría aplicarse a un influencer. Pero en la práctica, perseguir cientos de microinfluencers sería poco eficiente; por eso, el foco regulatorio se dirige más bien a exigir **transparencia** (que digan cuando es publicidad) y a que las marcas anunciantes sean corresponsables.

De hecho, la FTC deja claro que las empresas no pueden escudarse en “yo no publiqué, fue el influencer”: si contratan a alguien, deben asegurarse de que cumple las guías, so pena de sanción para la empresa también (Talip Pinarbasi, 2025). Este principio puede permear nuestra región por vía de buenas prácticas corporativas; muchas multinacionales ya instruyen a sus agencias locales para que cualquier campaña con influencers incluya disclosure, justamente para no violar lineamientos globales.

Casos de publicidad engañosa con influencers.

Aunque todavía incipiente, ya hubo algunos escándalos resonantes: En 2020, en plena pandemia, varios influencers mexicanos promovieron un partido político

en plena veda electoral a cambio de pagos ocultos, lo que fue expuesto y generó multas del INE a ese partido (el caso “Green Influencers”); esto evidenció la necesidad de regular también la publicidad política encubierta.

En 2022, en Argentina, una influencer de belleza recomendó un protector solar que en realidad no tenía eficacia probada; sus seguidores reportaron quemaduras y el tema llegó a TV, lo que forzó a la marca a responder y a la ANMAT (Administración Nacional de Medicamentos, Alimentos y Tecnología Médica) a intervenir sobre la publicidad de cosméticos.

Estos episodios van marcando la agenda: se discute, por ejemplo, si debería obligarse a los influencers profesionales a registrarse en algún padrón (como insinuó España con su nueva ley) o si bastaría con reforzar la normativa general de publicidad y capacitar tanto a creadores como a consumidores.

Falta de regulación clara vs. autorregulación activa.

La balanza en Latinoamérica aún está inclinada hacia la **autorregulación**. Organismos como el **eCommerce Institute** han elaborado manuales de buenas prácticas en marketing de influencers, y asociaciones de publicidad lanzan campañas educativas. Un efecto interesante es el rol de la **comunidad digital**: los propios usuarios muchas veces detectan y denuncian en redes cuando un influencer oculta publicidad (#publiencubierta).

Esta suerte de **“fiscalización 2.0”** ha llevado a más de un creador a rectificarse públicamente. Sin embargo, no

se puede depender sólo de eso; se requiere un marco mínimo. Países como **Colombia** analizan modificar su Estatuto del Consumidor para añadir obligaciones de divulgación en comunicaciones comerciales digitales. **Perú** actualizó en 2022 su Código de Protección al Consumidor incorporando sanciones a publicidad digital engañosa, lo que podría servir de base para casos con influencers.

Ludovino Lopes sugiere que una solución regional ideal sería que los países adopten lineamientos similares a la FTC, adaptados al idioma y contexto local, de modo que haya uniformidad. *“No tiene sentido reinventar la rueda; las guías de la FTC básicamente dicen ‘sé honesto, no escondas que te pagan’.* ¿Quién podría oponerse a eso?”, comenta Lopes (eLíderes Podcast x25, 2025). Su perspectiva subraya que la transparencia beneficia a todos: los consumidores confían más cuando ven honestidad, los influencers resguardan su credibilidad a largo plazo, y las marcas evitan crisis de imagen.

Responsabilidad de plataformas versus creadores. Un aspecto final es cómo reparten la responsabilidad las **plataformas de redes sociales**. Por ahora, Instagram, YouTube, etc., proveen herramientas (p.ej., la etiqueta “Paid partnership with...” en IG) pero no obligan a su uso. No suelen interferir a menos que haya violación de políticas (como promoción de drogas, esquemas piramidales, etc.). Pero a medida que los gobiernos presionen, podrían verse compelidas a involucrarse más; quizá reportando publicidad encubierta si es flagrante, o cooperando con autoridades en identificar a infractores mayores.

Esto abre la puerta al debate sobre libertad de expresión: es un área sensible porque regular influencers podría interpretarse como regular a individuos hablando en redes. La distinción clave es enfocarse sólo en comunicaciones **comerciales**, no en opiniones genuinas. Ahí es donde la claridad de definiciones será fundamental.

En resumen, la publicidad y responsabilidad en redes sociales constituyen un **terreno regulatorio emergente** en Latinoamérica. Estamos aún en las etapas iniciales de reconocimiento del problema y de soft law (autorregulación), con pocos instrumentos duros específicos. La experiencia de otros mercados indica que eventualmente será necesario algún grado de regulación explícita para evitar abusos sistemáticos.

Mientras tanto, la concientización juega un papel enorme: tanto influencers como audiencia deben comprender que “no todo lo que brilla es espontáneo”. Como reflexión final, vale citar un principio central de las guías FTC: *“Si tienes que pensar si debes revelar una conexión, **revelala**”* (Talip Pinarbasi, 2025). Aplicar esa simple regla de honestidad podría resolver la mayoría de los dilemas actuales sin requerir más leyes. Hasta que logremos ese estándar cultural, será tarea de las autoridades, las plataformas y los mismos líderes de opinión digitales impulsar entornos en que la publicidad en redes sea **responsable y transparente**, para cimentar la confianza en esta poderosa forma de comunicación comercial.



Radar de riesgos regulatorios 0–5

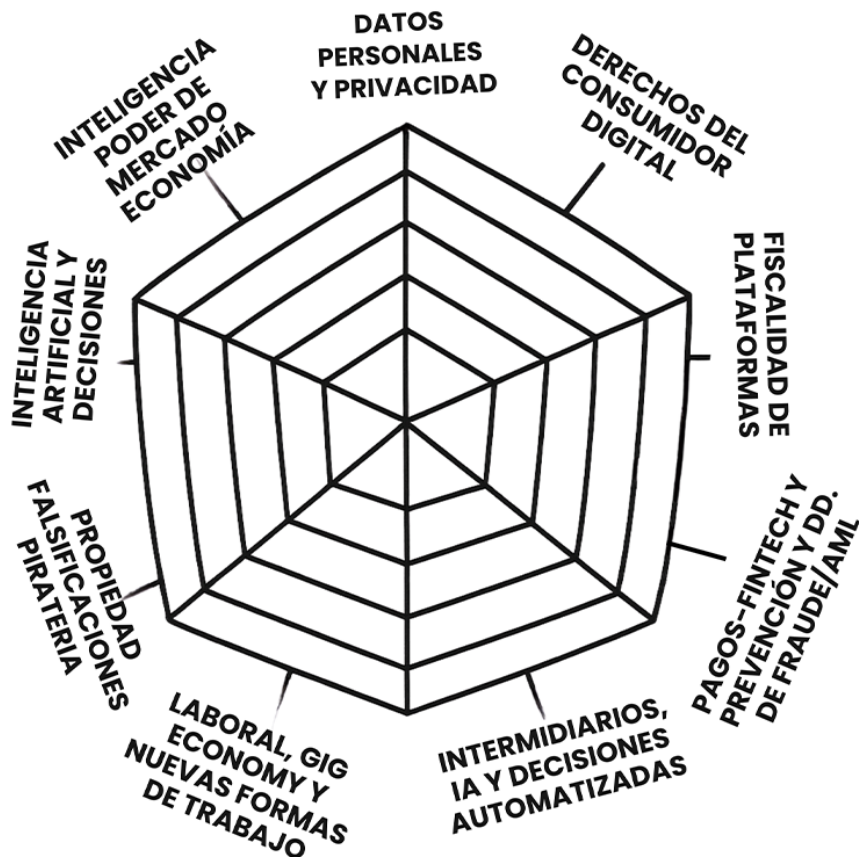
Después de recorrer estos focos de tensión —datos personales, propiedad intelectual, fiscalidad, derechos del consumidor y publicidad en redes sociales— es fácil sentir que el mapa regulatorio es un enjambre caótico de normas, agencias, casos y siglas. Pero si ponemos todo en una misma hoja, lo que aparece no es un ruido ininteligible, sino un **radar de riesgos** bastante reconocible: ciertas áreas concentran hoy la mayor probabilidad de conflicto y sanciones, mientras otras funcionan como frentes emergentes que van ganando intensidad a medida que maduran los modelos de negocio.

Este **Radar de riesgos regulatorios 0–5** propone justamente eso: transformar la lista de temas legales en una herramienta visual y dinámica para el comité ejecutivo. En lugar de preguntarse “¿qué ley nueva salió?”, el C-level puede preguntarse: *¿en qué cuadrantes de probabilidad–impacto están mis riesgos hoy y quién los está monitoreando dentro de la organización?* El objetivo no es asustar, sino **priorizar**: enfocar primero energía, presupuesto y capacidades —incluida la IA-Unificada— allí donde un cambio normativo o una sanción podrían reconfigurar el negocio.

En una primera aproximación, el radar puede organizarse en nueve “rebanadas”:

- ❑ **Datos personales y privacidad**
- ❑ **Derechos del consumidor digital**
- ❑ **Fiscalidad digital y tributación de plataformas**
- ❑ **Pagos, fintech y prevención de fraude/AML**
- ❑ **Propiedad intelectual, falsificaciones y piratería**
- ❑ **Publicidad, influencers, retail media y uso de datos comerciales**
- ❑ **Competencia, poder de mercado y economía de plataformas**
- ❑ **Laboral, gig economy y nuevas formas de trabajo**
- ❑ **Inteligencia artificial, algoritmos y decisiones automatizadas**

RADAR DE RIESGOS REGULATORIOS 0-5



**"LO QUE ES INVISIBLE A LOS OJOS
PUEDE PONER EN JAQUE EL NEGOCIO"**

MARCOS PUEYRREDON

Cada organización asigna a cada ámbito un nivel de riesgo entre 0 y 5, donde 0 implica “tema hoy prácticamente irrelevante para nuestra operación” y 5 significa “riesgo existencial que puede amenazar ingresos, licencia de operación o reputación si no se gestiona bien”.

En muchos players B2C de la región, por ejemplo, el radar tiende a mostrar **datos personales** y **derechos del consumidor digital** en niveles 4 o 5: son ámbitos donde ya existen leyes específicas, autoridades activas y casos que han dejado huella. Esta lectura dialoga directamente con lo que desarrollamos en el libro vivo [“La revolución de los datos y el nacimiento del ciudadano digital”](#), donde mostramos cómo los datos pasaron de “nuevo petróleo” a “nuevo derecho” y por qué el Data Trust Flywheel sólo gira si hay un marco de confianza y cumplimiento explícito.

Algo similar ocurre con la fiscalidad **digital** y **pagos/fintech**, que en buena parte de Iberoamérica se ubican también en niveles altos: los físicos han afinado la puntería sobre servicios digitales, y los bancos centrales han endurecido los requisitos para billeteras, emisores y agregadores. Esta capa del radar se entiende mejor si se la conecta con la historia que contamos en [“El boom del comercio electrónico”](#): allí se ve la primera ola de “ingeniería fiscal creativa” y, luego, el ajuste de los Estados para capturar parte del valor generado por la economía de plataformas y los nuevos medios de pago.

En **propiedad intelectual y falsificaciones**, el riesgo varía según modelo: para marketplaces horizontales y plataformas C2C suele estar en niveles 3–4, mientras que

para retailers con surtido propio puede ubicarse más abajo. En [“La implementación de los modelos Unified & Collaborative Commerce”](#) profundizamos justamente en cómo la elección del modelo (retail, marketplace, *drop shipping*, pure player, híbrido) define desde el día cero la exposición a reclamos por falsificación, uso indebido de marcas o distribución paralela.

El bloque de **publicidad, influencers y retail media** aparece como un frente **claramente ascendente**: en muchos modelos todavía está en 2–3, porque las autoridades están dando sus primeros pasos en lineamientos y casos, pero todo indica que migrará rápido hacia niveles 4–5. El desarrollo de redes de retail media que combinan datos transaccionales con audiencias digitales —tema que exploramos en el libro [“El desarrollo del Retail Media Network”](#) y en la saga [#RetailReset](#)— amplifica el potencial de impacto: un uso incorrecto de datos o una campaña mal etiquetada puede derivar en sanciones y, sobre todo, en pérdida de confianza del consumidor.

En **competencia y economía de plataformas**, el radar varía según escala. Un emprendimiento local puede sentirse “fuera del radar” (niveles 1–2), pero a medida que se construyen posiciones dominantes en ciertos verticales —algo que analizamos en profundidad en [“La implementación de los modelos Unified & Collaborative Commerce”](#)— aparecen preguntas sobre abuso de posición, auto-preferencia, cláusulas de paridad o acceso discriminatorio a datos. Incluso cuando la autoridad de competencia todavía no actúa, el riesgo reputacional ya está en juego.

En **laboral y gig economy**, muchos actores digitales siguen operando en una zona de grises: los niveles de riesgo suelen percibirse como 2–3, pero la experiencia internacional muestra que basta un fallo emblemático para que un país reconfigure reglas de juego completas. Aquí el radar se cruza con lo que contamos en [“El ecosistema emprendedor y el impulso de las nuevas iniciativas”](#): la forma en que definimos el vínculo con colaboradores, repartidores, creadores o desarrolladores externos no es sólo una decisión de costos, sino también de exposición regulatoria futura.

Finalmente, el bloque de **IA, algoritmos y decisiones automatizadas** es hoy, para muchos, una especie de “nube de tormenta en el horizonte”: el riesgo se percibe en 1–2, pero el potencial impacto es 4–5. En [“El arribo de las tecnologías exponenciales y la transformación del ecosistema”](#) hablamos de cómo la IA razonante y generativa se vuelven tejido de fondo de todos los procesos; en este libro, esa misma IA aparece como nueva frontera regulatoria: scoring crediticio, fijación dinámica de precios, segmentación de audiencias, recomendaciones personalizadas. El radar ayuda a no subestimar este frente sólo porque todavía no explotó ningún gran caso local.

La utilidad real del radar aparece cuando lo **llenamos en equipo**. Un ejercicio simple —que conecta con el Risk-Impact Canvas que venimos trabajando en la colección— consiste en convocar a líderes de legal, compliance, tecnología, producto y negocio y pedirles que asignen, de manera independiente, un valor de 0 a 5 a cada rebanada.

Las diferencias entre percepciones son tan reveladoras como el promedio: si legal ve el riesgo de datos en 5 y tecnología en 2, hay una conversación pendiente sobre exposiciones, controles y prioridades de inversión.

A partir de esa lectura compartida, el radar se puede cruzar con otros marcos de la colección:

- ❑ Con el **data trust flywheel**, para entender cómo la confianza regulatoria alimenta o frena el giro del flywheel de datos, experiencia y monetización.
- ❑ Con el **flywheel retail 4.0**, para mapear en qué parte del ciclo (atracción, conversión, recurrencia, recomendación) un cambio normativo podría tener más impacto.
- ❑ Con el **risk-impact canvas**, para traducir cada rebanada del radar a efectos concretos en ingresos, margen, crecimiento, talento y reputación.

En una fase más avanzada, este radar incluso puede **dejar de ser estático**. Integrado a la arquitectura de IA-Unificada, puede alimentarse en tiempo real con novedades regulatorias, proyectos de ley, fallos y guías de autoridades, ajustando automáticamente la puntuación de cada rebanada. La imagen ideal —que retoma la lógica de human augmented AI que recorre toda la colección— es la de un comité ejecutivo que ya no se entera de los cambios legales por un mail perdido, sino que ve en su panel de control cómo el “semáforo” regulatorio cambia de color y dispara conversaciones estructuradas sobre estrategia, producto y ecosistema.

Este radar no reemplaza al análisis jurídico profundo ni al rol de los especialistas. Pero, igual que los otros frameworks que venimos construyendo a lo largo de *Génesis de un Futuro Digital*, cumple una función clave: **hacer visible lo que suele quedar escondido en documentos técnicos**, y convertir el riesgo regulatorio en una conversación de negocio, de ecosistema y de futuro compartido.

GÉNESIS

DE UN FUTURO DIGITAL



GÉNESIS

DE UN FUTURO DIGITAL





Jurisprudencia clave y casos que sentaron precedentes

Este capítulo destaca los fallos, sanciones y resoluciones más relevantes en Iberoamérica que marcaron un antes y un después en la regulación del ecosistema digital y del comercio electrónico. A medida que la innovación tecnológica avanza más rápido que las leyes, los tribunales y autoridades han tenido que **llenar vacíos normativos** y moldear *reglas de juego* mediante sus decisiones.

Veremos casos emblemáticos –desde disputas fiscales hasta protección al consumidor y datos personales– para entender cómo la **jurisprudencia** se ha convertido en un pilar regulatorio, en un entorno donde la ley suele llegar tarde frente a la innovación. También recopilaremos **testimonios de expertos** que vivieron estas batallas legales de cerca, que aportan contexto desde su experiencia en primera persona.

La función de la jurisprudencia en un ecosistema en mutación

En ausencia de leyes específicas para cada nueva tecnología o modelo de negocio digital, la **jurisprudencia** –es decir, las decisiones judiciales y administrativas– juega un rol crucial como fuente normativa. Los jueces y reguladores a menudo deben **interpretar principios generales del derecho** (contratos, responsabilidad civil, derechos fundamentales) para **situaciones inéditas** del mundo digital. Así, la jurisprudencia actúa como un **laboratorio legal** donde se adaptan conceptos tradicionales a nuevos escenarios: ¿es un marketplace “proveedor” como lo sería una tienda física? ¿Aplican las leyes de consumo a plataformas globales? ¿Puede equipararse la moderación de contenido en redes sociales con la libertad editorial de un medio de prensa?

Los enfoques varían. En algunos casos, tribunales adoptan posturas **restrictivas** para proteger intensamente a consumidores o derechos individuales, aun a riesgo de frenar modelos innovadores. En otros, priman visiones **proinnovación** que buscan no “matar la gallina de los huevos de oro” digital con sobrerregulación. Encontrar el **equilibrio** no es fácil.

Jacobo Cohen Imach recuerda que Argentina, a diferencia de marcos más rígidos como el GDPR europeo, optó por **incluir a todos los actores en la mesa**, con lo que logró acuerdos viables para proteger a los usuarios **sin frenar la innovación**. En su experiencia, la regulación

efectiva “no se impone desde el desconocimiento sino que se construye desde la **escucha** y el entendimiento del ecosistema” (eLíderes Podcast x25, 2025).

Un ejemplo temprano fue la implementación de la factura electrónica en Argentina, un proceso de cocreación entre regulador e industria: “El regulador nos invitó, nos dijo ‘vengan, díganme cómo esto se puede implementar’, y juntos lo logramos”. Gracias a esa colaboración público-privada, Argentina fue pionera en adoptar sistemas como la firma digital (aunque Cohen Imach admite que “a nivel de implementación fue un desastre” y sigue siendo un pendiente).

En otros contextos, sin embargo, han primado respuestas más reactivas. Frente al auge de plataformas digitales, hubo intentos de aplicarles responsabilidad directa por actos de sus usuarios, o prohibiciones tajantes cuando surgían vacíos legales. Aquí nuevamente la autorregulación y la jurisprudencia han sido claves para **llenar el vacío**.

Jacobo Cohen Imach cuenta que, cuando se pretendía responsabilizar a los intermediarios por lo que hacían (o dejaban de hacer) los usuarios, Mercado Libre adoptó un enfoque audaz: **autorregulación para construir estándares**. Fue el llamado *notice and take down*, -que ya mencionamos. Esta práctica, nacida de la experiencia latinoamericana, anticipó la línea que luego muchas cortes validarían: las plataformas no son absolutamente irresponsables, pero tampoco pueden supervisarlos todo. Una notificación del afectado activa su deber de actuar.

La jurisprudencia en la región ha debido **balancear innovación y protección**. Algunos tribunales han optado por proteger valores tradicionales (privacidad, veracidad comercial, competencia leal), aun forzando a las plataformas a cambiar prácticas. Otros han reconocido explícitamente que una regulación mal calibrada puede ahuyentar la innovación. Nuevamente Jacobo, desde su perspectiva regional, advierte que muchas iniciativas legales están desconectadas de la realidad digital y se basan en suposiciones: *“Se prohíben cosas o se ponen límites cuando la gente comparte mucho más de lo que el regulador cree”*.

Regular mal no sólo frena la innovación *“sino que **expulsa talento y oportunidades**; la tecnología no es como ensamblar autos. Si no lo hacés acá, lo hacen en otro lado, pero se va todo el ecosistema”*. Su mensaje final es claro: la transparencia, el respeto al usuario y la confianza construida por las propias empresas pueden ser más efectivos que *“cualquier ley mal diseñada”*. En definitiva, a falta de leyes perfectas, son las decisiones caso a caso –y la conducta responsable de los actores– las que van marcando la pauta en este entorno en mutación.

Casos emblemáticos en Iberoamérica

Pasemos ahora a ejemplos concretos donde fallos y sanciones marcaron un antes y después. Cada caso emblemático reveló tensiones propias de cada país, pero sus **repercusiones trascendieron fronteras** e influyeron

en todo el ecosistema iberoamericano. A continuación, revisamos varios hitos jurisprudenciales en Brasil, México, Colombia, Chile y Argentina.

Serie “Caso corto regulatorio”: Radiografías rápidas para aprender

A lo largo del libro venimos recorriendo leyes, fallos, sanciones y acuerdos que moldearon el ecosistema digital iberoamericano. Son historias densas, llenas de matices. Pero, en la práctica, muchos lectores —sean C-level, emprendedores o policy makers— necesitan también **“fotografías rápidas”** que les ayuden a conectar cada caso con decisiones concretas de negocio y de política pública.

Por eso propongo estructurar una serie de **“Casos cortos regulatorios”** a lo largo de este capítulo y del anterior. Son pequeñas cápsulas narrativas que condensan en 10–15 líneas tres preguntas clave:

- ❑ **¿Qué pasó?** El contexto y el conflicto concreto.
- ❑ **¿Qué decidió el regulador o el tribunal?** El criterio que terminó imponiéndose.
- ❑ **¿Qué aprendimos?** La lección que debería quedar pegada en la cabeza de quien diseña productos, regula o emprende.

La lógica es similar a la que uso en otros libros de la colección *Génesis de un Futuro Digital*. En [“El boom del](#)

[comercio electrónico](#)” reconstruimos hitos a partir de anécdotas concretas de pioneros; en [“El ecosistema emprendedor y el impulso de las nuevas iniciativas”](#) mostramos cómo decisiones de política pública, vistas desde los casos, aceleran o frenan vocaciones; en [“El desarrollo del Retail Media Network”](#) utilizamos ejemplos puntuales para ilustrar tensiones entre monetización, datos y confianza. Aquí hacemos algo parecido, pero con foco en la **interfaz entre innovación y regulación**.

Los casos cortos que siguen no agotan la casuística de la región —para eso está el resto del capítulo con fallos y sanciones desarrollados en detalle—, pero sí funcionan como **puertas de entrada rápidas** a temas que reaparecen en varios libros de la saga:

- ❑ La protección de datos y la biometría, que dialoga con [“El arribo de las tecnologías exponenciales y la transformación del ecosistema”](#).
- ❑ La experimentación fintech y los sandboxes, conectada con [“La implementación de los modelos unified & collaborative commerce”](#) y con los capítulos sobre ecosistema emprendedor.
- ❑ La publicidad con influencers y el retail media, que se enlaza con [“El desarrollo del retail media network”](#) y con la saga #RetailReset.
- ❑ Los primeros pasos en regulación de IA, en sintonía con los principios de la OCDE y UNESCO, que analizamos en el momentum de tecnologías exponenciales.

A continuación presento **cuatro ejemplos tipo**. Podés usarlos tal cual como recuadros o adaptarlos a diseño editorial, y repetir el mismo formato en otros capítulos (por ejemplo, en *Déjà vos regulatorios* y en *Focos de tensión legal*), manteniendo siempre la estructura **¿qué pasó? / ¿qué decidió el regulador? / ¿qué aprendimos?**

Caso regulatorio sobre biometría y reconocimiento facial: el límite de “todo vale por seguridad”

¿Qué pasó? Una plataforma de ecommerce y servicios digitales en Colombia decidió exigir a sus usuarios el uso obligatorio de reconocimiento facial para autenticar operaciones y abrir cuentas. La medida se justificaba en nombre de la “seguridad” y la prevención de fraude, pero implicaba recolectar y tratar **datos biométricos sensibles** de millones de personas sin un análisis profundo de proporcionalidad ni alternativas menos invasivas. Como contamos más adelante en la sección *Colombia: datos personales y responsabilidad de las plataformas*, las quejas de usuarios y las investigaciones de la autoridad de datos encendieron las alarmas.

¿Qué decidió el regulador? La Superintendencia de Industria y Comercio (SIC) consideró que la empresa había ido demasiado lejos: ordenó **cesar la recolección y el uso obligatorio de datos biométricos para fines no estrictamente necesarios**, le recordó que los datos biométricos tienen protección reforzada por su carácter sensible y dejó claro que el consentimiento no puede ser “tómalo o déjalo” cuando se trata de acceder a servicios

básicos. El mensaje fue contundente: la innovación en seguridad no puede pasar por encima del *hábeas data* ni de los principios de necesidad y proporcionalidad.

¿Qué aprendimos? Este caso sintetiza una lección clave que recorre este libro y *El arribo de las tecnologías exponenciales*: **no toda tecnología que es técnicamente posible y comercialmente atractiva es jurídicamente legítima**. Para C-levels y equipos de producto, la pregunta no debería ser sólo “¿podemos hacerlo?”, sino “¿tenemos base legal sólida y alternativas menos intrusivas?”. Para los reguladores, el fallo refuerza la idea de que los datos biométricos merecen un tratamiento diferenciado y que las plataformas, por más innovadoras que sean, no pueden redefinir por su cuenta los límites de los derechos fundamentales.

Caso regulatorio sobre fintech vs. banco central: cuando el sandbox se convierte en ley

¿Qué pasó? Durante años, múltiples fintech en la región operaron en una zona gris: no eran bancos, pero ofrecían billeteras, cuentas prepago y servicios de pago que, en la práctica, competían con la banca tradicional. La receta inicial fue “innovar primero, regular después”: modelos como los que describimos en [“El boom del comercio electrónico”](#) y en [“La implementación de los modelos unified & collaborative commerce”](#) se apoyaban en figuras jurídicas pensadas para otro tiempo. Llegó un punto en que el regulador financiero empezó a preocuparse: riesgo sistémico, protección del usuario, prevención de lavado. La tensión “banco vs. fintech” se hizo explícita.

¿Qué decidió el regulador? En vez de optar por la prohibición o por equiparar de golpe a las fintech con bancos, algunos países —empezando por México con su Ley Fintech y seguida por experiencias en Colombia y Brasil— apostaron por **sandboxes regulatorios**: espacios controlados donde startups y grandes jugadores podían probar modelos bajo supervisión, con límites claros de tamaño, tiempo y tipo de riesgo asumido. A partir de esos pilotos, se ajustaron definiciones, se crearon categorías intermedias (instituciones de fondos de pago electrónico, sociedades de financiamiento, etc.) y **se transformó parte de la experimentación en regulación estable**.

¿Qué aprendimos? El mensaje que recorre este caso y el bloque sobre sandboxes en este libro es simple: **es mejor aprender en pequeño bajo supervisión que improvisar en grande con impacto sistémico**. Para emprendedores y C-levels, la lección es que participar activamente en estos espacios —en lugar de verlos sólo como “trabas”— ayuda a dar forma a las reglas de juego futuras. Para los reguladores, el caso muestra que el enfoque de **regulación adaptativa 4R** (riesgo, resultados, revisión, redes) funciona mejor que reaccionar a golpes de titular. Este tipo de diseños dialoga con lo que analizamos en [“El arribo de las tecnologías exponenciales”](#) sobre cómo gobernar tecnologías emergentes sin ahogar el ecosistema.

Caso regulatorio sobre influencers y publicidad encubierta: cuando “lo auténtico” se vuelve engañoso

¿Qué pasó? Con el auge de redes sociales y creadores de contenido, muchas marcas empezaron a usar

influencers como canal principal de promoción. En varios países, se multiplicaron los casos de publicaciones donde la recomendación parecía espontánea, cuando en realidad formaba parte de una campaña paga. Tal como relatamos en la sección *Publicidad y responsabilidad en redes sociales*, durante la pandemia se vieron ejemplos extremos: influencers promocionando productos “milagro” para bajar de peso, cremas sin evidencia o inversiones de alto riesgo, sin ninguna advertencia de que se trataba de publicidad.

¿Qué decidió el regulador? Aunque el marco latinoamericano avanzó de forma desigual, algunas autoridades de defensa del consumidor y organismos sectoriales comenzaron a intervenir: exigieron **identificar claramente las publicaciones patrocinadas**, sancionaron campañas por publicidad engañosa y emitieron guías sobre cómo deben etiquetarse colaboraciones pagas. En México, por ejemplo, la autoridad elaboró lineamientos específicos para influencers; en otros países se tomaron como referencia las guías de la FTC estadounidense mientras se prepara normativa local. En todos los casos, el criterio de fondo fue el mismo: el consumidor tiene derecho a saber cuándo le están vendiendo algo.

¿Qué aprendimos? Este caso conecta directamente con [“El desarrollo del Retail Media Network”](#) y con la saga #RetailReset: **cuando la frontera entre contenido y anuncio se borra, la línea entre persuasión legítima y engaño se vuelve muy fina**. Para las marcas y redes de retail media, la lección es que la transparencia no sólo evita sanciones, sino que protege el valor de la propia

audiencia. Para reguladores y cámaras empresarias, muestra la necesidad de actualizar marcos pensados para TV y radio a un entorno donde el “medio” es una persona con un smartphone y millones de seguidores. Y para los consumidores, recuerda que “lo auténtico” también puede estar guionado.

Caso regulatorio sobre IA y decisiones automatizadas: cuando los principios globales se vuelven locales

¿Qué pasó? A medida que la IA se integró en más procesos —desde scoring crediticio hasta precios dinámicos, pasando por selección de personal y moderación de contenidos— empezaron a aparecer denuncias de **sesgos, discriminación y falta de explicabilidad**. Empresas que se presentaban como innovadoras se encontraron con titulares sobre algoritmos que negaban servicios a ciertos grupos, fijaban precios distintos sin justificación clara o amplificaban desinformación. En [“El arribo de las tecnologías exponenciales”](#) describimos cómo la región fue adoptando modelos avanzados sin siempre actualizar sus capacidades de gobernanza.

¿Qué decidió el regulador? En paralelo, organismos internacionales como la OCDE y la UNESCO aprobaron principios sobre **IA confiable, explicable y centrada en derechos humanos**, y varias autoridades de datos y consumo de la región empezaron a usarlos como referencia. En lugar de esperar a una “ley de IA” integral, algunas agencias comenzaron a aplicar marcos existentes (datos, consumidor, antidiscriminación) a casos concretos de decisiones automatizadas. Se

exigieron explicaciones mínimas, se cuestionó el uso de ciertos datos para perfilar personas y se abrió la puerta a que, en el futuro, se exijan **registros de sistemas de alto riesgo**, al estilo de lo que anticipa el AI Act europeo.

¿Qué aprendimos? La lección para las organizaciones es doble. Primero: **no hay atajos regulatorios mágicos para la IA**; si un modelo decide sobre personas, está tocando derechos que ya están protegidos, aunque no exista aún una “ley de IA” con nombre y apellido. Segundo: los principios globales dejan de ser papers abstractos cuando un regulador local los cita en una resolución. Para los policy makers, este caso muestra que se puede avanzar por capas —aplicando marcos existentes mientras se diseñan leyes específicas— siempre que haya una brújula clara como la que desarrollamos en este libro y en el momentum de tecnologías exponenciales. Para el ecosistema emprendedor, el mensaje es que diseñar IA **explicable y auditable** ya no es sólo buena práctica ética: es una inversión preventiva en cumplimiento.

Brasil:

Responsabilidad de marketplaces y lucha contra la falsificación

Brasil, siendo uno de los mayores mercados digitales de la región, ha protagonizado casos clave sobre la **responsabilidad de las plataformas** por contenidos y productos ilícitos. Un ejemplo paradigmático es el reciente caso *Mercado Libre vs. A3D Chile*. Aunque ocurrido en Chile, tuvo eco en Brasil por la similitud de la cuestión jurídica:

A3D (empresa que comercializa productos para el hogar) demandó a Mercado Libre acusándolo de **competencia desleal** al permitir la venta de productos falsificados con sus marcas registradas en la plataforma.⁵³

En 2025, el 7° Juzgado Civil de Santiago rechazó la demanda, concluyendo que Mercado Libre “*no es el vendedor, distribuidor o comercializador de los productos*” en cuestión, y por tanto **no compete directamente** con A3D. El fallo estableció que los vendedores en Mercado Libre son terceros independientes y que la plataforma opera como un **marketplace puro**, que no fija condiciones de la oferta ni realiza ventas directas (Cárdenas, 2025).

Citando incluso precedentes de la Corte de Apelaciones de Santiago, se afirmó que “*Mercado Libre no es un proveedor en los términos que exige el legislador*” para responsabilidad directa, ya que no determina las condiciones comerciales ni cobra a los compradores (Cárdenas, 2025). Este razonamiento –que refleja también jurisprudencia del Superior Tribunal de Justiça (STJ) de Brasil– sienta un precedente importante: **los marketplaces no son responsables como vendedores** de los ilícitos cometidos por terceros, siempre que actúen con la diligencia debida al conocer una infracción.

No obstante, el mismo caso evidenció la expectativa de las marcas: A3D argumentó que Mercado Libre “facilita” esas ventas ilegales y desvía clientela aprovechando su posicionamiento en buscadores. Aunque el tribunal chileno negó la competencia desleal en esta instancia, A3D apeló en la búsqueda de una interpretación más

estricta. Esta tensión entre **libertad de empresa vs. protección de la propiedad intelectual** también se vivió en Brasil: inicialmente, Mercado Livre era visto como “vilão” (villano) por las autoridades antipiratería.

Richard Gantus, fiscal del Grupo Especial de Delitos Organizados de São Paulo, recordaba que hacia 2019 la plataforma era considerada un obstáculo en la lucha contra la piratería.⁵⁴ Sin embargo, en pocos años la situación dio un giro notable. Según un reportaje de *CNN Brasil*, Mercado Livre pasó de villano a aliado del Ministerio Público en el combate a la piratería (Estadão Conteúdo, 2024).

¿Qué cambió? La empresa intensificó sus esfuerzos con un **Programa de Protección de Marcas (Brand Protection Program, BPP)** inspirado en la lógica norteamericana: inicialmente, que las marcas denuncien los listados ilícitos. Pero reconociendo que ese mecanismo reactivo era lento y engorroso, Mercado Libre empezó a **buscar proactivamente anuncios sospechosos** mediante algoritmos de *machine learning* e inteligencia artificial, incluso antes de recibir denuncias (Estadão Conteúdo, 2024). El propio **Federico Deyá, Director Legal de Mercado Libre**, explica que desde 2021 invitaron a marcas estratégicas a compartir datos (por ejemplo, diseños industriales de sus productos) para entrenar a los algoritmos que detectan falsificaciones en fotos y descripciones (Estadão Conteúdo, 2024).

Esta iniciativa llamada *MACA (Mercado Libre Anti-Counterfeiting)* tuvo resultados impresionantes: “en el

*primer semestre de 2024, por cada publicación removida tras una queja en el BPP, la empresa retiró proactivamente otras 9” (Estado Conteúdo, 2024). Y con el programa avanzado de cooperación con marcas, por cada reclamo tradicional se logró remover otras 25 publicaciones de oficio (Estado Conteúdo, 2024). Gracias a este trabajo conjunto, en enero de 2024, Mercado Libre colaboró en una investigación que terminó con la incautación de **21 toneladas de bebidas adulteradas** de una marca global (Diageo).*

Este cambio de actitud, apoyado en inversiones en equipos especializados y tecnología, fue reconocido por el fiscal Encinas como un *game changer*: hoy el Ministerio Público brasileño ve a la plataforma como un **aliado clave** en la lucha contra la piratería, en una demostración de que la **autorregulación reforzada con cooperación judicial** puede tomar la delantera allí donde la ley sola no alcanza.

En síntesis, la jurisprudencia brasileña –sumada a acuerdos con autoridades– ha definido una **responsabilidad subsidiaria** para los marketplaces: no se les trata como delincuentes por los ilícitos de sus usuarios, pero sí se espera que actúen diligentemente para prevenir y reprimir abusos. Los fallos del STJ han enfatizado el “*deber de control*” razonable: si la plataforma, tras ser notificada, no remueve contenido ilegal o no implementa medidas proactivas disponibles, puede incurrir en responsabilidad.

Esta línea ha repercutido en toda la región, al dar margen a la innovación de plataformas pero en paralelo exigiendo

compromiso activo contra la ilegalidad. Como reflexiona Ludovino Lopes –abogado brasileño pionero en derecho digital–, el avance normativo en Brasil pasó también por modernizar herramientas como la **certificación y firma digital**, y por construir confianza legal en el comercio electrónico. Hoy Brasil cuenta con la LGPD (Ley General de Protección de Datos) y una jurisprudencia sólida que equilibra derechos de consumidores, titulares de datos y el dinamismo del mercado digital.

México:

Protección al consumidor digital – Profeco vs. Amazon y Mercado Libre

En México, la Procuraduría Federal del Consumidor (Profeco) ha sido protagonista en fijar límites a las plataformas en defensa de los usuarios. Un caso emblemático ocurrió a raíz de reclamos de vendedores y compradores en marketplaces. A finales de 2016, Profeco realizó un **análisis exhaustivo de los términos y condiciones** de Amazon México y Mercado Libre, y detectó decenas de cláusulas abusivas o contrarias a la Ley Federal de Protección al Consumidor.⁵⁵

Hallaron 9 violaciones en los términos de Amazon (más 19 en su acuerdo para vendedores) y 18 en Mercado Libre. Estas incluían la facultad unilateral de las plataformas para modificar servicios o políticas, retener pagos a vendedores o exigir que los litigios se resolvieran en el extranjero. En resumen, contratos desequilibrados donde las compañías “no son responsables por nada”

y aprovechan vacíos legales mientras cabildean para minimizar regulaciones.

El detonante concreto fue la queja de un vendedor, Jorge Pozo, quien llevó a conciliación (Concilianet) disputas tanto con Mercado Libre como con Amazon. En el caso de **Mercado Libre**, Pozo reclamó por servicios cobrados y no prestados (publicaciones destacadas) y por políticas que permitían cancelaciones fuera de plazo legal, lo que lo perjudicaba económicamente.

Profeco resolvió en 2015 a su favor: mediante Oficio SPSP/DGP/0101/2015, sancionó a Mercado Libre con una multa de **800.000 pesos** por violar múltiples artículos de la Ley de Protección al Consumidor (El Economista, 2017). La investigación reveló incluso que la empresa tenía registrado ante Profeco un contrato de adhesión distinto al que publicaba en su sitio, lo que indicaba una falta de transparencia contractual. Este fallo sentó el precedente de que los marketplaces deben **cumplir sus ofertas y términos**; no pueden publicitar un servicio (ej., posicionamiento premium) y luego no honrarlo, ni tener “letras chiquitas” ocultas al usuario. El principio de **veracidad y cumplimiento de oferta** quedó afianzado: si cobras por un servicio, debes prestarlo tal cual, o es una práctica abusiva.

Con **Amazon**, el vendedor enfrentó problemas mayores: la empresa le suspendió la cuenta por supuestamente exceder el 1% de órdenes con quejas (no previsto claramente en contrato) y le retuvo más de 1 millón de pesos en ingresos (Sánchez Onofre, 2017). Esto afectó su

capacidad de cumplir entregas durante el Buen Fin y generó una cascada de incumplimientos.

Pozo intentó la conciliación; Amazon se negó a un acuerdo en Concilianet, y la Profeco impuso una **multa simbólica de 6.000 pesos** a Amazon por no acreditar que había notificado debidamente al vendedor sobre ciertos reembolsos a compradores (Sánchez Onofre, 2017). Aunque la sanción fue pequeña (un apercibimiento), abrió cuatro expedientes de investigación adicionales contra el marketplace.

Más allá del monto, el mensaje fue claro: Amazon debía **mejorar sus procedimientos** de comunicación y respeto a plazos legales con vendedores, o enfrentaría mayores consecuencias. El caso evidenció además la **limitación de las multas** existentes: expertos señalaron que para gigantes con tal poder económico, muchas veces “es más fácil pagar la multa que cumplir la ley”, lo que motivó llamados a reformar la norma para elevar sanciones (por ejemplo, modificar el artículo 76 bis de la Ley para que las multas sean disuasivas).

Profeco también ha actuado del lado de los compradores en grandes eventos de comercio electrónico. Durante cada *Buen Fin* (la mayor campaña de descuentos en México), se monitorea que las tiendas en línea **respeten los precios anunciados y los tiempos de entrega**. Hubo casos en que Amazon, tras un error de precio o sobreventa, canceló pedidos o demoró entregas, y Profeco intervino para que se compensara a los consumidores. De hecho, Profeco publicó lineamientos específicos sobre comercio

electrónico e incluso creó el “*Quién es quién en la venta online*” para exhibir a empresas incumplidas.

En 2020, el Procurador Ricardo Sheffield reveló que tanto Amazon como Mercado Libre, si bien tenían cientos de quejas al año, conciliaban la mayoría a favor del consumidor (el 76–90% de casos),⁵⁶ a diferencia de plataformas extranjeras ausentes como Alibaba o eBay. Esto demuestra que, bajo escrutinio, las grandes plataformas **aceptaron cooperar con Profeco** y mejorar sus prácticas de atención al cliente, devoluciones y garantías.

Un caso notable de **publicidad engañosa y ofertas no respetadas** involucró a Amazon en 2017. Como se mencionó, Mercado Libre fue multado con \$800 mil por incumplimientos; en paralelo, **Amazon México también enfrentó sanciones**: la Profeco detectó casos donde Amazon canceló compras ya pagadas argumentando error de precio o problemas de inventario, lo cual viola el artículo 7 de la Ley de Protección al Consumidor, que obliga a respetar los términos publicitados o acordados (Sánchez Onofre, 2017).

Estas intervenciones establecieron que en México las plataformas en línea están sujetas a las **mismas obligaciones** que un proveedor tradicional: “*oferta puesta, oferta respetada*”. Si un sitio anuncia un producto a cierto precio y acepta el pago, no puede luego unilateralmente invalidarlo sin incurrir en responsabilidad.

En síntesis, los casos mexicanos realzaron el **rol proactivo de la autoridad de consumo (Profeco)** y su coordinación

con afectados para forzar cambios en los marketplaces. Tras estos precedentes, tanto Mercado Libre como Amazon ajustaron aspectos de sus términos y procesos en México. Por ejemplo, Mercado Libre actualizó sus Términos en 2016 –aunque, según periodistas, muchas observaciones de Profeco seguían pendientes– (El Economista, 2017), y Amazon empezó a detallar mejor sus políticas de suspensiones y pagos a vendedores.

Asimismo, ambas empresas –copresidentes de asociaciones de la industria (AMVO, Asociación de Internet. mx)– participaron en **códigos de buenas prácticas** para autorregularse y evitar así sanciones mayores. México demostró que una agencia de consumo activa puede lograr *en la práctica* lo que la ley escrita a veces no detalla, y empujar a las plataformas hacia mayor **transparencia, cumplimiento y equilibrio contractual** con sus usuarios.

Colombia:

Datos personales y responsabilidad de las plataformas (Linio, Rappi, Mercado Libre)

Colombia ha sido pionera en la región en la **protección de datos personales**, con una ley robusta (Ley 1581 de 2012, Habeas Data) y una autoridad activa – la Superintendencia de Industria y Comercio (SIC) –, que ha sentado jurisprudencia importante frente a las plataformas digitales. Un ejemplo reiterado es **Linio Colombia**, un marketplace de comercio electrónico

que fue sancionado *cuatro* veces por la SIC entre 2015 y 2018 por violaciones al régimen de datos personales.⁵⁷ Las multas acumuladas suman cerca de 1.000 millones de pesos colombianos (Valencia, 2018), y evidenciaron una conducta reincidente. ¿El motivo central? Linio **no respetó el derecho de los titulares a suprimir sus datos personales** cuando así lo solicitaban.

En el caso más emblemático (resolución 83.882 de 2018), la SIC comprobó que una usuaria pidió hasta **seis veces** que Linio dejara de enviarle correos publicitarios y eliminara sus datos, sin obtener respuesta efectiva (Valencia, 2018). La empresa continuó usando su información con fines de marketing, en vulneración del derecho de **habeas data** en su faceta de cancelación. La sanción en esa ocasión superó los \$350 millones (Valencia, 2018).

En su decisión, el Delegado de Datos Personales, Nelson Remolina, fue contundente: no se puede tolerar que el titular deba “rogar e insistir” para que se respeten sus derechos; tampoco es aceptable que las empresas esperen a ser sancionadas para cumplir sus obligaciones legales. Este pronunciamiento jurisprudencial dejó claro que las compañías deben implementar mecanismos sencillos y efectivos para que los usuarios **ejercen sus derechos ARCO** (acceso, rectificación, cancelación, oposición), so pena de severas consecuencias.

Otro frente ha sido el uso indebido de datos **sensibles y biométricos**. En 2025, la SIC impuso una multa histórica a **Mercado Libre Colombia** por **exigir reconocimiento facial obligatorio** a sus usuarios para acceder a sus

cuentas.⁵⁸ La sanción superó los 214 millones de pesos y se basó en que la plataforma obligaba a entregar datos biométricos (rostro) sin una justificación legal válida. Según el comunicado oficial, esto constituyó un *uso indebido de información sensible* y, además, Mercado Libre **se negó a eliminar esos datos** cuando los usuarios lo solicitaban, lo que infringía gravemente el derecho al habeas data.

La SIC ordenó inmediatamente a la compañía **cesar la recolección forzada de biometría** y ofrecer alternativas de autenticación no intrusivas. También recordó que en Colombia (como en muchas legislaciones), la recolección de datos biométricos está *prohibida por regla general*, salvo excepciones de ley y bajo estrictos criterios de necesidad y proporcionalidad. Es decir, **ninguna app o plataforma puede exigir huellas, rostro, iris, etc., sólo para crear una cuenta o prestar un servicio común** (Cifuentes Quintero, 2025).

Este fallo es un parteaguas: reafirma que los datos biométricos (hipersensibles por naturaleza) merecen la máxima protección. Además, pone en jaque la tendencia de algunas fintech o plataformas a implementar verificaciones de identidad invasivas sin base legal local. Tras la sanción, Mercado Libre anunció que implementaría métodos alternativos (OTP, 2FA, etc.) y eliminaría los datos recolectados indebidamente, con lo que marcó un precedente de **adecuación tecnológica a la normativa de privacidad**.

Colombia también sancionó a la popular plataforma de delivery **Rappi** por manejo indebido de datos. En 2022, la SIC multó a Rappi con \$1.245 millones por, entre otras cosas, **ignorar repetidamente solicitudes de usuarios para eliminar sus datos y no contar con políticas claras de tratamiento.**⁵⁹ Sumado a infracciones a deberes de calidad en el servicio, el caso de Rappi mostró que las startups disruptivas no están exentas de cumplir la ley: la SIC las vigila tanto por protección al consumidor (entregas, cobros, cláusulas abusivas) como por protección de datos.

Estos casos colombianos evidencian una **línea jurisprudencial estricta**: las plataformas deben respetar al pie de la letra los derechos de los usuarios sobre sus datos. La SIC ha desarrollado a través de resoluciones un cuerpo doctrinal que exige: consentimiento informado y explícito para datos sensibles, mecanismos sencillos de opt-out de comunicaciones, supresión inmediata de datos a pedido salvo obligación legal de conservarlos, y proporcionalidad en la recolección (sólo datos necesarios para el fin declarado). Cuando Linio no acató, fue sancionada repetidamente hasta casi el máximo legal (Valencia, 2018). De hecho, la SIC publicita estos casos como ejemplo aleccionador para todo el sector. El efecto ha sido que otras empresas han reforzado sus áreas de compliance y protección de datos.

Eugenio Sánchez, experto legal en fintech entrevistado en *eLíderes Podcast X25*, comentaba que cumplir con las normas de datos ya no es opcional sino central para cualquier emprendimiento digital:



“Si no construyes la confianza del usuario desde el día uno, cumplir la ley no te salvará después de un escándalo; pero si la incumples, con seguridad tendrás un problema con la SIC o la autoridad que sea”.



Eugenio
Sánchez

Su reflexión resume la lección: la jurisprudencia ha puesto el listón alto, y las empresas serias han de interiorizar esos principios en su **cultura corporativa** (eLideres Podcast x25, 2024).

Por último, cabe mencionar que la **Corte Constitucional de Colombia** ha respaldado esta evolución. En varias sentencias ha enfatizado el carácter fundamental del *habeas data*, e incluso derivado de él el **derecho al olvido** en ciertos contextos. Aunque Colombia no tiene una norma explícita de “derecho al olvido” como tal, la Corte ha ordenado a veces a motores de búsqueda desindexar información lesiva de datos personales, inspirada en parte por el precedente europeo (Google Spain, que veremos más adelante). Así, la interacción entre jurisprudencia local y comparada sigue enriqueciendo la protección de los usuarios colombianos frente a gigantes digitales.

Chile:

El derecho a retracto en lo digital – nuevos criterios de protección al consumidor

Chile ha vivido en años recientes un debate interesante sobre la **aplicación del derecho a retracto (devolución o desistimiento)** en el comercio electrónico, especialmente respecto de productos o servicios digitales. El *derecho de retracto* en Chile –similar a la “revocatoria de aceptación” en otras jurisdicciones– permite al consumidor **arrepentirse de una compra online dentro de 10 días** desde la recepción del producto o contratación del servicio, sin necesidad de causa, y obtener reembolso.⁶⁰ Sin embargo, la ley chilena (ley 19.496 de 1997, art. 3 bis) originalmente **excluía ciertos bienes y servicios** de este derecho, atendiendo a su naturaleza. Por ejemplo, por regulación comparada, suelen exceptuarse bienes perecederos, personalizados, prensa y, en algunos países, los contenidos digitales una vez descargados o utilizados.

El desafío fue determinar **si estos límites se aplican en la era digital**: ¿puede un consumidor retractarse de la compra de un *e-book*, un curso online o una licencia de software después de haber accedido al contenido? ¿Y qué hay de servicios digitales ya prestados? Un caso concreto llegó al Servicio Nacional del Consumidor (*SERNAC*): una empresa de cursos online se negaba a devolver el dinero a clientes que, tras inscribirse y acceder al contenido, querían ejercer el retracto alegando insatisfacción con el servicio. La empresa argumentaba que, al tratarse de

“contenido digital intangible” ya entregado, no era viable la devolución (similar a no poder “devolver” una película ya vista).

El **SERNAC**, a través de dictámenes interpretativos en 2023, abordó estas cuestiones. En una interpretación importante, aclaró que el derecho a retracto **rige para compras online de bienes y servicios**, salvo exclusiones que **deben ser reglamentadas expresamente**. Señaló que aún falta el reglamento que detalle cuáles bienes por su naturaleza pueden excluirse y cómo informar esa exclusión (Carey & Hara, 2023). Mientras ese reglamento no exista, los proveedores no pueden simplemente negarse a aceptar devoluciones invocando excepciones genéricas. De hecho, el SERNAC indicó que **corresponde al proveedor comunicar de forma previa y clara si un producto o servicio no tendrá derecho a retracto**, una vez que la reglamentación lo determine (Carey & Hara, 2023).

En la práctica, SERNAC ha sostenido que *“el consumidor podrá hacer valer el retracto en aquellos casos en que no tenga acceso al bien”*. Por ejemplo, en ventas de vestuario online: aun en tienda física, si no hay posibilidad de probar la prenda, se aplica el retracto al comprador en línea (Carey & Hara, 2023). Pero si el consumidor **ya utilizó o accedió plenamente** al bien digital, la situación es más compleja. Un **fallo relevante** del SERNAC en 2022 resolvió a favor de unos consumidores que adquirieron un programa digital de ejercicios; tras descargarlo y usarlo brevemente, pidieron retracto por insatisfacción. El proveedor se rehusó alegando que no podía “devolver” un producto digital ya copiado. El SERNAC interpretó que,

dado que la ley chilena aún no reglamenta la exclusión para bienes digitales, correspondía hacer **efectivo el retracto**, y ordenó reembolsar al consumidor. Este caso marcó precedente: hasta que la regulación lo precise, *prima el principio proconsumidor*.

Adicionalmente, en 2023, el SERNAC emitió lineamientos sobre **“retracto digital”** indicando que la simple apertura de un empaque o el *testing* razonable de un producto **no anula el derecho**. En otras palabras, un consumidor puede probar un producto (incluso instalar un software o iniciar un curso) y aún así desistir dentro del plazo si el producto no presenta deterioro imputable al consumidor (Carey & Hara, 2023). Esto extiende al mundo online el estándar del mundo físico, donde uno puede desembalar un artículo y, si no cumple expectativas, devolverlo (siempre que esté en buen estado). De igual forma, para servicios digitales ya iniciados (p.ej., una suscripción mensual), se ha tendido a permitir el retracto dentro del periodo legal, aunque con matices en la devolución proporcional si el servicio fue parcialmente prestado.

En definitiva, **Chile se encuentra actualizando su normativa de consumo para la era digital**, y la jurisprudencia administrativa del SERNAC ha llenado temporalmente el vacío. Se espera la aprobación de una reforma a la ley 19.628 (protección del consumidor), que incorpore explícitamente los derechos digitales, cree una autoridad específica y establezca **multas elevadas hasta de USD 700.000** por infracciones.⁶¹ Mientras tanto, casos emblemáticos –como el de los cursos online– han dejado la enseñanza de que las empresas deben ser

claras en sus términos desde el inicio. Si no desean ofrecer retracto en un contenido digital por razones legítimas, deberán esperar a que el reglamento lo habilite y, aun así, informar de forma **destacada y previa** esa condición al consumidor. De lo contrario, la balanza en Chile se ha inclinado a favor del usuario: ante la duda, puede **“arrepentirse”** también en las compras digitales.

Argentina:

Tributación digital – Mercado Libre, Netflix y el largo brazo fiscal de la AFIP

Argentina ha librado sus propias batallas legales en torno al comercio digital, especialmente en materia **fiscal**. Un caso icónico fue la confrontación entre **Mercado Libre y la AFIP** (Administración Federal de Ingresos Públicos) acerca de las obligaciones impositivas de la plataforma y sus usuarios. Históricamente, Mercado Libre argumentaba que, como mero intermediario, no debía responder por obligaciones fiscales de las transacciones entre terceros. Sin embargo, la AFIP buscó mecanismos para **capturar impuestos en la economía digital**, por ejemplo, requiriendo a Mercado Pago (el brazo financiero de Mercado Libre) actuar como agente de retención de IVA e impuesto a las ganancias en ciertas operaciones.

Hubo varios amparos y litigios en la década de 2010: algunas provincias pretendían gravar con Ingresos Brutos las comisiones de plataformas, y Mercado Libre litigó por la **territorialidad** de esos impuestos (dado que operaba a través de Internet sin presencia física en todas

las jurisdicciones). En líneas generales, hacia 2017-2019, la tendencia jurisprudencial dio la razón al fisco en que **las plataformas deben colaborar con la recaudación**.

Un antecedente relevante fue el llamado “**impuesto Netflix**” en la ciudad de Buenos Aires (2014). La capital estableció un régimen de retención del impuesto bruto (ingresos brutos) sobre los servicios de suscripción online (Netflix, Spotify, etc.), equivalente a un pequeño porcentaje del abono mensual.⁶² La medida fue cuestionada judicialmente por legisladores opositores, pero el Tribunal Superior de Justicia porteño la **avaló por unanimidad** en 2014. La corte local sostuvo que no había inconstitucionalidad en gravar a quienes “hacen su negocio acá”, al igual que se grava a los cableoperadores tradicionales.

En otras palabras, confirmó que los servicios digitales transnacionales pueden ser sujetos de impuestos locales, si hay consumo en la jurisdicción. Enrique Carrier, analista, acotó entonces: *“Si el cable paga Ingresos Brutos, no veo por qué no una compañía que hace su negocio acá”* (Infobae, 2014). Este fallo marcó un hito porque despejó el camino para que, pocos años después, la AFIP a nivel nacional estableciera percepciones impositivas a los servicios digitales extranjeros.

En 2018-2020, Argentina implementó el **impuesto PAIS** y percepciones del 35% a gastos en moneda extranjera, lo que incluyó abonos a Netflix, Amazon Prime, Spotify, etc.⁶³ Si bien estas medidas fiscales no pasaron por litigios de constitucionalidad al nivel de llegar a la Corte (fueron más

bien resistidas políticamente), en la práctica, consolidaron el criterio de que *“lo digital también tributa”*. Algunos usuarios judicializaron devoluciones de percepciones, pero con poco éxito.

En 2021, trascendió un fallo de la justicia federal Argentina que ordenaba a Mercado Libre **informar y embargar fondos de cuentas de sus usuarios deudores de la seguridad social**, lo que sentó otro precedente en la colaboración plataforma-fisco.⁶⁴ Y en 2022 se conoció la primera resolución judicial que **habilitó a la AFIP a embargar directamente una cuenta de Mercado Pago** de un contribuyente moroso, pese a la oposición inicial de la empresa.⁶⁵ La Cámara Federal de Mar del Plata razonó que los saldos en billeteras electrónicas son equiparables a activos embargables, y que la tecnología no puede ser refugio para la elusión. Citó “el auge de la actividad financiera a través de cuentas digitales” como motivo para interpretar las normas conforme a la realidad actual (iProfesional).

Este fallo histórico dejó en claro que no existe excepción legal que vuelva **inembargables** los fondos en plataformas como Mercado Pago; al contrario, deben cumplir la misma función de garantía frente a deudas que una cuenta bancaria tradicional. Esta jurisprudencia fue celebrada por la AFIP como un triunfo en su “embestida judicial” para sujetar la economía digital a las reglas generales.

En cuanto a la doble imposición y territorialidad –un debate de fondo–, los tribunales argentinos han seguido

en general la doctrina de la **realidad económica**: si un servicio digital es consumido en Argentina, genera base imponible aquí, aunque el proveedor esté en otro país. Asimismo, para evitar doble carga, se han articulado mecanismos de acreditación de impuestos pagos en el extranjero o regímenes simplificados para que empresas extranjeras (como Netflix) se registren y paguen IVA local. La evolución internacional (ej., los proyectos de *digital tax* de la OCDE/G20) también presiona a Argentina a actualizar su marco.

En resumen, los casos en Argentina muestran a un Estado decidido a **extender su soberanía fiscal al mundo digital** y a los jueces generalmente convalidando esa potestad, siempre que se siga el debido proceso. Mercado Libre tuvo que aceptar ser agente de retención de impuestos a las ventas de sus usuarios; Netflix y similares repasan parte de sus abonos a las arcas públicas; y los deudores ya no pueden ocultar su dinero en *fintechs* pensando que están fuera del alcance judicial.

Como observador de estos 25 años de ecommerce, suelo decir que Argentina tuvo “*déjà vu*” regulatorios: cada nueva tecnología reabre discusiones viejas (impuestos, control de capitales, etc.), pero, al final, la jurisprudencia tiende a **equiparar lo digital a lo físico** en cuanto a obligaciones. La innovación no exime de la ley: quizás se demora la adecuación normativa, pero cuando llega – sea vía ley o fallo –, termina consolidando un principio de **neutralidad tecnológica** (lo que está prohibido o gravado offline también lo está online).

Casos transversales:

La influencia del derecho comparado

El ecosistema digital es global por naturaleza, y las decisiones judiciales en una jurisdicción resuenan en otras. En Iberoamérica, muchas controversias se han alimentado de precedentes extranjeros o han seguido parámetros fijados fuera. Tres ámbitos son ilustrativos: el *derecho al olvido*, la moderación de contenidos en redes sociales, y la adopción de estándares tipo GDPR en privacidad.

El “derecho al olvido” tuvo su origen en Europa con el famoso caso *Google Spain vs. Agencia Española de Protección de Datos (AEPD)*, resuelto por el Tribunal de Justicia de la UE en 2014. En esa sentencia se reconoció que los individuos pueden solicitar a los buscadores de Internet la desindexación de resultados que contengan información personal desactualizada o irrelevante, para proteger su privacidad. Este concepto rápidamente encontró eco en Latinoamérica. Por ejemplo, en Argentina se debatió en el caso “Belén Rodríguez vs. Google” (2014) algo similar: una modelo demandó a buscadores por enlazar su nombre a sitios de contenido erótico. Si bien la Corte Suprema argentina finalmente **no consagró un derecho al olvido general** (falló a favor de Google en ese caso, salvo que se trate de contenido ilícito específico), el solo planteo mostró la influencia europea.

Años después, en 2017, un tribunal argentino sí aplicó la doctrina europea para ordenar a Google bloquear

resultados que afectaban la honra de un individuo por un hecho ocurrido hacía décadas. En México, la Suprema Corte atrajo un caso sobre derecho al olvido en 2015 (un personaje público que quería eliminar noticias de hemerotecas digitales), aunque finalmente prevaleció la libertad de expresión en ese asunto.

No obstante, **autoridades de protección de datos latinoamericanas** han incorporado la idea. La unidad de protección de datos de Colombia (SIC) ha reconocido el derecho de supresión de datos en línea cuando no cumplen con principios de veracidad o actualidad, con inspiración en Google Spain. Perú, en su reciente ley de 2021, incluyó expresamente el derecho al olvido. Brasil, en la LGPD, no lo nombra directamente pero sí prevé derechos de cancelación y oposición que se asemejan. Es decir, el principio de que “Internet no tiene por qué ser eterna para los datos personales” va ganando terreno, adaptado a los marcos locales.

[Jacobo Cohen Imach](#) señalaba que en nuestra región a veces se exagera esta noción sin adaptarla al contexto: *“Se prohíben cosas o se ponen límites cuando la gente comparte mucho más de lo que el regulador cree”* (eLíderes Podcastx25,2025), con lo que sugiere que antes de copiar tal cual conceptos europeos, hay que entender las dinámicas culturales locales (muchos usuarios latinoamericanos son voluntariamente muy abiertos en redes, por ejemplo). Aun así, la influencia del caso Google Spain ha sido notable para abrir la discusión: hoy se habla en Iberoamérica de equilibrio entre reputación digital y memoria colectiva directamente gracias a aquel hito europeo.

El segundo ámbito es la **moderación de contenido en redes sociales** y la tensión con la libertad de expresión. Aquí el referente más reciente proviene de Estados Unidos. En 2023-2024, la Suprema Corte de EE. UU. tomó el caso *NetChoice vs. Paxton* (leyes de Texas y Florida que buscaban prohibir a las plataformas eliminar contenido por razones políticas). En julio de 2024, la Corte **decidió proteger a las plataformas** bajo la Primera Enmienda, y equiparó su moderación editorial a un ejercicio propio de libertad de expresión.⁶⁶ Es decir, dictaminó que el gobierno (en este caso, los estados) *no puede obligar a las redes sociales a alojar discursos que no desean*, del mismo modo que no puede obligar a un periódico a publicar todas las cartas al director. Este fallo puso freno a la tendencia de algunos estados de EE. UU. de convertir a Facebook, X o YouTube en “plazas públicas” sin control de contenidos.

La Corte afirmó que las plataformas realizan **“control editorial” protegido** y que las leyes de Texas/Florida muy probablemente violaban la Constitución al intentar dictar cómo moderar. Si bien la decisión ordenó a cortes inferiores reexaminar con ese estándar, en la práctica dejó casi sin efecto aquellas leyes, consolidando la autonomía privada de las redes en gestionar sus comunidades.

La repercusión en Latinoamérica fue inmediata en términos de debate. En países como México, Brasil o Chile, donde han surgido propuestas para que las plataformas no puedan “censurar” contenido lícito o deban reportar sus algoritmos, el criterio de la Corte estadounidense fue citado como referente de la importancia de la

libertad de expresión online. Organizaciones como R3D en México celebraron que *“las legislaciones estatales no podrán regular la forma en que las plataformas moderan contenidos”*, por ser actividad protegida (R3D, 2024). Ahora bien, la Corte también dejó claro que esto no blinda a las Big Tech de **otro tipo de regulaciones**: mencionó explícitamente que leyes de competencia, privacidad, transparencia u otros derechos de usuarios **sí** pueden imponerse a las plataformas sin chocar con la Primera Enmienda, siempre que no interfieran con la función editorial (R3D, 2024).

Este matiz es relevante: en Latinoamérica, los fallos de EE. UU. no son vinculantes pero sí persuasivos. Así, es probable que en futuras discusiones legales, nuestras cortes consideren esta distinción: *no* se puede obligar a Twitter o Facebook a no moderar (por ejemplo, a no remover desinformación o discurso de odio), ya que eso afecta su derecho (y también el de otros usuarios) a un entorno expresivo libre. Pero *sí* se puede exigirles responsabilidades en otras áreas: combate a delitos (ej., pornografía infantil), protección de datos de usuarios, reglas antimonopolio, etc. De hecho, en 2023, Brasil aprobó una ley para que las redes sociales eliminen contenidos ilícitos graves rápidamente, inspirada en parte en estándares europeos de control de contenidos ilegales, lo cual puede coexistir con la idea de libertad editorial, siempre que ataque mensajes claramente que están al margen de la legalidad y no opiniones legítimas.

Por último, la **influencia del GDPR europeo** se ha dejado sentir fuertemente en nuestra región, con el impulso

de reformas legales y criterios de autoridades. Como señalamos, la **Ley General de Protección de Datos de Brasil (LGPD)** de 2018 fue elaborada tomando al GDPR como modelo (Banco Interamericano de Desarrollo, 2019). Introdujo principios y conceptos casi calcados: data protection officer obligatorio, alcance extraterritorial (aplica a empresas fuera de Brasil que traten datos de brasileños), categorías especiales de datos sensibles y multas de hasta un 2% de los ingresos anuales (con topes millonarios) por incumplimiento (Bojalil & Vela-Treviño, 2019).

Del mismo modo, Chile tiene un proyecto de nueva Ley de Datos que crea una agencia independiente y eleva sanciones hasta US\$700 mil, también para alinearse con GDPR (Bojalil & Vela-Treviño, 2019). Argentina, que fue el primer país latinoamericano reconocido como adecuado por la UE, trabaja en una reforma para modernizar su ley 25.326 de 2000 e incluir definiciones nuevas (datos biométricos, genéticos), portabilidad de datos y demás derechos GDPR.

México, tras una situación peculiar (el instituto INAI estuvo en riesgo de disolución en 2024), emitió en 2025 una nueva Ley Federal de Protección de Datos Personales que actualiza varios puntos para equipararse a estándares internacionales. Perú en 2021 incluyó explícitamente el derecho a la portabilidad y amplió definiciones de datos sensibles. Colombia discute extender su ley 1581 para tener alcance internacional y obligar la creación de delegados de protección de datos, siguiendo el modelo europeo (Bojalil & Vela-Treviño, 2019).

No sólo leyes: las **autoridades latinas citan al GDPR en sus decisiones**. Un ejemplo es la SIC de Colombia cuando impone sanciones por tratamientos sin consentimiento: suele referir a principios de finalidad y minimización consagrados también en GDPR. En casos de filtraciones masivas (data breaches), autoridades de Brasil o Argentina han mencionado las obligaciones de notificación y medidas de seguridad “tal como prevé el reglamento europeo”, aún si localmente no estaba detallado. Esta **ósmosis jurídica** ha elevado la vara de cumplimiento para las empresas: quienes operan en la región entienden que, aunque la multa local sea menor que la europea, pueden enfrentar igualmente acciones severas y deben adoptar *best practices* globales.

La complementariedad es innegable: las transferencias internacionales de datos requieren que Latam tenga regímenes adecuados para comerciar con la UE, lo que ha acelerado estas reformas (Bojalil & Vela-Treviño, 2019). Y en jurisprudencia, se observa que muchas resoluciones de nuestras autoridades mencionan doctrina europea (por ejemplo, la Agencia Española de Protección de Datos) como guía interpretativa.

En síntesis, los casos transversales muestran un **diálogo global de jurisprudencias**. Lo que decide Europa o EE. UU. en materia digital rápidamente alimenta argumentos y decisiones en Iberoamérica, adaptado a nuestra realidad. Esta “comunidad de precedentes” tiene un efecto democratizador del conocimiento legal: hoy un juez en Lima o Bogotá puede leer al detalle el fallo de la Corte europea sobre Google, o la sentencia de la Suprema

Corte norteamericana, y aplicarlos creativamente en su fallo local. Así, el derecho comparado se vuelve una herramienta para no reinventar la rueda y para elevar los estándares de protección de usuarios digitales.

Efecto cascada: Cómo impactan estos fallos en el ecosistema

Cada uno de los casos repasados no termina en sí mismo; produce un **efecto cascada** de cambios en políticas empresariales, conductas del mercado y futuras regulaciones. La jurisprudencia, una vez asentada, obliga a las plataformas y actores digitales a *mover sus fichas* para acomodarse al nuevo panorama.

Tras las sanciones en Brasil y Chile por falsificaciones, **los marketplaces de toda la región reforzaron sus programas antipiratería**. Mercado Libre, como vimos, pasó a la ofensiva integrando a las marcas en la detección proactiva (Estado Conteúdo, 2024). Otros marketplaces más pequeños replicaron el modelo de *notice and takedown* y muchos se unieron a la *Alianza Contra la Piratería* liderada por entidades de la industria audiovisual.⁶⁷

En términos prácticos, hoy es común que cualquier plataforma tenga botones de “Denunciar infracción” visibles, acuerdos con estudios de cine, discográficas o fabricantes para remover contenidos truchos, e incluso

colaboren con las fiscalías. Se pasó de la negación a la **tolerancia cero con la piratería**, no sólo por ética sino porque jurídicamente quedó claro que mirar hacia otro lado aumenta el riesgo de responsabilidad. Un directivo de Mercado Libre declaraba: *“Seguiremos innovando para mejorar todo lo que ya hacemos [en seguridad y confianza]”* (Ámbito, 2023), para destacar cómo los reportes de transparencia semestrales de la empresa hoy publican métricas de contenidos removidos, pedidos de autoridades atendidos (más del 90% es respondido) y eficacias de sus algoritmos (Ámbito, 2023). Esto hubiera sido impensable sin la presión de casos legales que los empujaron a esa transparencia.

Del lado de **consumidor y competencia**, después de las multas de Profeco, **las plataformas ajustaron sus términos y condiciones**. Por ejemplo, a raíz de aquel procedimiento de 2017, Mercado Libre eliminó o clarificó cláusulas abusivas: hoy su contrato en México (y otros países) ya no contiene la obligación de ir a arbitraje en sede extranjera para usuarios comunes, una crítica que se le hizo entonces (Sánchez Onofre, 2017).

Amazon, por su parte, implementó políticas de notificación a vendedores más claras y estableció ciertos umbrales en sus *dashboards* de performance para que los vendedores sepan cuándo están en riesgo de suspensión (lo que antes hacía de forma sorpresiva). Además, tanto Amazon como Mercado Libre desplegaron programas de **garantía al cliente** (Amazon A-to-Z, Mercado Libre Compra Protegida) para que ante un incumplimiento en tiempos de entrega o producto no recibido, el comprador obtenga

reembolso sin necesidad de pelear extensamente; esto en parte para atender las preocupaciones de Profeco sobre la indefensión de consumidores (Sánchez Onofre, 2017). Incluso, Profeco destacó públicamente en años recientes a Amazon y Mercado Libre como “empresas serias que sí atienden reclamos”, en contraste con otras que ni responden (Sánchez Onofre, 2017), lo cual indica una mejora en su relación con la autoridad.

Las **campañas de publicidad y marketing digital** también se volvieron más cautelosas tras fallos y sanciones. Un ejemplo es el ámbito de los **influencers** y la publicidad encubierta: luego de las multas en Perú por parte de Indecopi (caso Alejandra Baigorria y otros en 2025), muchas marcas en países vecinos tomaron nota y empezaron a exigir a sus influencers contratados que usen hashtags como #Publicidad o #Ad en sus posts.

En España, desde 2021 existe un código de autorregulación (y la ley General de Comunicación Audiovisual de 2022) que obliga a identificar la publicidad en redes; esta tendencia llegó a Iberoamérica. De hecho, Indecopi indicó que presentará una guía para creadores de contenido, y en México, la Profeco lanzó en 2023 una **guía de publicidad para influencers** con lineamientos claros y posibilidad de multas considerables a quien no los siga.⁶⁸ Vemos así cómo un caso local (Perú sancionando a seis influencers con multas de hasta 51 UIT, aproximadamente USD 65 mil)⁶⁹ repercute en toda la región: la **conciencia legal** de influencers y agencias ha aumentado, sabiendo que *lo que hacen en Instagram o TikTok está regulado* y que ya no es tierra de nadie.

Adicionalmente, **términos y condiciones, políticas de privacidad y avisos legales** en sitios web han sido revisados minuciosamente. Tras las sanciones de datos en Colombia, muchas apps en Latinoamérica incorporaron ventanas de consentimiento más explícitas, opciones de *opt-out* de reconocimiento facial o biometría (donde antes era obligatorio), y vías accesibles para que el usuario ejerza sus derechos ARCO. Incluso, startups pequeñas, asesoradas por fondos de inversión, reciben como recomendación “asegúrate de estar *compliant* con la ley de datos de Colombia/México/Brasil, porque si no, cierras deals”. Esto es un **cambio cultural** provocado en parte por ver a gigantes como Rappi o Mercado Libre penalizados: si a ellos los multaron con cifras importantes y escarnio público, ninguna empresa quiere ser “el próximo caso ejemplar”.

En el plano regulatorio, los fallos han servido de **insumo para nuevas leyes** (efecto legislativo). Por ejemplo, la jurisprudencia chilena y comparada alimentó la reciente **ley de influencers** aprobada en Francia y debatida en otros países, que podría tener ecos en América Latina con la formalización de obligaciones de transparencia en publicidad digital.

Los problemas detectados por Profeco en 2016–2017 sobre cláusulas abusivas en marketplaces se incorporaron en proyectos de reforma a la Ley de Consumidor en México (que, entre otras cosas, busca obligar al registro de contratos de adhesión de plataformas para que la autoridad pueda revisarlos previamente). Los fallos sobre retracto en Chile seguramente quedarán consolidados en

su nueva legislación proconsumidor. Y los tributos fiscales argentinos, tras los casos de percepciones y embargos fintech, impulsaron la actualización de normativas para que las definiciones de “cuenta bancaria” incluyan a las **cuentas de pago digitales**, a fin de cerrar grietas legales.

Por último, cabe destacar el impacto en las **nuevas tecnologías como IA y automatización**. Si bien este capítulo trata casos hasta el presente, las resoluciones aquí analizadas marcan una *base* sobre la cual se evaluarán las próximas innovaciones. Por ejemplo, la responsabilidad de plataformas definidas en Brasil y Chile seguramente se invocará cuando se discuta la responsabilidad por contenidos generados por usuarios con **inteligencia artificial** (*deepfakes*, etc.). Las obligaciones de transparencia publicitaria aplicarán igual si en lugar de un influencer humano es un **avatar virtual** el que promociona un producto: las reglas de autenticidad y no engaño seguirán vigentes. Del mismo modo, el reconocimiento facial forzado que sancionó la SIC en Colombia sirve de antecedente si mañana una empresa de **metaverso** pretende recolectar datos biométricos de gestos o mirada: habrá un precedente de que eso está prohibido sin consentimiento explícito y ley habilitante.

En conclusión, los fallos y casos pioneros de la región han tenido un efecto dominó positivo: **profesionalizar el ecosistema digital**. Han obligado a las empresas a subir sus estándares y a los reguladores a afinar sus herramientas. El ecosistema digital iberoamericano de 2025 es más **maduro y confiable** gracias a estos “déjà vu” legales: situaciones que inicialmente fueron

traumáticas o conflictivas, pero de las cuales se aprendió para el futuro.

La jurisprudencia de estos 25 años nos deja lecciones valiosas: *las reglas del juego pueden adaptarse sobre la marcha, pero siempre con el norte de equilibrar la innovación con la protección del usuario.* Cada caso analizado es un recordatorio de que detrás de la tecnología, hay personas y derechos que merecen ser tutelados. Y aunque la ley a veces corra detrás de la realidad, cuando finalmente actúa –ya sea vía un juez, un fiscal o una agencia–, puede cambiar esa realidad para mejor, **y moldear un futuro digital más seguro, justo y transparente.**

GENESIS
DE UN FUTURO
DIGITAL

GÉNESIS

DE UN FUTURO DIGITAL





Los desafíos del marco normativo en la era digital:

Diseñando regulaciones adaptativas y colaborativas

En Iberoamérica vivimos un **déjà vu regulatorio**: la tecnología avanza a pasos agigantados mientras las leyes llegan con retraso. Este desfase no es nuevo. Como ya lo mencioné, antes la **confianza del consumidor** era frágil porque el marco jurídico simplemente *no acompañaba* a la innovación. Con esfuerzo multisectorial, fuimos llenando esos vacíos – por ejemplo, creando códigos de buenas prácticas y convenios de protección al comprador en línea (como el acuerdo AMVO–Profeco en México en 2025 para atender publicidad engañosa, garantías y devoluciones). Cuidar al comprador digital no sólo es un deber ético sino condición para consolidar el mercado.

Hoy, la aparición de tecnologías exponenciales – **inteligencia artificial (IA) generativa, big data, blockchain, plataformas de gig economy**– está desbordando nuevamente la capacidad de respuesta de los reguladores. En muchos casos, **la regulación simplemente no llega** a tiempo. Persiste un mosaico de lagunas e inconsistencias: por ejemplo, cada país impone reglas distintas a fintech o comercio digital, lo que genera incertidumbre jurídica y fricciones para la innovación regional.

La **falta de armonización normativa** en Mercosur es un caso evidente: distintas exigencias fiscales, cambiarias y técnicas entre países dificultan la interoperabilidad de servicios digitales, lo que limita su potencial regional.⁷⁰ Algo parecido observamos en la Alianza del Pacífico, donde pese a los esfuerzos de integración, cada nación aún aplica sus propios estándares en comercio electrónico, protección de datos o firma electrónica, lo que encarece y enlentece los proyectos digitales transfronterizos.

Las cifras ilustran la urgencia de cerrar estos vacíos. Según eMarketer, **Latinoamérica es la región del mundo donde la gente pasa más tiempo en internet (más de un tercio del día)**, con lo que lidera el crecimiento del comercio electrónico y medios digitales.⁷¹ Statista proyecta incluso que las ventas en línea **prácticamente se duplicarán entre 2023 y 2028** (de aproximadamente US\$117 mil millones a más de US\$205 mil millones).⁷² Este *boom* digital representa oportunidades enormes de desarrollo, pero también expone la brecha regulatoria: nuestras políticas actuales fueron diseñadas para un mundo analógico o un internet incipiente, no para ecosistemas donde

confluyen **algoritmos autónomos, criptoactivos, datos biométricos y marketplaces globales en tiempo real**. En términos simples, estamos intentando encauzar autos de Fórmula 1 con semáforos pensados para carretas.

Diversos organismos internacionales han advertido sobre estos vacíos. La **Comisión Económica para América Latina y el Caribe (CEPAL)** señala que, sin acciones decididas, la revolución digital podría incluso ampliar las brechas existentes en la región.⁷³

Un reporte reciente del **Observatorio Regional de Comercio y Geopolítica** resume nuestra situación: la regulación latinoamericana de IA y tecnologías emergentes está aún en fase **incipiente**, con avances dispares y no lineales entre países.⁷⁴ Hemos pasado de un período de inacción o normas generales vagas a una etapa actual de **proyectos aislados** – proyectos de ley de IA en discusión, normas fintech en algunos países, actualizaciones de leyes de datos personales –, pero carecemos de un enfoque integral y coordinado. Esto genera un entorno de incertidumbre: **empresas y ciudadanos temen riesgos legales**, y a la vez, organismos multilaterales como CEPAL, OCDE o BID instan a acelerar la actualización normativa para **fomentar la innovación sin sacrificar la protección al consumidor**.

Según un informe del BID, *“sin innovación regulatoria, las innovaciones tecnológicas corren el riesgo de no desarrollarse lo suficiente o de ocurrir por fuera del alcance del regulador, con todos los riesgos que ello conlleva”*.⁷⁵ En suma, el diagnóstico es claro: **o adaptamos**

nuestros marcos o nos arriesgamos a un desarrollo digital caótico, concentrado y poco equitativo.

Principios regulatorios para un marco adaptativo y coherente: El Marco 4R

A lo largo de las últimas décadas, cada ola tecnológica —del ecommerce inicial a la economía de plataformas, de la gig economy a las cripto y ahora la IA generativa— ha expuesto la misma tensión: los marcos legales llegan tarde, reaccionan mal o se fragmentan en soluciones parciales que terminan generando más incertidumbre que confianza. Lo vimos en [“El boom del comercio electrónico”](#), cuando los primeros pioneros vendían “en modo piloto de tormenta” sin reglas claras, y lo volvemos a ver hoy con la IA razonante que analizamos en [“El arribo de las tecnologías exponenciales y la transformación del ecosistema”](#).

A partir de esos déjà vu regulatorios, y de decenas de conversaciones con reguladores, emprendedores y C-levels que recogemos en esta colección *Génesis de un Futuro Digital*, podemos sintetizar una brújula común en lo que llamo el **Marco 4R de Regulación Adaptativa**. Más que un check-list técnico, es una forma de decidir **cómo** regular, **para qué** y **con quién**, evitando caer en el péndulo entre la selva sin reglas y la sobrerregulación paralizante.

Las **4R** son:

- ❑ **Riesgo**: regular por riesgo real, no por hype ni pánico moral.

- ❑ **Resultados:** evaluar impacto y resultados concretos, no sólo cumplir procedimientos.
- ❑ **Revisión:** incorporar mecanismos de revisión y ajuste continuo (sunset clauses, pilotos, evaluaciones ex post).
- ❑ **Redes:** diseñar y aplicar la regulación en red, con diálogo público–privado y cooperación internacional.

Riesgo significa asumir que no todas las actividades digitales representan el mismo nivel de amenaza ni de impacto sistémico. En *El arribo de las tecnologías exponenciales* ya trabajamos este enfoque cuando diferenciamos entre casos de uso de IA de “bajo riesgo” (automatizar una tarea interna) y “alto riesgo” (decidir crédito, salud, acceso a derechos). Trasladado a la regulación, implica dejar de legislar por anécdota o por titular de prensa y concentrarse en **dónde está el verdadero daño posible**: datos sensibles, servicios esenciales, infraestructuras críticas, concentración de poder de mercado, manipulación de audiencias vulnerables. En lugar de “prohibir la tecnología X”, el Marco 4R empuja a preguntar: *¿qué usos concretos de esta tecnología generan un riesgo inaceptable y cuáles, bien diseñados, pueden potenciar el desarrollo?*

La segunda R, **Resultados**, dialoga con la lógica de flywheels que desarrollamos en la saga [#QuantumRetail](#) y en [“El desarrollo del Retail Media Network”](#): lo que no se mide, se degrada. Una regulación que sólo mira si se cumplieron pasos formales —llenar formularios, registrar bases de datos, publicar una política— pero no se pregunta

si bajó el fraude, si mejoró la protección al consumidor o si se expandió el acceso a servicios financieros, se queda atrapada en el teatro del cumplimiento. El enfoque por resultados obliga a los reguladores a definir **objetivos claros** (por ejemplo, reducir las estafas en canales digitales, mejorar la transparencia de los algoritmos de recomendación, aumentar la bancarización real) y a ajustar las herramientas cuando esos objetivos no se cumplen. Para el ecosistema emprendedor que describimos en [“El ecosistema emprendedor y el impulso de las nuevas iniciativas”](#), esto es clave: reglas que se obsesionan con el papel y no con el impacto terminan expulsando talento o empujándolo a la informalidad.

La tercera R, **Revisión**, es quizás la más contraintuitiva en sistemas jurídicos acostumbrados a normas largas y difíciles de cambiar. En este libro ya vimos cómo muchas leyes de la primera ola digital quedaron viejas mientras se terminaban de reglamentar, y cómo varios países empezaron a experimentar con **sandboxes regulatorios** y pilotos justamente para introducir esa flexibilidad. El Marco 4R propone institucionalizar esta lógica: que las normas críticas para el ecosistema digital vengan con **cláusulas de revisión periódica**, con evaluaciones ex post y con la posibilidad de ajustar parámetros a la luz de la evidencia. En otras palabras: pasar de regulaciones “esculpidas en piedra” a regulaciones “vivas”, que aprenden junto con el mercado, tal como hacemos en los modelos de Unified & Collaborative Commerce cuando iteramos sobre acuerdos y reglas entre retailers, marketplaces, marcas y fintechs.

La cuarta R, **Redes**, reconoce algo que recorre todos los libros de la colección: el ecosistema digital y de comercio unificado **no se gobierna en solitario**. En [“La implementación de los modelos Unified & Collaborative Commerce”](#) mostramos cómo ningún actor —ni siquiera el player dominante— puede sostener solo la experiencia del usuario; necesita construir redes de colaboración con proveedores, partners tecnológicos, cámaras, startups. En [El ecosistema emprendedor](#) vemos lo mismo desde el lado del talento: comunidades, hubs, universidades, fondos. En el plano regulatorio, la R de Redes significa pasar de un regulador que emite normas desde un silo a una **gobernanza en red**, donde participan:

- ❑ agencias de datos, consumo, competencia, banca central, fiscalidad;
- ❑ cámaras y asociaciones empresarias;
- ❑ organizaciones de consumidores y sociedad civil;
- ❑ academia y centros de investigación;
- ❑ y, cada vez más, organismos internacionales que ofrecen marcos de referencia (OCDE, ONU, BID, CEPAL, entre otros).

Trabajar en red también implica cooperar **entre países**, algo crítico en una región donde las plataformas y las cadenas de valor son, por diseño, transfronterizas. Lo vemos en la colección cuando comparamos los avances de Brasil, México, Chile o Colombia en fintech, IA o protección de datos: cuando un país intenta regular en soledad algo que opera regional o globalmente, termina

generando fricciones innecesarias o simplemente quedando irrelevante.

En síntesis, el **Marco 4R** funciona como una capa superior que ordena y da coherencia a los principios que desarrollamos en detalle a continuación —neutralidad tecnológica, proporcionalidad y enfoque basado en riesgos, agilidad y experimentación a través de sandboxes, y evidencia con cocreación multisectorial— y los conecta con el resto de *Génesis de un Futuro Digital*. En “[El arribo de las tecnologías exponenciales](#)” veíamos la necesidad de marcos flexibles para IA, blockchain y datos; en “[El desarrollo del Retail Media Network](#)”, la tensión entre monetizar la atención y respetar la privacidad; en *El ecosistema emprendedor...*, los efectos de marcos hostiles o inestables sobre la creación de valor. Aquí damos un paso más: **ofrecer a reguladores, C-levels y emprendedores una brújula simple** para no volver a cometer los mismos errores cada vez que aparece una nueva ola tecnológica.

A partir de este punto, cuando hablemos de neutralidad tecnológica, proporcionalidad basada en riesgos, sandboxes y evidencia con cocreación, podés leerlos como las cuatro caras operativas de este Marco 4R. Son los principios que separan a los países y ecosistemas que logran transformar la regulación en palanca de desarrollo de aquellos que la convierten, una vez más, en un déjà vu de oportunidades perdidas.

Frente a este panorama, la respuesta no puede ser volver a las viejas recetas de control burocrático o prohibición

indiscriminada. *La respuesta no está en más control sino en mejor gobernanza*, como suelo remarcar en foros regionales. Necesitamos **marcos regulatorios flexibles, adaptativos, basados en evidencia y en diálogo multisectorial**. ¿Qué significa esto en la práctica? En primer lugar, asumir principios rectores modernos al diseñar la regulación digital:

- **Neutralidad tecnológica:** Regular los usos y riesgos, no la tecnología en sí. Las leyes deben ser lo suficientemente generales para aplicarse a distintas soluciones tecnológicas, y evitar casarse con plataformas o modelos específicos que quedarán obsoletos. Por ejemplo, en vez de una ley para “regular plataformas de taxi por app”, promulgar normas sobre **transporte colaborativo** que alcancen a las modalidades actuales y futuras.

La OCDE y varios entes locales recomiendan consagrar este principio para garantizar un campo de juego parejo y permitir la innovación: si dos servicios plantean el mismo desafío (p. ej., seguridad del usuario), deben regirse por las mismas obligaciones, sin importar si operan vía web, smartphone o la próxima interfaz futurista. La neutralidad tecnológica evita que la ley se vuelva obsoleta al primer cambio de paradigma.

Un marco tecnológico neutral fue clave, por ejemplo, en la legislación de comercio electrónico argentina de 2004, que reconocía la equivalencia legal de un “mensaje de datos” con un documento escrito, sin importar si el mensaje venía por email, web

o cualquier medio electrónico. Esa visión amplia dio durabilidad a la norma. Hoy debemos aplicar igual filosofía a la IA, el IoT o la realidad virtual: establecer *principios funcionales* (responsabilidad, transparencia, seguridad) válidos para cualquier tecnología que ofrezca determinados servicios digitales.

□ **Proporcionalidad y enfoque basado en riesgos:**

No todas las innovaciones representan el mismo peligro; por tanto, la regulación no debe ser uniforme ni excesiva. Debemos calibrar las exigencias según el nivel de **riesgo real** que una tecnología entraña para la sociedad. Europa nos da un ejemplo inspirador con el **Reglamento de IA de la UE (AI act)**, que clasifica las aplicaciones de IA por niveles de riesgo (desde mínimo hasta inaceptable) y ajusta las obligaciones en consecuencia. Así, sistemas de “riesgo inaceptable” (p.ej., vigilancia masiva ilegítima, scoring social al estilo distópico) directamente se prohíben, mientras que las IA de *alto riesgo* (como las usadas en reclutamiento laboral o diagnósticos médicos) deberán cumplir requisitos estrictos de transparencia, trazabilidad y supervisión humana.

Latinoamérica empieza a adoptar este enfoque: Chile, por ejemplo, discute un proyecto de Ley de IA (boletín 16.821-19, 2024) que **establece criterios de riesgo** para **prohibir sistemas de IA inaceptables** y regular con distintas exigencias las demás aplicaciones (Ulloa, s.f.). Esta filosofía de proporcionalidad tiene que permear todo nuevo marco: desde la protección del consumidor digital (no es lo mismo un retraso logístico que una filtración

masiva de datos personales) hasta la supervisión de fintech (diferenciando un monedero digital de una criptobolsa compleja). Regular *mejor* no es regular más sino **regular con bisturí y no con mazo**.

□ **Agilidad y experimentación (sandbox regulatorios):**

Dado que las leyes tardan en debatirse y aprobarse, es vital contar con mecanismos dinámicos que permitan probar innovaciones bajo supervisión sin esperar la ley perfecta. Aquí brillan los sandboxes regulatorios, entornos de prueba controlados donde startups o empresas pueden operar temporalmente al margen de ciertas regulaciones, con autorización del regulador, para testar nuevos modelos de negocio.

Esta herramienta ya ha dado frutos en el ámbito financiero: Reino Unido fue pionero con su sandbox fintech en 2016, y hoy países de la región la han adoptado. *México* incorporó un sandbox en su Ley Fintech (2018) y **Colombia** creó el suyo por decreto en 2020, para complementar su esquema de supervisión innovadora.⁷⁶ ¿El resultado? La experimentación de decenas de proyectos (pagos digitales, créditos online, cryptoactivos) en condiciones reales pero acotadas, cuyos aprendizajes luego nutrieron regulaciones formales.

Eugenio Sánchez insiste, durante la entrevista para el *Líderes Podcast x25*, en que esta flexibilidad legal es fundamental: sin espacios para equivocarse y ajustar, corremos el riesgo de ahogar la innovación o, peor, que florezca en la informalidad. Los *sandboxes* son un ganar-ganar: las empresas innovan más rápido y las autoridades absorben conocimiento de

punta para diseñar normas efectivas. El BID destaca que herramientas como *sandbox*, *innovation hubs* y mesas de innovación permiten encauzar la tecnología financiera a la velocidad necesaria (Bijkerk, 2021). La sinergia que se logra: regulatorios tradicionalmente adversos al riesgo pudieron ver de primera mano cómo operaba, por ejemplo, una plataforma de préstamos P2P, e identificar riesgos reales vs. temores infundados, y ajustar las condiciones sobre la marcha.

- **Evidencia y cocreación multisectorial:** Un principio rector es **legislar basado en datos y diálogo**, no en intuiciones ni presiones unilaterales. La velocidad tecnológica exige que gobierno, industria, academia y sociedad civil trabajen juntos para entender fenómenos nuevos y consensuar respuestas. *Ningún actor puede transformar por sí solo un ecosistema tan complejo.* En Europa, esto se ha logrado en parte a través de consultas públicas amplias para la DSA/DMA y la coordinación en organismos como el European AI Alliance.

En nuestra región debemos institucionalizar esas instancias: consejos consultivos de transformación digital, observatorios participativos y consulta temprana a expertos antes de regular una tecnología. **Alejandro Prince**, pionero analista digital, me recalca en su entrevista que regular tecnologías exponenciales demanda una **“lógica adaptativa y contextual”**, casi caso por caso, con sentido común.



“No se puede hacer una ley para algo que todavía no se sabe cómo va a funcionar. Hay que regular caso por caso, con sentido común y contexto”.



Alejandro
Prince

Apunta, justamente, a la necesidad de involucrar a los conocedores de cada tema en la elaboración normativa. Esto liga con la idea de **sandbox** antes mencionada y con la creación de **laboratorios regulatorios** permanentes, donde autoridad y sector privado exploren tendencias (tal como sugirió **Eugenio Sánchez** en relación con ecommerce en Colombia). Además, un enfoque basado en evidencia implica revisar las normas una vez implementadas: ¿están logrando el objetivo? ¿han generado efectos adversos? La adaptabilidad significa no esculpir la ley en piedra, sino monitorearla y ajustarla dinámicamente según los datos. Este ciclo de mejora continua es quizás uno de los mayores desafíos culturales para nuestros legisladores, acostumbrados a promulgar y pasar página.

Estos principios –neutralidad tecnológica, proporcionalidad por riesgo, experimentación flexible y co-creación basada en evidencia– sientan las bases de un **marco normativo moderno**, capaz de **acompañarse al cambio tecnológico en lugar de perseguirlo a la distancia**. En definitiva, **regular no es reprimir; es habilitar de forma segura y justa**. Dicho esto, llevarlos a la práctica

requiere abordar concretamente una serie de **temas emergentes** donde hoy la falta de reglas claras o consensos éticos es más evidente. A continuación profundizo en aquellos que considero más críticos en el ecosistema digital iberoamericano actual, integrando visiones de expertos que entrevisté en el marco de *Génesis de un Futuro Digital*.

Del riesgo regulatorio al P&L: **Risk–impact canvas regulatorio**

El error clásico —en Iberoamérica y fuera de ella— es mirar el riesgo regulatorio como un asunto reservado a abogados, lobistas y estudios especializados. Se lo trata como un “costo hundido” inevitable o, peor, como una variable externa sobre la que el negocio no tiene mucho para hacer salvo reaccionar cuando llega una sanción o un cambio de norma. En la práctica, eso significa que la mayoría de los comités ejecutivos **no ve el riesgo regulatorio en el mismo tablero** donde se discute ingresos, margen, crecimiento, talento o reputación.

En varios libros de la colección *Génesis de un Futuro Digital* —especialmente en [“El arribo de las tecnologías exponenciales y la transformación del ecosistema”](#) y en la saga *#QuantumRetail*— propongo el **Risk–Impact Canvas** como forma de obligarnos a conectar los riesgos estratégicos con el P&L y con el flywheel del negocio. Aquí llevamos esa idea al terreno regulatorio y legal, construyendo un **risk–impact canvas regulatorio** que ponga en la misma hoja:

- En las **columnas**, los grandes tipos de riesgo que atraviesan al ecosistema digital.
- En las **filas**, los impactos concretos que esos riesgos pueden tener en la operación y en la cuenta de resultados.

Una versión simple del canvas puede trabajar con ocho tipos de riesgo:

- **Riesgo legal** (contratos, T&Cs, litigios individuales).
- **Riesgo regulatorio** (cambios de normas, licencias, requerimientos de autoridades).
- **Riesgo de datos y privacidad** (brechas, tratamientos ilegítimos, uso indebido de perfiles).
- **Riesgo de IA y algoritmos** (sesgos, opacidad, decisiones automatizadas sin supervisión).
- **Riesgo fiscal y tributario** (impuestos digitales, retenciones, sanciones por incumplimiento).
- **Riesgo laboral y de gig economy** (recalificación de vínculos, cargas sociales retroactivas).
- **Riesgo de competencia y plataformas** (abuso de posición dominante, auto-preferencia, paridad).
- **Riesgo reputacional** (crisis de confianza, boicots, pérdida de licencia social para operar).

Y con seis impactos clave en las filas:

- **Ingresos** (ventas, facturación, take rate).

- ❑ **Margen** (costos adicionales, multas, indemnizaciones).
- ❑ **Crecimiento** (posibilidad de escalar o entrar a nuevos mercados).
- ❑ **Licencias y permisos** (autorizaciones para operar, acceso a infraestructuras críticas).
- ❑ **Talento** (capacidad para atraer y retener equipos clave).
- ❑ **Reputación** (confianza de consumidores, proveedores, inversores, reguladores).

La idea es muy sencilla: en cada casillero del canvas, el equipo directivo se pregunta “**¿cómo podría pegarme este tipo de riesgo en este tipo de impacto?**”. Por ejemplo:

- ❑ ¿Qué pasaría con mis **ingresos** si un cambio fiscal digital obliga a retener un porcentaje mayor en origen o si pierdo la exención de IVA para cierto servicio?
- ❑ ¿Cómo afectaría mi **margen** una sanción por mal manejo de datos personales o una obligación de reembolsos masivos a consumidores que hoy no tengo contemplada?
- ❑ ¿Qué implica para mi **crecimiento** una nueva norma de licenciamiento fintech, o la obligación de operar bajo un esquema regulatorio bancario más pesado?
- ❑ ¿Cómo incide en mi **reputación** un caso de discriminación algorítmica en precios o en acceso a crédito, o una polémica pública por campañas de retail media mal etiquetadas?

En “[El boom del comercio electrónico](#)” se ven con claridad muchos de estos impactos en estado “prehistórico”: compañías que crecieron rápido sin dimensionar su exposición y luego tuvieron que frenar, reconfigurar o pagar el aprendizaje con multas y pérdida de confianza. En *El desarrollo del Retail Media Network* mostramos la otra cara: cómo un marco regulatorio claro y bien gestionado puede habilitar nuevos modelos de monetización sobre datos y audiencias sin dinamitar la confianza del consumidor ni del regulador.

El valor del **risk–impact canvas regulatorio** es que obliga a todos los actores relevantes —no sólo al director legal o al área de cumplimiento— a **poner el riesgo sobre la mesa del negocio**. Lo ideal es completarlo en una sesión donde participen:

- ☐ Alguien de **finanzas** (P&L, estructura de costos, cash flow).
- ☐ Alguien de **producto y tecnología** (cómo funcionan realmente las plataformas, datos y algoritmos).
- ☐ Alguien de **operaciones y experiencia de cliente** (qué promete y entrega la marca).
- ☐ Alguien de **legal / compliance / asuntos públicos**.
- ☐ Y, cuando existe, alguien de **datos e IA** (CDO, CAIO, IA-unificada como “súper agente” interno).

En la práctica, el ejercicio suele revelar dos cosas:

- 1. Asimetrías de percepción:** para legal, el riesgo de

datos está en nivel rojo; para producto, todavía en amarillo; para finanzas, ni figura. Lo mismo con IA, fiscalidad o gig economy. El canvas ayuda a que afloren esas diferencias y se discutan con datos, no con intuiciones sueltas.

- 2. Puntos ciegos:** áreas donde el impacto potencial es enorme pero nadie lo está mirando en serio. Es común que IA y algoritmos aparezcan aquí: todavía no hay grandes casos locales, pero el cruce con datos, crédito, scoring o fijación de precios puede explotar de un día para el otro.

Este enfoque se integra de manera natural con otros marcos de la colección:

- ❑ Con el **data trust flywheel** que desarrollamos en [“El arribo de las tecnologías exponenciales y la transformación del ecosistema”](#): sin una gestión consciente del riesgo regulatorio en torno a datos, el flywheel se frena o incluso se revierte.
- ❑ Con el **flywheel retail 4.0** de la saga #QuantumRetail: cualquier impacto fuerte en cumplimiento, fiscalidad o reputación puede cortar el flujo entre adquisición, recurrencia y recomendación.
- ❑ Con los análisis de **ecosistema emprendedor** de [“El ecosistema emprendedor y el impulso de las nuevas iniciativas”](#): para una startup en etapa temprana, un error regulatorio puede significar no sólo una multa, sino la imposibilidad de levantar capital o entrar a un mercado clave.

La otra gran ventaja del canvas es que sirve como **punto directo hacia IA-unificada y human augmented AI**. Una vez que la organización tiene claro qué tipos de riesgo le preocupan más y dónde podrían pegar más fuerte, puede preguntarse:

- ❑ ¿En qué casilleros del canvas tiene sentido desplegar sensores de IA-Unificada para monitorear cambios normativos, tendencias de casos o señales tempranas de conflicto?
- ❑ ¿Qué tareas rutinarias de análisis documental, monitoreo de boletines oficiales o seguimiento de jurisprudencia puede asumir un coprocesador de IA, liberando tiempo del equipo humano para las decisiones de criterio?
- ❑ ¿Dónde conviene usar IA para simular escenarios (“¿qué pasa con mi P&L si aparece tal impuesto digital o tal requisito de licencia?”) antes de que el cambio ocurra?

La intención no es “automatizar el riesgo regulatorio”, sino **convertirlo en material de trabajo cotidiano para equipos aumentados por IA**. En lugar de aparecer como un shock exógeno que obliga a improvisar, el riesgo se vuelve un factor modelado, discutido y anticipado con tiempo.

En términos prácticos, un primer paso razonable para cualquier organización que opera en el ecosistema digital es dedicar una jornada de trabajo —como las que describimos en [“La implementación de los modelos unified & collaborative commerce”](#) cuando hablamos

de comités de estrategia omnicanal— a completar este Risk-Impact Canvas regulatorio con los principales referentes internos y, si es posible, con la participación de cámaras empresarias u otros actores del ecosistema. Esa conversación suele ser más valiosa que cualquier informe aislado: ordena prioridades, revela tensiones y, sobre todo, ayuda a alinear la **agenda regulatoria** con la **agenda de negocio**.

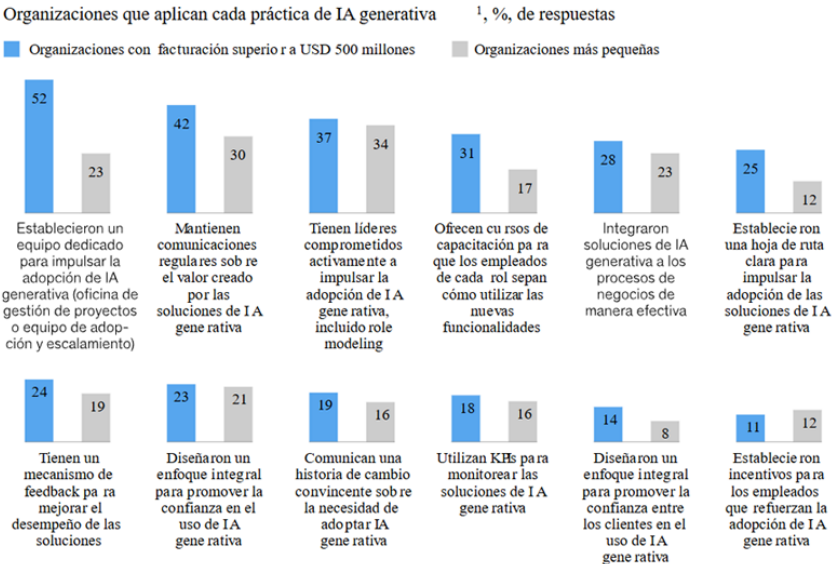
A partir de ahí, completar el canvas una vez al año, o actualizarlo cuando haya cambios regulatorios significativos, se vuelve parte natural del ciclo de planificación estratégica. Y el libro que estás leyendo —en diálogo con el resto de *Génesis de un Futuro Digital*— pasa de ser una radiografía del caos normativo a convertirse en una **plantilla de trabajo** para navegarlo con criterio, datos y futuro compartido.

Emergentes disruptivos: IA generativa, algoritmos y nuevos riesgos digitales. La inteligencia artificial generativa (IA) ha irrumpido como quizás el tema más desafiante de 2023-2025. Su capacidad para crear texto, imágenes, videos y decidir en fracciones de segundo plantea dilemas que hasta hace poco eran ciencia ficción jurídica.

Enrique Dans, experto español en transformación digital, suele decir que estamos ante “*una nueva capa tectónica*” del ecosistema digital, llamada a reconfigurar interfaces, negocios y la forma misma de tomar decisiones. Los datos confirman la rápida adopción: según McKinsey, el **78% de las organizaciones globales ya utiliza IA en al menos**

una función de negocio en 2024, comparado con un 55% apenas un año antes.⁷⁷ Y más del 70% ha incorporado herramientas de **IA generativa** regularmente en áreas como marketing, servicio al cliente o software.

Las organizaciones más grandes aplican más prácticas de adopción y escalamiento de IA generativa que las más pequeñas



¹Solo se preguntó a los participantes cuyas organizaciones usan IA en al menos una función de negocios. Las cifras se calcularon luego de eliminar las respuestas "no sabe". No se muestran las respuestas "ninguna de las anteriores".
Fuente: Encuesta Global de McKinsey sobre el Estado de la IA, 1.491 participantes de todos los niveles organizacionales, 16-31 de julio de 2024.

McKinsey & Company

Figura. Prácticas de adopción y escalamiento de IA generativa según tamaño de organización (2024). Las empresas con facturación superior a USD 500 millones aplican más prácticas sistemáticas de adopción de IA generativa que las organizaciones más pequeñas, especialmente en liderazgo, capacitación, integración tecnológica y monitoreo de desempeño. Fuente: McKinsey & Company, Encuesta Global sobre el Estado de la IA, julio de 2024.

Este salto exponencial en uso ha encendido alarmas: casi la mitad de las empresas reportó ya algún incidente negativo por IA, desde errores hasta brechas de seguridad

(Singla *et al.*, 2025). **¿Cómo diseñar un marco que potencie los beneficios de la IA generativa (eficiencia, personalización, nuevos productos) y minimice sus riesgos (sesgos, desinformación, desempleo, opacidad)?**

IA-Unificada como radar regulatorio y traductor del caos normativo

En otros libros de la colección *Génesis de un Futuro Digital* introduje la idea de **IA-Unificada**: una capa de inteligencia que orquesta modelos, datos y reglas de negocio para ayudar a equipos humanos a tomar mejores decisiones. En [“El arribo de las tecnologías exponenciales y la transformación del ecosistema”](#) la usamos para explicar cómo integrar IA, datos y automatización en la operación diaria. Aquí damos un paso más: miramos a la IA-Unificada como un **radar de cambios normativos** y un traductor del caos regulatorio al lenguaje del comité ejecutivo.

El problema de fondo es simple: el volumen y la velocidad de cambios regulatorios que afectan al ecosistema digital ya son **humanamente imposibles de seguir** con métodos tradicionales. Boletines oficiales, proyectos de ley, consultas públicas, fallos judiciales, guías de autoridades de datos y consumo, normas fiscales, lineamientos sobre IA y plataformas, cada semana se suman piezas nuevas, dispersas en diferentes fuentes y países. En [“El boom del comercio electrónico”](#) vimos cómo, en la primera etapa del ecommerce, muchos pioneros aprendían “a los golpes” porque no tenían marcos claros ni alertas

tempranas. Hoy ya no podemos darnos ese lujo.

Una arquitectura de **IA-Unificada en modo radar regulatorio** puede cumplir al menos cuatro funciones críticas:

1. Monitorear y recolectar señales

La IA rastrea de forma continua fuentes públicas relevantes: boletines oficiales, sitios de reguladores (datos, consumo, competencia, banco central, fiscos), diarios oficiales de tribunales, portales de transparencia legislativa, comunicados de organismos multilaterales. No reemplaza el criterio de qué mirar: se entrena, junto con el equipo humano, para priorizar temas vinculados al modelo de negocio (comercio electrónico, fintech, retail media, IA, economía de plataformas, etc.) que describimos en este libro y en *momentums* como [“La implementación de los modelos Unified & Collaborative Commerce”](#) y [“El desarrollo del Retail Media Network”](#).

2. Clasificar por tema, jurisdicción y tipo de riesgo

Cada nueva pieza (proyecto de ley, fallo, circular, guía, consulta) se etiqueta automáticamente según:

- Ámbito (datos, consumidor, fiscal, pagos, laboral, competencia, IA, contenidos).
- Jurisdicción (país/región).
- Grado de madurez (idea, borrador, proyecto avanzado, norma vigente, caso aislado, tendencia jurisprudencial).

- Tipo de riesgo (legal, regulatorio, reputacional, de modelo de negocio). Esta clasificación conversa de forma directa con el **radar de riesgos regulatorios 0–5** y con el **risk–impact canvas regulatorio** que proponemos en este mismo libro: la IA-unificada no “decide”, pero ayuda a ubicar rápidamente cada novedad en el mapa que ya construyó el equipo.

3. Traducir el lenguaje legal al lenguaje de negocio

Un desafío central —que aparece en las entrevistas recogidas en [“El desarrollo del Retail Media Network”](#) y en los análisis de [“El ecosistema emprendedor y el impulso de las nuevas iniciativas”](#)— es que los textos normativos suelen ser crípticos para quien no es abogado. La IA-unificada puede generar, para cada cambio relevante, **fichas ejecutivas** adaptadas a distintos perfiles:

- Para el C-level: “¿qué cambia en el modelo?, ¿qué riesgos suben o bajan?, ¿qué decisiones hay que evaluar en los próximos 90 días?”.
- Para producto: “impacto sobre diseño de funcionalidades, journeys o flujos de datos”.
- Para legal/compliance: “¿cómo se conecta con la normativa existente?, ¿dónde hay dudas de interpretación?”.
- Para asuntos públicos: “¿qué actores impulsan este cambio?, ¿en qué etapa está?, ¿qué oportunidades hay de dialogar o proponer ajustes?”. No se trata de que la IA “haga de abogado”, sino

de que prepare el terreno para que el tiempo del especialista humano se concentre en el análisis fino y la estrategia, no en tareas repetitivas de lectura y resumen.

4. Simular escenarios y cruzarlos con el P&L

En la medida en que conectamos este radar con los datos del negocio —algo que trabajamos extensamente en *El arribo de las tecnologías exponenciales* y en la saga *#QuantumRetail*— la IA-Unificada puede ayudar a simular escenarios:

- ¿Qué pasaría con nuestros márgenes si tal impuesto digital se generaliza a todos los servicios que ofrecemos?
- ¿Qué implica, en términos de ingresos y recurrencia, una obligación de cambios en políticas de devoluciones o en cargas de prueba frente a reclamos de consumidores?
- ¿Cómo afectaría nuestro negocio un régimen más estricto de consentimiento para el uso de datos en retail media?

5. Estas simulaciones no reemplazan modelos financieros detallados, pero ofrecen **órdenes de magnitud** y direcciones de cambio que permiten priorizar con tiempo ajustes de producto, de procesos y de relaciones con stakeholders regulatorios.

En conjunto, IA-unificada puede verse como un **sistema nervioso regulatorio** de la organización. No “decide” si

una norma es buena o mala, ni se pronuncia sobre su constitucionalidad. Lo que hace es:

- ❑ Reducir el ruido.
- ❑ Mostrar patrones.
- ❑ Poner sobre la mesa, de manera oportuna, la información que el comité ejecutivo necesita para conectar regulaciones con modelos de negocio.

Hay, por supuesto, condiciones para que este enfoque funcione:

- ❑ **Gobernanza clara:** alguien tiene que ser dueño del radar (legal/compliance, asuntos públicos, un comité de riesgo), definir qué se monitorea, cómo se prioriza y cómo se integran las alertas al ciclo de decisión.
- ❑ **Datos confiables:** las fuentes a las que se conecta la IA-unificada deben ser oficiales o tener calidad suficiente; las salidas se validan con humanos, especialmente en temas sensibles.
- ❑ **Transparencia interna:** los resúmenes y alertas deben estar disponibles de forma transversal, no sólo en un silo jurídico; el riesgo regulatorio es un tema de negocio, no sólo de áreas “back-office”.
- ❑ **Capacitación en human augmented AI:** los equipos que usan el radar necesitan desarrollar habilidades para trabajar con estos copilotos, algo que cruzamos a lo largo de la colección, desde el uso de IA en analytics hasta su rol en experiencia del cliente y retail media.

Desde la perspectiva de los reguladores, lo interesante es que esta misma lógica puede jugar a favor de una **regulación adaptativa y basada en evidencia**. Un país que adopta el **marco 4R** que proponemos en este libro —riesgo, resultados, revisión, redes— puede valerse de sistemas de IA-Unificada para:

- ❑ Monitorear el cumplimiento real de normas.
- ❑ Detectar efectos no deseados.
- ❑ Identificar sectores que se quedan fuera de los beneficios de la regulación.
- ❑ Ajustar con mayor precisión los instrumentos (sandboxes, guías, reformas) para no ahogar innovación ni dejar desprotegidos a los usuarios.

En síntesis, la IA-unificada entendida como **radar regulatorio** no es un gadget futurista, sino la extensión natural de la lógica que venimos construyendo en toda la colección *Génesis de un Futuro Digital*: usar tecnologías exponenciales para **aumentar la capacidad humana de leer el contexto, anticipar escenarios y decidir con criterio**. En un mundo donde el caos normativo parece la norma, este tipo de copilotos puede marcar la diferencia entre organizaciones que viven apagando incendios y aquellas que participan activamente en el diseño del futuro marco de juego.

Una primera arista son los **sesgos algorítmicos y la equidad**. Los algoritmos aprenden de datos históricos y **pueden reproducir prejuicios** de género, raza o clase presentes en esos datos. Sin supervisión, esto conlleva

discriminación en decisiones automatizadas: **a quién se le otorga un crédito, qué candidato es filtrado en un proceso de selección, o incluso qué información ve un usuario en redes sociales.**

Ya hemos visto casos reales preocupantes: sistemas de IA rechazando desproporcionadamente solicitudes de mujeres a ciertos empleos, motores de recomendación mostrando productos más caros según el perfil socioeconómico del visitante, o chatbots que “alucinan” contenido tóxico. La **ética de IA** demanda que incorporemos barreras a estos sesgos. Chile, por ejemplo, trabaja en políticas de IA *inclusiva*: ha conformado consejos asesores interdisciplinarios para asegurar datasets diversos y libres de prejuicios en el *machine learning*, y promueve auditorías algorítmicas regulares.

A nivel global, la **Declaración de Nueva Delhi del G20 (2023)** –suscrita también por Argentina, Brasil y México– enfatiza abordar los sesgos y asegurar transparencia y rendición de cuentas en IA (Ulloa, s.f.). Nuestra región se ha alineado con principios internacionales: países latinoamericanos miembros de la OCDE (Argentina, Brasil, Colombia, etc.) adoptaron en 2019 los **Principios de IA de la OCDE**, que priorizan transparencia, seguridad y respeto a derechos humanos en el desarrollo de IA (Ulloa, s.f.). Y UNESCO ha desplegado desde 2023 su programa de asesoría para implementar su **Recomendación de Ética de la IA (2021)** en más de 50 países, incluyendo varios de la región (Ulloa, s.f.).

Todo esto apunta a un consenso incipiente: **la IA debe ser justa, explicable y centrada en el ser humano**. El desafío es llevar esos principios a obligaciones concretas. En Europa, la AI act exigirá que sistemas de *alto riesgo* demuestren evaluación de impacto algorítmico, mitigación de sesgos y “*explicabilidad*” de sus decisiones. Varios países latinoamericanos ya impulsan la regulación de IA con este enfoque de **proteger derechos humanos e integrar estándares éticos en el diseño**. Es alentador ver estos avances: significa que entendimos la lección de la web 2.0 (donde la autorregulación *laissez-faire* de las plataformas derivó en abusos). Ahora se busca una **IA centrada en valores**, que incorpore desde su concepción la no discriminación y la transparencia.

Otra preocupación emergente es la “**caja negra**” **algorítmica**: muchos sistemas de IA son opacos; ni los mismos creadores pueden explicar con facilidad por qué el algoritmo tomó tal decisión. Esto es inaceptable en ámbitos sensibles. *Los consumidores, reguladores y empresas piden saber cómo decide un algoritmo*, especialmente si afecta sus derechos. Por eso, se avanza hacia el **derecho a la explicabilidad**. La Unión Europea lo incluye en la AI act y también en su **Ley de Servicios Digitales (DSA)**, para algoritmos de recomendación en plataformas grandes.

Ya se discute exigir “*etiquetas*” o informes de impacto para algoritmos que seleccionan contenido o determinan precios. *En lo personal*, creo que la transparencia algorítmica será tan crucial en esta década como la transparencia financiera lo fue en las pasadas. **Verónica**

Pinazo, Board Member de YPO y experta argentina, señalaba en nuestra conversación que la verdadera promesa de la IA sólo se alcanzará *“garantizando la calidad de los datos que la alimentan y su normatización; sin estructuras sólidas, será imposible extraer valor real”*.

Esto implica estandarizar cómo documentamos los conjuntos de datos, cómo auditamos los modelos y cómo los integramos en procesos de negocio. Pinazo ve la IA como *“una ola súper disruptiva, con mucho potencial y también amenazas”*, y enfatiza que nuestra generación tiene la responsabilidad de sentar las bases para encauzarla. Coincido plenamente: nos toca definir **estándares de gobernanza de datos y algoritmos** ahora, antes de que la IA permee cada rincón (como de hecho lo hará). Ese es quizás el rol más importante del regulador en la era de la IA: *no frenar la innovación sino **garantizar que se desarrolle sobre cimientos de calidad, ética y transparencia.***

Junto a la IA llega la necesidad de proteger a un nuevo sujeto: el **consumidor algorítmico**. Me refiero al usuario/ciudadano cuyas decisiones de consumo, información o incluso voto están cada vez más moldeadas por algoritmos. ¿Cómo aseguramos sus **derechos** en entornos automatizados? Aquí convergen varias áreas: defensa del consumidor tradicional, protección de datos personales, no discriminación y hasta derecho a la información.

Ya se plantea, por ejemplo, el derecho del consumidor a *no ser perfilado sin consentimiento* o a recibir una

explicación cuando un precio dinámico varía en función de sus datos. En la Unión Europea, la **Ley de Servicios Digitales (DSA)** obliga a grandes plataformas a permitir al usuario optar por feeds no personalizados y a explicar con criterios comprensibles las lógicas de recomendación.⁷⁸ Este tipo de medidas habrá que adaptarlas localmente.

También surgen iniciativas de “**protección del consumidor en línea**” en foros regionales: la Alianza del Pacífico, por ejemplo, en su Hoja de Ruta de Mercado Digital Regional propone el **reconocimiento mutuo de leyes de protección al consumidor en comercio electrónico**, mecanismos de resolución de disputas transfronterizas y combatir prácticas engañosas digitales.⁷⁹

En Iberoamérica, autoridades de defensa del consumidor empiezan a coordinar esfuerzos para vigilar publicidad dirigida, cláusulas abusivas en plataformas y otros posibles abusos algorítmicos. Un caso concreto: en 2025, agencias de consumo de varios países latinoamericanos investigaron conjuntamente a aplicaciones de delivery por sus sistemas de propinas y asignación de pedidos, ante denuncias de trato desigual a repartidores y falta de claridad a usuarios. Esto demuestra que el **enfoque basado en riesgos** debe permear también la protección al consumidor: priorizar la supervisión de aquellos algoritmos cuyo impacto potencial sobre usuarios sea mayor (finanzas, salud, educación, movilidad). La **tecnoética** ya no es un lujo académico; es una necesidad práctica para garantizar que el consumidor digital no quede indefenso ante cajas negras.

Equipos legales en modo **human augmented AI**

Así como en otros libros de esta colección hablo de equipos comerciales, de producto y de operaciones aumentados por IA, aquí el protagonista es otro: el **equipo legal y de cumplimiento en modo human augmented AI**. Si hay un área que está desbordada por el volumen, la complejidad y la fragmentación del entorno normativo, es justamente la jurídica. Y, paradójicamente, es una de las que más puede beneficiarse de trabajar con copilotos inteligentes.

Imaginemos a una directora jurídica (GC) de una compañía que opera en varios países de Iberoamérica. Su equipo debe seguir, al mismo tiempo, cambios en regulaciones de datos personales, normas de defensa del consumidor digital, criterios fiscales sobre servicios digitales, reglas de medios de pago, jurisprudencia sobre marketplaces y ahora, además, lineamientos sobre IA, algoritmos y decisiones automatizadas. En *El boom del comercio electrónico* vemos cómo, en la primera ola, muchos GC vivieron este recorrido en modo reactivo: llegaban las multas o las noticias de prensa, y recién entonces el tema escalaba al comité ejecutivo. Hoy la escala del problema ya no permite ese lujo.

En [“El arribo de las tecnologías exponenciales y la transformación del ecosistema”](#) propuse un modelo de **human augmented AI** donde la IA no reemplaza equipos humanos sino que amplifica su capacidad de procesar

información, explorar escenarios y decidir con criterio. Trasladado al mundo jurídico, esto implica imaginar **equipos legales aumentados**, donde:

- ❑ Una IA está entrenada en la **jurisprudencia local y regional** relevante para el modelo de negocio.
- ❑ Comprende el **corpus de contratos, T&Cs, políticas internas y dictámenes** de la propia organización.
- ❑ Tiene mapeadas las **regulaciones sectoriales clave** (datos, fintech, consumo, competencia, laboral, plataformas, IA).
- ❑ Se conecta con fuentes públicas para actualizarse cuando aparece una nueva ley, guía o fallo relevante.

El trabajo del GC y de su equipo deja de ser leer PDFs infinitos y empezar siempre desde cero, para pasar a ser **orquestar y validar** el trabajo de este coprocesador de IA: pedirle síntesis comparadas, verificar riesgos, pedir escenarios de impacto y, sobre todo, traducir esos insumos en decisiones estratégicas para el negocio.

En términos prácticos, un equipo legal en modo **human augmented AI** puede apoyarse en la IA para al menos cinco tipos de tareas:

1. **Lectura masiva y síntesis contextual.** En vez de repartir entre el equipo la lectura de un nuevo paquete de normas o de una sentencia extensa, la IA-Unificada puede generar un primer resumen técnico y luego distintos “cortes” según el público

interno: un memo ejecutivo para el C-level, una ficha específica para producto/tecnología, una nota para finanzas, una guía para atención al cliente. Esto dialoga con lo que planteamos en [“El ecosistema emprendedor y el impulso de las nuevas iniciativas”](#): la clave no es sólo tener la información, sino lograr que el lenguaje legal se conecte con el lenguaje de negocio y de producto.

2. Búsqueda inteligente y “memoria viva” del criterio jurídico interno. Muchas organizaciones pierden horas de trabajo buscando “qué dijimos sobre este tema hace tres años” o “cómo resolvimos un caso parecido en tal país”. Un equipo legal aumentado puede apoyarse en IA para crear una **memoria viva de dictámenes, contratos tipo, posiciones frente a reguladores y acuerdos con cámaras**. Lo que en [“La implementación de los modelos Unified & Collaborative Commerce”](#) aparece como gobernanza de acuerdos entre actores, aquí se convierte en gobernanza del propio criterio jurídico de la compañía.

3. Análisis de riesgos y escenarios. Combinando el Radar de riesgos regulatorios y el Risk-Impact Canvas que proponemos en este libro con capacidades analíticas de IA, el equipo legal puede explorar preguntas como:

- ¿Qué pasa si tal impuesto digital se extiende a esta categoría de servicios?

- ¿Qué impacto tendría en nuestro P&L y en nuestro modelo de datos una obligación más estricta de consentimiento?
- ¿Qué cambios habría que hacer en contratos con sellers o partners si nuevos criterios jurisprudenciales nos consideran corresponsables de ciertas conductas?

4. En la saga *#QuantumRetail* mostramos cómo simular escenarios de negocio ayuda a gobernar el flywheel. Aquí el ejercicio es similar, pero aplicado a regulaciones: se simulan shocks normativos y se discute, con tiempo, cómo absorberlos o incluso cómo anticiparse.

5. Soporte a negociaciones y diálogo público-privado.

Un equipo legal en modo Human Augmented AI también es más fuerte en la mesa de diálogo con reguladores, cámaras y otras empresas. Puede llegar con mejores datos, comparativas internacionales, ejemplos de buenas prácticas recogidas de otros mercados (por ejemplo, los que analizamos en [“El desarrollo del Retail Media Network”](#) en materia de privacidad y transparencia). La IA ayuda a preparar documentos, propuestas y posiciones informadas, pero la decisión sobre qué negociar y cómo sigue siendo profundamente humana.

6. Formación continua del propio equipo y de la organización. Finalmente, estos co-pilotos pueden usarse para crear **itinerarios de capacitación**

interna personalizados: módulos sobre datos y privacidad para marketing y producto, sobre defensa del consumidor para atención al cliente, sobre IA y algoritmos para datos y tecnología. En la colección ya vimos, en varios libros, que la brecha no es sólo tecnológica sino de capacidades. Los equipos legales aumentados pueden ser curadores y facilitadores de una cultura de cumplimiento inteligente, no meros guardianes de la puerta.

Es importante subrayar que esto no se trata de “tener menos abogados”, sino de **llevar a los abogados al lugar donde más valor generan**: el diseño de estrategias, la interpretación final de ambigüedades reguladoras, la construcción de acuerdos sostenibles con otros actores del ecosistema. La IA se ocupa de tareas intensivas en lectura, clasificación y síntesis; el equipo humano se ocupa de discernir qué batallas dar, qué riesgos asumir, qué compromisos proponer. En otras palabras: menos tiempo buscando, más tiempo pensando.

Desde la perspectiva de la colección *Génesis de un Futuro Digital*, los equipos legales en modo human augmented AI son una pieza natural del rompecabezas:

- Complementan al **data trust flywheel** al asumir un rol activo en la construcción de confianza normativa.
- Se integran con los modelos de **unified & collaborative commerce**, donde la gobernanza de acuerdos entre múltiples actores es clave.

- Son aliados centrales en la expansión de **retail media 4.0** y de la economía de plataformas que analizamos en otros libros, porque permiten escalar modelos complejos sin perder de vista el marco de juego.

En una región donde el caos normativo parece, a veces, parte del paisaje, la figura del GC y del equipo legal en modo Human Augmented AI no es un lujo futurista; es una condición para que los negocios digitales puedan escalar de forma sostenible y para que los países puedan regular con inteligencia, apoyándose en profesionales que no sólo conocen la letra de la ley, sino que cuentan con las mejores herramientas para interpretarla, aplicarla y mejorarla.



Identidad digital e innovación financiera: tokenización y protección de datos. Otro frente emergente clave es la gestión de la **identidad digital** y la irrupción de tecnologías de **tokenización** (representación de activos o derechos en tokens digitales, usualmente sobre blockchain). Estos temas entrelazan aspectos de **soberanía de datos, privacidad, inclusión financiera y ciberseguridad**.

Sebastián Bellagamba, VP External Engagement de Internet Society, remarcaba la importancia de la **gobernanza multistakeholder** para preservar un internet abierto y seguro⁸⁰



“La gobernanza de Internet debe seguir siendo inclusiva y colaborativa, con gobiernos, empresas, academia y técnicos cooperando”.



**Sebastián
Bellagamba**

Sólo así la red reflejará valores democráticos. Esto aplica directamente al desafío de la **identidad digital soberana**: ¿quién controla nuestros datos de identidad en línea? Hoy dependemos de gigantes tecnológicos (cuentas de Google, Facebook) o de esquemas gubernamentales tradicionales poco interoperables. Se vislumbra un cambio de paradigma con la **identidad digital descentralizada** (self-sovereign identity), apoyada en blockchain, donde cada individuo podría gestionar sus credenciales (DNI, certificados, historiales) sin intermediarios onnipotentes.

Enrique Dans pinta un escenario futurista muy ilustrativo:



“Habrá un momento de la verdad cuando aparezcan las primeras aplicaciones que te permitan hacer login con tu wallet [criptográfica] (...) En una web distinta en la cual tú tienes el control de los datos”.



Enrique
Dans

Dans imagina un internet donde el **login con billetera digital reemplace al usuario-id tradicional**, y le devuelva al individuo la autoridad sobre su información. Esto permitiría usar una misma identidad blockchain para votar, acceder a salud o cobrar remesas, con mayor seguridad y privacidad que los sistemas actuales. La **“soberanía de datos”** del ciudadano pasaría de eslogan a realidad técnica. Ahora bien, lograrlo requerirá **estándares comunes y reconocimiento legal** de esas identidades descentralizadas.

La UE ya avanza con su propuesta de **Identidad Digital Europea (EUDI Wallet)**, que interoperará certificados oficiales en todos los Estados miembro. En América Latina, países como **Brasil** y **Uruguay** exploran proyectos de identidad digital basados en blockchain, y organismos como la OEA discuten marcos regionales. *Argentina* lanzó en 2022 una prueba de concepto de *identidad auto soberana* para credenciales académicas, con apoyo del BID. Sin embargo, falta mucho camino regulatorio: ¿se reconocerá legalmente una firma con clave criptográfica

autogestionada igual que una firma digital expedida por el gobierno? ¿Cómo se previene el fraude de identidades descentralizadas? ¿Qué pasa si el ciudadano pierde sus claves? Aquí, de nuevo, la colaboración multilateral es clave.

Declaraciones regionales como la de *Cartagena* y *Montevideo* en 2022 ya asoman principios: la IA (y, por extensión, las nuevas tecnologías de datos) debe respetar derechos humanos, diversidad cultural y promover desarrollo sostenible, con el impulso de marcos de gobernanza responsables (Ulloa, s.f.). Traduzco esto a identidad digital: *debe servir a las personas*, no al revés. Cualquier sistema de identidad digital ha de ser voluntario, proteger la privacidad por diseño y estar bajo control del usuario. Son líneas rojas que nuestras legislaciones de protección de datos y cibercriminos deben actualizar para cubrir estas nuevas formas de identificación.

Por otro lado, la **tokenización de activos** vía blockchain promete revolucionar sectores como finanzas, logística, arte y hasta gestión pública, pero aún carece de regulación clara. Tokenizar implica convertir derechos sobre un activo (dinero, acciones, propiedad y hasta obras de arte) en *tokens digitales* transferibles. Esto mejora la liquidez y transparencia, pero también trae riesgos de fraude, volatilidad y lavado de dinero.

Europa marcó un hito con el reciente **reglamento MiCA (markets in crypto-assets)**, aprobado en 2023 y aplicable desde 2026, que establece reglas uniformes para

criptoactivos, incluyendo **estándares de transparencia, divulgación y supervisión** para emisores y proveedores. En otras palabras, MiCA exige white papers con información clave para emitir tokens, obliga al registro de proveedores de servicios cripto y otorga potestades a supervisores para vigilar abusos. Es un modelo que **Latinoamérica puede aprovechar** en la creación de sus propios marcos.

Hoy nuestra situación cripto es heterogénea: *El Salvador* declaró bitcoin como moneda de curso legal; *Brasil* aprobó en 2022 una ley que regula la intermediación de criptoactivos; *Argentina* grava las ganancias cripto pero no tiene regulación específica; *Colombia* y *México* prueban proyectos pilotos pero sin ley marco aún. Esta falta de uniformidad genera incertidumbre y limita la escala de innovaciones legítimas. Paradójicamente, también puede verse como una oportunidad: si actuamos coordinadamente ahora, podemos evitar errores ajenos y **adoptar “lo mejor de ambos mundos”**; incentivar lo bueno de blockchain (trazabilidad, descentralización) pero mitigando sus peligros.

Una idea concreta es crear un **sandbox regional para tokenización**, donde startups de distintos países puedan testar proyectos bajo la tutela conjunta de múltiples reguladores. Esto fomentaría un *aprendizaje compartido* y, eventualmente, **normas regionalmente armonizadas**. De hecho, el **Consejo de Estabilidad Financiera (FSB)** ya aboga por marcos internacionales unificados para criptoactivos.

Un aspecto asociado a identidad y tokenización es la **privacidad y protección de datos personales**. Nuestra región tiene un mosaico de leyes de datos, muchas inspiradas en el estándar global del **GDPR europeo**. Brasil tiene su LGPD; México y Colombia, sus leyes federales; Chile acaba de actualizar la suya (ley 21.719 de 2024) equiparándola a GDPR; Argentina está en proceso de reformar su Ley 25.326 del año 2000 para modernizarla. En un mundo de IA y blockchain, la protección de datos cobra nuevas dimensiones: ¿cómo se ejerce el derecho al olvido en cadenas de bloques inmutables? ¿Quién es responsable cuando tus datos pasan por decenas de algoritmos en un flujo automatizado? ¿Cómo se maneja el consentimiento informado cuando las decisiones las toman máquinas en milisegundos?

Vamos a necesitar **innovar también en la regulación de datos**: incorporar conceptos como *privacy by design* (exigir que todo sistema digital incorpore medidas de privacidad desde su concepción), *privacy by default* (que la configuración por defecto de servicios sea la más protectora), y normativas sobre **datos anonimizados y seudonimizados**. En entornos de big data, a veces los datos personales no vienen con nombre y apellido pero igual pueden identificar patrones sensibles. Europa ya discute actualizar su marco ePrivacy para abordar Internet de las Cosas e IA.

En Latinoamérica, un avance clave fue la adhesión de varios países (Argentina, México, Chile, etc.) a la **Red Global de Privacidad** y la reciente creación de un **Observatorio Iberoamericano de Protección de Datos**,

para intercambiar mejores prácticas regulatorias. Es fundamental potenciar esas colaboraciones, porque los desafíos (biometría, geolocalización, datos de niños, etc.) son comunes.

Recuerdo cuando implementamos en la empresa una solución de IA que personalizaba ofertas analizando el comportamiento de los clientes. Tuvimos que detener el despliegue en cierto país por dudas regulatorias: ¿era necesario pedir consentimiento explícito para ese nivel de análisis? ¿Debíamos ofrecer opt-out fácil? Ante la ausencia de claridad legal, **optamos por la autorregulación responsable**: imitamos el estándar GDPR en mercados donde ni siquiera era obligatorio, para darle transparencia y control al usuario.

Esta anécdota muestra que muchas empresas líderes ya se *adelantan* y aplican las mejores prácticas globales aun sin obligación local, en parte para ganar confianza. Pero no deberíamos depender sólo de la buena voluntad. Necesitamos actualizar las leyes de datos para contemplar estos escenarios y exigir esas buenas prácticas a todo el mercado, para nivelar la cancha.

Hacia marcos regionales armonizados y gobernanza multilateral. Un aprendizaje que he tenido a lo largo de estos 25 años en el ecosistema digital es que **ninguna jurisdicción aislada puede resolver desafíos que por naturaleza son transnacionales**. Internet no conoce fronteras; las regulaciones nacionales sí. De ahí nace la importancia de la **armonización regulatoria regional** y la cooperación internacional.

Iberoamérica, con sus más de 600 millones de habitantes y un idioma casi común, tiene una oportunidad de oro para presentarse unida en la era digital, creando un **mercado digital regional** integrado. Esto beneficiaría tanto a emprendedores locales –que podrían escalar soluciones a mercado regional sin chocar con 20 marcos distintos– como a los consumidores, que gozarían de derechos homogéneos y mayor oferta competitiva.

En el plano comercial, bloques como **Mercosur** y la **Alianza del Pacífico** ya reconocen esta prioridad. Mercosur históricamente avanzó poco en integración digital, centrado en bienes agrarios e industriales; pero la aceleración tecnológica está forzando un cambio. Un artículo reciente señalaba que el comercio intrarregional Mercosur lleva años estancado en menos 15%, y que las herramientas digitales, en especial fintech y pagos, podrían dinamizarlo si se reducen trabas ([Prensa Mercosur](#), 2025).

Uno de los **principales obstáculos** identificados es justamente *la falta de armonización regulatoria en materia financiera y tecnológica* dentro del bloque. Cada país hoy tiene reglas distintas para las fintech, regímenes fiscales no coordinados, requisitos diversos para comercio electrónico transfronterizo; así es difícil que una plataforma o pasarela de pagos opere fluidamente en Argentina, Brasil, Uruguay y Paraguay a la vez. También inciden controles de capital y ausencia de acuerdos para reconocimiento mutuo de firmas digitales o medios de pago (Prensa Mercosur, 2025). La buena noticia es que esto empieza a asumirse en la agenda política. *Mercado*

Pago, por ejemplo, se ha posicionado en varios países Mercosur y está llevando de facto integración “desde abajo” al facilitar pagos entre fronteras (Prensa Mercosur, 2025). Los gobiernos están viendo que deben acompañar esa tendencia con **normativas comunes**.

En julio de 2025, los ministros de Finanzas del Mercosur discutieron por primera vez la creación de un **marco regional de pagos digitales**, y se habló de estándares compartidos de *open banking*. Igualmente, se evalúa una **pasarela aduanera digital unificada** para simplificar el ecommerce transfronterizo –quizá inspirada en la interoperabilidad de ventanillas únicas que la Alianza del Pacífico impulsa– (Alianza del Pacífico, 2021). Es incipiente, pero la dirección es correcta: pasar de la retórica a construir **“arquitectura digital regional”** que respalde los nuevos hábitos de consumo y producción (Prensa Mercosur, 2025).

La **Alianza del Pacífico (AP)**, por su parte, lleva ventaja conceptual: desde 2016 habla de conformar un **mercado digital regional** entre Chile, Colombia, México y Perú. Tienen una agenda digital conjunta y han firmado capítulos de economía digital en sus acuerdos comerciales. La *Hoja de Ruta para el Mercado Digital Regional de la AP* (2020) establece pilares concretos: facilitar comercio digital (interoperabilidad de ventanillas únicas, documentación electrónica), promover ciberseguridad coordinada, proteger al consumidor en línea de forma homogénea, asegurar privacidad y **libre flujo de datos con confianza** entre los países.

Esto último es clave: libre flujo de datos no significa “barra libre” de explotación, sino acordar estándares altos de protección de datos para permitir que la información circule sin temor a abusos. La AP incluso menciona cooperar en **neutralidad de red** y compartir mejores prácticas regulatorias en temas emergentes. Si bien la implementación de esa hoja de ruta ha sido lenta (la pandemia y vaivenes políticos interrumpieron avances), es un **norte valioso**. Ojalá retome el impulso con apoyo de organismos como CEPAL o CAF.

Además de la integración regional, es necesaria la **gobernanza multilateral** más allá de la región. Latinoamérica debe participar activamente en la construcción de las “reglas digitales” globales, en foros como la OCDE, el G20, la OMC (en comercio electrónico) y la ONU (ej., el Roadmap de Cooperación Digital del Secretario General). No podemos simplemente importar regulaciones de EE.UU. o Europa sin adaptarlas a nuestra realidad, ni tampoco quedar como meros receptores pasivos de tecnología extranjera.

Como suelo decir: ni China ni Silicon Valley van a pensar por nosotros. Necesitamos una visión **geopolítica propia** en digital. Por ejemplo, en debates sobre regulación de IA a nivel ONU, América Latina podría impulsar la inclusión de sus principios: equidad social, reducción de brechas, respeto a la diversidad cultural y lingüística (pensemos en IA entrenadas mayormente en inglés, ¿cómo aseguramos que funcionen bien en español, portugués o lenguas indígenas?).

También podemos contribuir con experiencias innovadoras: Colombia y Brasil fueron de los primeros en el mundo en adoptar **sandboxes** fintech; Uruguay tiene uno de los **gobiernos digitales** más avanzados; México desarrolla marcos de interoperabilidad de identidad. Nuestra participación con casos de éxito y lecciones aprendidas enriquecerá las discusiones globales. A su vez, podemos *aprender y adaptar* rápidamente las mejores prácticas ajenas: por ejemplo, **el paquete digital europeo (DSA/DMA)** que entró en vigor en 2023 nos sirve de inspiración para abordar el poder de las grandes plataformas y la seguridad en línea. La **Digital Markets Act (DMA)** de la UE establece criterios objetivos para identificar “guardianes de acceso” (grandes plataformas dominantes) y les impone obligaciones procompetitivas: compartir ciertos datos con competidores, no darle preferencia a sus propios servicios, asegurar interoperabilidad básica, etc.

La **Digital Services Act (DSA)**, por su parte, exige a las grandes plataformas mayor responsabilidad en moderación de contenidos, transparencia en sus algoritmos y mecanismos ágiles para que usuarios reporten y remedien contenidos ilegales. Ambas buscan equilibrar innovación con protección de usuarios, alineando el sector digital con principios democráticos. Que la UE –una jurisdicción de 450 millones de habitantes– haya logrado consenso en estas leyes sugiere que *sí es posible* regular lo digital de manera integral. Claro, nuestro contexto difiere (no tenemos un mercado común tan institucionalizado ni un tribunal supranacional fuerte), pero podemos aspirar a algo similar en nuestro marco regional: **garantizar un**

entorno digital seguro, competitivo y confiable para 600 millones de iberoamericanos.

Parte de esa gobernanza multilateral incluye también la creación de **observatorios y centros de monitoreo**. Mencioné antes la idea de observatorios digitales: estos pueden ser espacios de investigación aplicada que provean evidencia continua a los reguladores. Un ejemplo es el **Observatorio Regional de IA** que propone la OCDE para América Latina, o el *Observatorio de Comercio Digital* sugerido en foros de la OMC.

Brasil inauguró en 2023 el **Observatorio para el Desarrollo Integrado y Sostenible (ODIS)**, una plataforma de datos abiertos impulsada por su instituto IBICT con apoyo internacional, para difundir políticas públicas de acceso tecnológico y desarrollo sostenible en la región. Iniciativas así ayudan a **tomar el pulso** al ecosistema: recopilan estadísticas, identifican brechas (por ejemplo, qué países no tienen ley de ciberseguridad, o cuántas startups aprovechan sandboxes) y evalúan el impacto de las normativas vigentes. Propongo que, a nivel Mercosur o AP, se establezcan observatorios específicos en áreas críticas – un observatorio regional de IA, uno de *economía de plataformas* y quizá uno de *ciudadanía digital* – que alimenten con datos locales las discusiones. Por ejemplo, un observatorio de plataformas podría medir la situación laboral en la gig economy en distintos países, e iluminar dónde urge legislar para proteger a repartidores o choferes sin frenar el modelo de negocio.

Ejemplos internacionales inspiradores. He ido mencionando varios a lo largo del capítulo. Vale la pena recapitular algunos casos que deben inspirarnos al diseñar nuestro camino regulatorio:

- ❑ La **Unión Europea** como referente de regulación integral: con el **GDPR** puso la vara global en privacidad (incluso empresas y países fuera de la UE adoptaron estándares GDPR por conveniencia), y ahora, con la **DSA/DMA**, marca un rumbo en regulación de plataformas que equilibra derechos de usuarios, competencia leal e innovación. Europa demostró que regular lo digital *no mata la innovación*; al contrario, brinda certidumbre y confianza a largo plazo. Sus principios de *tecnoneutralidad*, *proporcionalidad* y *foco en riesgos* calaron en muchas de nuestras iniciativas. Sin ir más lejos, la **Ley Modelo de IA del Parlatino** (Parlamento Latinoamericano y Caribeño, 2022) se inspiró fuertemente en la estructura de la AI Act europea.

El **DMA** nos inspira especialmente en cómo abordar a las Big Tech en nuestro terreno: América Latina sufre tanto como Europa (o más) las prácticas monopólicas de algunas plataformas, pero individualmente nuestros países tienen menos poder de negociación. Una respuesta coordinada, por ejemplo vía Mercosur o a nivel panregional, para adoptar principios tipo DMA (identificar *gatekeepers* locales/regionales y establecer reglas de juego justas) podría empoderar a nuestros emprendedores y proteger a pymes que hoy dependen de esos ecosistemas.

- **El enfoque británico de sandboxes:** Reino Unido no sólo inauguró el sandbox fintech, también ha aplicado la filosofía sandbox a **regTech** (tecnología regulatoria) e IA. En 2023 lanzó un *AI Sandbox* para que empresas prueben sistemas de IA con soporte de reguladores sectoriales, y evaluar cumplimiento ético antes de una regulación formal. Esta mentalidad pragmática –“probar antes de regular”– es muy valiosa para nosotros. *Colombia* fue uno de los primeros de la región en replicarla, con su **sandbox financiero** desde 2018 (Superintendencia Financiera) y uno especial para proyectos con **blockchain e IA** desde 2021.

Los resultados en Colombia han sido positivos: la SFC reportó en 2024 que más de 20 innovaciones pasaron por el sandbox, varias de las cuales derivaron en productos fintech aprobados o ajustes normativos (ej., normas de crowdfunding y pagos digitales). **Eugenio Sánchez**, que vivió de cerca el caso colombiano, subraya cómo el sandbox fomentó un diálogo continuo entre innovadores y supervisores, lo que generó confianza mutua y permitió corregir el curso rápidamente cuando fue necesario. *La lección: la flexibilidad regulatoria controlada acelera el aprendizaje* y evita tener que “congelar” la innovación a la espera de leyes.

- **La apuesta de organismos multilaterales por pautas éticas:** La UNESCO, con su **Recomendación de Ética de IA (2021)**, que ya aplican Brasil, México, Uruguay y otros (Ulloa, s.f.); la **OCDE**, con sus *Principios de IA* (transparencia, robustez, rendición de cuentas); el **G20**, con principios de IA y la mencionada Declaración de Delhi (2023), que enfatiza en una IA

responsable, explicable y centrada en el ser humano (Ulloa, s.f.). También la **ONU** está formando un grupo asesor para la gobernanza global de IA.

Todos estos esfuerzos nos sirven de marco de referencia: muestran que existe convergencia en valores fundamentales, los cuales debemos reflejar en nuestras leyes nacionales. De hecho, varios países de la región incorporaron esos valores en sus **estrategias nacionales de IA** (Argentina y Brasil hablan de IA “fiable” basada en derechos; Colombia enfatiza la adopción ética y sostenible de IA en su hoja de ruta).

□ **Experiencias de gobernanza de internet inclusiva:**

Por ejemplo, el modelo multistakeholder de **ICANN** o los **Foros de Gobernanza de Internet (IGF)** anuales, donde gobiernos, empresas y sociedad civil dialogan en igualdad de condiciones sobre políticas de internet. **Sebastián Bellagamba** suele destacar que en Latinoamérica, LACNIC (registro regional de direcciones IP) fue pionero en esa gobernanza colaborativa, lo que redujo tensiones entre sectores y generó comunidad.⁸¹

Esa experiencia exitosa en infraestructura (manejamos las direcciones IP regionalmente con participación de todos) puede extrapolarse a otros ámbitos digitales: ¿por qué no concebir un **consejo latinoamericano de IA** con múltiples actores, que emita recomendaciones y buenas prácticas? ¿O una **Coalición regional para la protección de datos**, que unifique criterios con la participación activa de expertos, ONGs, etc.? El caso de ICANN nos enseñó que

la autorregulación con participación abierta puede funcionar en entornos técnicos; quizás combinar eso con respaldo gubernamental en otros campos logre agilidad sin perder legitimidad.

- **Casos de sandbox regulatorios sectoriales:** Además del fintech, está el ejemplo del **sandbox en gobierno digital** de *Estonia*, que permitió probar servicios públicos digitales innovadores antes de escalarlos; o el **sandbox de movilidad** en Singapur, donde se testearon vehículos autónomos en un distrito delimitado antes de regularlos. *Colombia* también implementó en 2022 un **sandbox de economía colaborativa** para que plataformas de delivery probaran esquemas de seguridad social voluntaria para repartidores, cuyos resultados están nutriendo un proyecto de ley sobre trabajo en plataformas. Todos estos ejemplos nos enseñan que la regulación puede *preceder* a la ley en sentido estricto, mediante estas autorizaciones temporales que luego alumbran la norma permanente.

Ciertamente, no todo es copiable tal cual. Debemos adaptar cada referencia a nuestras **prioridades y contextos locales**. Iberoamérica tiene niveles de informalidad económica altos, gobiernos con recursos limitados para enforcement, brechas educativas y de conectividad importantes. Por eso insisto en que cualquier marco regulatorio **debe ser también “glocal”**: inspirado en estándares globales pero calibrado a las realidades nacionales.

Un ejemplo: el **derecho al olvido** de la UE (que permite a

ciudadanos pedir que se eliminen resultados de búsqueda perjudiciales) suena muy bien, pero ¿cómo aplicarlo en países donde la judicatura está saturada o donde gran parte de la población ni siquiera sabe ejercer sus derechos digitales? Quizá acá pase más por autoridades administrativas ágiles que por procesos judiciales largos. O en ***gig economy***, Europa debate obligar a plataformas a formalizar a los repartidores como empleados; en nuestra región, dada la alta desocupación, quizás convenga un modelo híbrido que extienda protecciones sociales básicas sin forzar la relación laboral clásica que podría expulsar a muchos. Son *discusiones complejas*, pero impostergables.

La **transformación digital**, en última instancia, **trata de personas**. Detrás de cada algoritmo, de cada transacción en línea, de cada token, hay un ser humano con aspiraciones, miedos, derechos y deberes. Los marcos normativos deben servir para que *la tecnología potencie a las personas, no que las avasalle*. No olvidemos que **la tecnología sin humanidad es solo código; con humanidad, se vuelve cultura**. Creo firmemente en eso. He visto emprendedores brillantes fracasar no por mala tecnología sino por no entender el entramado legal o social en que operaban. He visto también iniciativas regulatorias bienintencionadas naufragar por no dialogar con el sector productivo o por temer tanto la innovación que la estrangularon.

Mi convicción es que debemos superar las posturas polarizadas de **techno-optimismo naíf** (dejar que el mercado resuelva todo, “move fast and break things”)

y de **tecnopesimismo paralizante** (“prohibir hasta nuevo aviso”). En su lugar, adoptar un **tecnorealismo humanista**: aprovechar la evidencia y la colaboración para regular adaptativamente, con el norte siempre fijo en el bienestar común. *La regulación es habilitadora cuando se hace bien.* Habilita confianza, que es la base de los mercados; habilita competencia justa, que es la base de la innovación sostenida; habilita inclusión, para que todos cosechen los frutos del progreso tecnológico, no sólo unos pocos.

En estos años he tenido el honor de participar en la génesis y evolución del ecosistema digital iberoamericano. He vivido **“dèjà vus” regulatorios**: debates que se repiten con cada ola tecnológica, desde el ecommerce básico hasta la IA avanzada. Pero cada ciclo trae sus matices y, sobre todo, nuevas herramientas para afrontarlos. Hoy contamos con mayor madurez institucional, con redes de expertos, con sociedades civiles vigilantes y con ejemplos internacionales tangibles de qué funciona. No partimos de cero. Por eso soy *optimista*.



Como decía [Sergio Candelo, Co-Founder & COO de Snoop Consulting](#), en una de las entrevistas, cada revolución tecnológica nos asustó al principio (la máquina de vapor, la electricidad, las computadoras), y, sin embargo, terminamos con **más empleos, más calidad de vida**.⁸²



“Hoy somos 8.000 millones de habitantes; con la IA creo que puede pasar lo mismo. La diferencia es la velocidad (...) pero lo que viene es un mundo increíble y esperanzador, con un montón de posibilidades”.



Sergio
Candelo

Concuerdo: la velocidad impone vértigo, pero confío en nuestra capacidad de adaptación. *Nuestra generación es bisagra*, como dijo Verónica Pinazo; hemos vivido la era analógica y la digital, y eso nos da una perspectiva única para tender puentes.

En Iberoamérica necesitamos esos puentes: entre innovación y regulación, entre países vecinos, entre sectores público y privado, entre lo global y lo local. Si logramos diseñar **marcos normativos adaptativos, colaborativos y coherentes con el avance tecnológico**, habremos sentado las bases de un **futuro digital inclusivo y próspero** para la región. No será tarea de un solo acto legislativo sino un proceso constante; un “libro vivo”, tal como esta colección, que se va escribiendo y corrigiendo en tiempo real. *Invito a todos los actores* a involucrarse en esta construcción: legisladores abiertos al aprendizaje,

empresarios con compromiso social, académicos que aporten evidencia, y ciudadanos digitales exigentes y participativos.

Termino con una imagen que uso a veces: la transformación digital es como un río caudaloso. Podemos intentar contenerlo con diques rígidos (y arriesgarnos a que desborde) o guiarlo con cauces flexibles para irrigar nuestros campos. La regulación inteligente es ese cauce: no detiene el río, le da dirección y evita inundaciones. Hagamos entonces el cauce juntos, con visión compartida. **El futuro digital iberoamericano no está escrito; escribámoslo con reglas claras, justas y humanas, para que la innovación tecnológica realmente mejore la vida de nuestras sociedades.** Como pionero y testigo de esta génesis digital, tengo la esperanza –y la determinación– de que así lo haremos, aprendiendo del déjà vu del pasado para forjar un mañana mejor.



DIQUES RÍGIDOS

CAUCES FLEXIBLES

REGULACIÓN INTELIGENTE

INNOVACIÓN

VALOR

GÉNESIS

DE UN FUTURO DIGITAL





Conclusión

A lo largo de esta colección, hemos revivido —una y otra vez— un patrón que acompaña al ecosistema digital desde su nacimiento: ***la innovación siempre llega antes que la regulación.***

Lo vivimos en los noventa, cuando vender por internet era casi un acto de fe. Lo volvimos a ver con la irrupción de las plataformas, el auge fintech y, ahora, con la inteligencia artificial generativa. En cada *momentum* de Génesis de un Futuro Digital, el progreso tecnológico se adelantó a la ley y obligó a los Estados a correr detrás de la realidad.

Pero sería injusto reducir esta historia a una sucesión de vacíos legales. Lo que emergió en estas dos décadas no fue un caos sino una forma distinta de gobernanza. Aprendimos —a fuerza de ensayo y error— que las reglas del mundo digital no se imponen: se construyen colectivamente.

Durante la primera década del comercio electrónico (1995–2005), el crecimiento en Iberoamérica fue

eminentemente silvestre. Internet crecía sin pedir permiso, y los emprendedores actuaban “a riesgo”, navegando entre la curiosidad de los consumidores y la indiferencia de los reguladores.

En aquellos años, **la penetración de internet en América Latina apenas supera el 15 %** y alcanza el 70 % recién en 2020.⁸³ No existían leyes de comercio electrónico ni marcos de protección al consumidor digital; mucho menos, estándares internacionales sobre privacidad o seguridad.

La referencia más sólida fue la **Ley Modelo de la CNUDMI** sobre Comercio Electrónico (UNCITRAL, 1996), que estableció los principios de **equivalencia funcional y neutralidad tecnológica**: un contrato digital debía valer tanto como uno en papel, sin importar el soporte.⁸⁴ Esa fue la semilla de las leyes fundacionales de Argentina (ley 25.506 de firma digital, 2001), México (Código de Comercio reformado en 2003) y Chile (ley 19.799, 2002).

Fue una época donde la **autorregulación sectorial** ocupó el vacío estatal. La Cámara Argentina de Comercio Electrónico (CACE), la Cámara Brasileña (camara-e.net) y las primeras asociaciones en México y Colombia actuaron como mediadoras entre la innovación y la norma. Ese modelo —empresas creando reglas para sí mismas— marcó el ADN del ecosistema digital regional.

A partir de 2015, la región dio un salto de madurez: **pasamos de la desregulación de facto a la regulación habilitante**. El caso más emblemático fue la **ley fintech**

de México (2018), la primera de su tipo en Iberoamérica. No buscaba restringir la innovación sino ofrecer un marco para canalizarla: licencias, custodias, activos virtuales y pagos electrónicos bajo supervisión.

Poco después, **Brasil lanzó su sandbox regulatorio (2020)**, y Colombia lo siguió con entornos controlados para probar modelos digitales. En lugar de “regular después del problema”, el Estado empezó a “probar antes de prohibir”. Estos cambios reflejan un principio fundamental de la nueva economía digital: la regulación no debe frenar la innovación sino garantizar que ocurra de forma segura, transparente e inclusiva. Tal como señalo en el libro [“El arribo de las tecnologías exponenciales y la transformación del ecosistema”](#), los países que adoptan marcos flexibles, basados en evidencia y colaboración público-privada, son los que logran atraer inversión, talento y desarrollo sostenido.

La revolución de los datos y el nacimiento del ciudadano digital

Si la década del 2000 fue la del comercio electrónico, la del 2020 es la era del dato. Como detallo en [“La revolución de los datos en la era del big data”](#) (momentum 16 de esta *Génesis de un futuro digital*), el poder ya no reside en la infraestructura sino en la información que circula dentro de ella. Los datos personales se convirtieron en el nuevo petróleo, pero también en el nuevo derecho.

La influencia del **Reglamento General de Protección de Datos (GDPR, 2018)** europeo fue decisiva. Inspiró leyes

como la **LGPD de Brasil (2018)**, la reforma de la ley 25.326 en Argentina y la **Ley 21.719 de Protección de Datos Personales en Chile (2024)**.

Hoy, más de veinte países de la región cuentan con marcos similares. Pero la diferencia está en la cultura del dato: el cumplimiento legal ya no basta. Las empresas que sobresalen no son las que “cumplen” sino las que convierten la privacidad en valor agregado.

Como dijo [**Jacobo Cohen Imach**](#), vicepresidente de Asuntos Legales de Mercado Libre, durante una de nuestras entrevistas: *“La confianza es el activo más importante del ecosistema. Las leyes ayudan, pero la verdadera regulación nace de cómo tratamos los datos de nuestros usuarios”*.

Ese cambio cultural dio origen a un nuevo tipo de ciudadano: **el ciudadano digital consciente de sus derechos**. En 2025, en América Latina los marcos de regulación y la actuación de las autoridades en protección de datos avanzan a pasos agigantados. Según el informe ***Regulatory Strategies and Priorities of Data Protection Authorities in Latin America: 2024 and Beyond*** de FPF,⁸⁵ la mayoría de los países ya reconoce la privacidad y la protección de datos como derechos separados, y muchas autoridades han hecho de la formación ciudadana, la participación pública y la educación en derechos digitales una prioridad clave.

Este nuevo escenario fortalece la exigencia de que las marcas y empresas asuman una responsabilidad mayor en el tratamiento de datos personales —no solo por cumplimiento legal, sino por la confianza y expectativas de los consumidores digitales.

De la autorregulación a la correulación: El caso del retail media y los marketplaces

Uno de los mejores ejemplos de autorregulación exitosa en la región fue el Black Friday de Brasil (2013). Luego del escándalo de 2012 —cuando miles de consumidores denunciaron la “maquiagem de preço” (subir precios antes para fingir descuentos)—, la Cámara Brasileña de Comercio Electrónico (camara-e.net) lanzó, con apoyo del gobierno, el Código de Ética de Black Friday, y permitió a las tiendas adherirse voluntariamente bajo supervisión de la cámara.⁸⁶

Ese episodio marcó un antes y un después: mostró que la confianza se puede institucionalizar. A partir de allí, los consumidores empezaron a reconocer sellos de buenas prácticas, los medios visibilizaron las empresas responsables y los reguladores encontraron un modelo replicable.

En [“El desarrollo del retail media network”](#) sostengo que la autorregulación ha sido la antesala de toda legislación efectiva en el entorno digital: primero la práctica, luego la norma. Los ecosistemas más dinámicos son aquellos donde el sector privado y el público coconstruyen la confianza.

Tecnologías exponenciales y gobernanza ética

La irrupción de la inteligencia artificial generativa y las tecnologías exponenciales trajo de regreso viejos dilemas con nuevos rostros. ¿Quién es responsable por los sesgos algorítmicos? ¿Cómo se protege la identidad digital? ¿Qué límites debe tener la automatización?

En 2024, la Unión Europea aprobó el AI act, el primer marco legal integral del mundo para regular la inteligencia artificial según su nivel de riesgo.⁸⁷ Latinoamérica, aunque más rezagada, avanza en la misma dirección: Chile discute su propio proyecto de ley de IA (Boletín 16.821-19, 2024), mientras Brasil impulsa una Estrategia Nacional de IA ética y responsable.

Como advierto en el libro [*“El arribo de las tecnologías exponenciales y la transformación del ecosistema”*](#) la IA nos obliga a revisar los cimientos del contrato social digital. No basta con la transparencia: necesitamos explicabilidad, rendición de cuentas y diversidad en los datos.

En ese sentido, la adopción de los principios de UNESCO (2021) y OCDE (2019) sobre IA —centrados en derechos humanos, inclusión y sustentabilidad— representan un avance enorme para la región.

Y no se trata sólo de IA. También el blockchain, la tokenización de activos y la identidad digital soberana están redefiniendo las reglas del juego. Como anticipaba [**Enrique Dans**](#) en su entrevista para eLíderes x25: *“Habrá un momento en que pidamos a Google, Facebook o los*

bancos que pongan nuestros datos en nuestra wallet, y desde ahí decidamos a quién dárselos”.

Esa visión sintetiza lo que será la próxima frontera regulatoria: el control del dato en manos del usuario.

El futuro: regulación como ventaja competitiva

Después de 25 años, la historia se repite pero con un final diferente. Si en los noventa la regulación llegaba tarde, hoy la región empieza a regular a tiempo, e incluso a anticipar.

Las empresas que incorporan ética algorítmica, privacidad por diseño y gobernanza de datos desde el inicio no sólo cumplen la ley: ganan confianza, reputación y sostenibilidad.

Los Estados que diseñan leyes flexibles y dialogadas atraen inversión, mientras los que legislan por reacción terminan frenando su propio desarrollo.

La próxima década nos pondrá a prueba. Inteligencia artificial, identidad digital y soberanía de datos serán los nuevos campos de batalla. Pero esta vez, Iberoamérica llega con experiencia, con marcos sólidos y, sobre todo, con la convicción de que la regulación inteligente no es un límite sino una palanca de desarrollo.

Porque, al final del día, lo digital no trata de tecnología: trata de personas, confianza y propósito. Y regular bien es, simplemente, diseñar el futuro.

GÉNESIS

DE UN FUTURO DIGITAL





Apéndice práctico: Operar en modo *regulatory-ready*

El objetivo de este libro no es que el lector termine sabiendo citar artículos de ley, sino que pueda **tomar mejores decisiones de negocio, de ecosistema y de política pública** en un entorno regulatorio cambiante. A lo largo de los capítulos vimos patrones, casos, principios y déjà vu. Este apéndice baja todo eso a un **kit de herramientas concretas** para cuatro perfiles que conviven en el ecosistema digital:

- ❑ C-levels de retailers, marcas, marketplaces, fintechs y plataformas.
- ❑ Emprendedoras y emprendedores que están lanzando o escalando iniciativas digitales.
- ❑ Responsables de asuntos públicos, legales y regulatorios.
- ❑ Diseñadores de políticas públicas y tomadores de decisión en el sector público.

A lo largo de esta documentación, presento varios *frameworks* para leer la evolución del comercio, de las plataformas, de los datos y de la IA. Aquí sumamos tres herramientas que funcionan como **plantillas transversales** a toda la colección:

1. Una **matriz 2x2 de riesgo regulatorio (impacto vs probabilidad)**, para priorizar dónde poner el foco
2. Un **árbol de decisión “¿cuándo necesito asesoría legal especializada?”**, para no sobrereaccionar ni subestimar el riesgo.
3. Un **mapa de stakeholders regulatorios**, para entender con quién hay que hablar y cómo construir confianza en red.

No son modelos teóricos; son hojas de trabajo que se pueden imprimir, pegar en la pared o integrar a una arquitectura de IA-Unificada para que se vuelvan parte del ciclo de planificación estratégica anual.

Matriz 2x2 de riesgo regulatorio (impacto vs probabilidad)

La primera herramienta es la más simple y, a la vez, la que más conversaciones incómodas dispara en un comité ejecutivo. Se trata de una **matriz 2x2** que cruza dos variables:

- ☐ **Probabilidad** de que un riesgo regulatorio se materialice en los próximos 12–24 meses.
- ☐ **Impacto** que tendría sobre el negocio si se materializa (en ingresos, margen, licencia de operación, reputación).

El ejercicio consiste en listar los principales frentes regulatorios que describimos en este libro:

- ☐ Datos personales y privacidad.
- ☐ Derechos del consumidor digital.
- ☐ Fiscalidad digital e impuestos sobre servicios y plataformas.
- ☐ Pagos, fintech y prevención de fraude/AML.
- ☐ Propiedad intelectual, falsificaciones y piratería.
- ☐ Publicidad, influencers y retail media.
- ☐ Competencia y poder de mercado en la economía de plataformas.
- ☐ Laboral y gig economy.
- ☐ IA, algoritmos y decisiones automatizadas.

Y ubicar cada uno en la matriz, en uno de estos cuatro cuadrantes:

- ☐ **Alta probabilidad / Alto impacto**
- ☐ **Alta probabilidad / Bajo impacto**
- ☐ **Baja probabilidad / Alto impacto**
- ☐ **Baja probabilidad / Bajo impacto**

En ["El arribo de las tecnologías exponenciales"](#) propongo hacer un ejercicio similar con casos de uso de IA: no todas las aplicaciones son igual de críticas. Aquí trasladamos esa lógica al terreno regulatorio. Para un banco digital o una billetera, por ejemplo, **pagos/fintech** y **prevención de lavado** probablemente estén en "Alta probabilidad / Alto impacto". Para un marketplace de bienes de consumo, **datos personales, consumidor** y **propiedad intelectual** van a disputarse ese cuadrante. Para muchas compañías, **IA y algoritmos** aparecen hoy como "Baja probabilidad / Alto impacto": todavía no hay grandes casos locales, pero el potencial de daño es enorme.

Lo importante no es acertar en el número perfecto, sino **obligar a que negocio, legal, tecnología, datos y asuntos públicos se sienten juntos a llenar el tablero**. En *El desarrollo del Retail Media Network* vimos cómo la monetización de audiencias puede convertirse en una máquina de margen o en una bomba reputacional según cómo se gestione la privacidad. En esta matriz, eso se traduce en una conversación concreta: ¿en qué cuadrante está hoy el riesgo regulatorio asociado a nuestra estrategia de retail media? ¿Lo estamos tratando como tema estructural o como detalle táctico?

Una vez ubicados los riesgos, la matriz se convierte en un pequeño mapa de acción:

- ❑ **Alta probabilidad / alto impacto** → requiere planes específicos: políticas internas, inversión en compliance, monitoreo con IA-Unificada, diálogo proactivo con reguladores.

- **Alta probabilidad / bajo impacto** → se gestiona con procesos estandarizados y automatización, evitando que robe tiempo de agenda.
- **Baja probabilidad / alto impacto** → zona de “cisnes negros regulatorio-legales”: no se monitorea todos los días, pero se tienen escenarios y protocolos preparados (por ejemplo, una regulación de IA que afecte scoring crediticio, como discutimos en *El arribo de las tecnologías exponenciales*).
- **Baja probabilidad / bajo impacto** → se observa de manera periódica, sin exagerar.

Esta misma matriz puede ser reconstruida por:

- Una startup en etapa temprana, después de leer [*“El ecosistema emprendedor y el impulso de las nuevas iniciativas”*](#), para entender en qué frentes no puede darse el lujo de improvisar.
- Un retail tradicional que está migrando hacia modelos de Unified & Collaborative Commerce, para ver cómo cambia su exposición al pasar de retailer puro a operador de marketplace y red de retail media.
- Un policy maker, para preguntarse si su agenda regulatoria está focalizada donde realmente hay más riesgo sistémico o donde hay más ruido mediático.

El paso siguiente —como vimos con el **risk-impact canvas regulatorio** en el cuerpo del libro— es cruzar esta matriz con los impactos concretos en el P&L. Pero incluso antes de llegar a ese nivel de detalle, la matriz 2x2 ya cumple

una función esencial: **sacar la conversación regulatoria del “ruido de fondo jurídico” y llevarla al centro de la mesa de estrategia.**

Árbol de decisión

“¿Cuándo necesito asesoría legal especializada?”

El segundo instrumento está pensado especialmente para emprendedores, product managers y equipos de innovación que viven en tensión permanente entre **moverse rápido y no estrellarse con el regulador**. El problema no es sólo el costo de un abogado; es el costo de consultar demasiado tarde.

En [*“El ecosistema emprendedor y el impulso de las nuevas iniciativas”*](#) nuestro cómo muchos proyectos nacen en un margen de informalidad tolerada y luego chocan con la realidad cuando quieren escalar, levantar capital o internacionalizarse. Para evitar tanto el “no consulto nunca” como el “consulta por todo y freno todo”, este árbol de decisión propone una serie de preguntas simples de sí/no.

La lógica es la siguiente: si respondés “sí” a ciertas combinaciones de preguntas, el semáforo pasa de verde a amarillo o a rojo, y **es momento de sentarse con alguien que entienda del marco normativo**, idealmente alguien que también hable “idioma negocio” y haya leído este libro.

Las preguntas clave del árbol:

1. ¿Tu modelo implica custodiar fondos de terceros o mover dinero en nombre de otros?

- ¿Retenés saldos, procesás pagos, ofreces crédito, wallet, tokenización de valor?
- Si la respuesta es sí, estás pisando terreno fintech: semáforo amarillo intenso tirando a rojo.

2. ¿Procesás datos sensibles o de alto riesgo?

- Salud, biometría, geolocalización permanente, menores de edad, historial financiero.
- Aquí el árbol se conecta con ["El arribo de las tecnologías exponenciales"](#) y con cualquier iniciativa de IA que use esos datos para perfilar o decidir.

3. ¿Permitís que los usuarios suban contenido propio (texto, imágenes, videos, reseñas, anuncios)?

- Cualquier cosa que huela a UGC (user generated content) dispara preguntas de responsabilidad por contenidos, moderación y posibles delitos o daños a terceros.

4. ¿Operas en más de un país o tenés usuarios/clientes en jurisdicciones con marcos robustos (UE, Estados Unidos, Brasil, México, etc.)?

- El cross-border hace que se crucen marcos

fiscales, de datos, de consumo, de aduanas y de plataformas.

5. ¿Intermediás entre terceros que venden o prestan servicios en tu plataforma?

- En otras palabras: ¿sos un marketplace, una superapp o una plataforma de servicios (delivery, transporte, alojamiento, etc.)?

6. ¿Usás IA o algoritmos para tomar decisiones que afectan derechos o condiciones materiales de las personas?

- Scoring crediticio, precios dinámicos, priorización de repartidores, recomendación de ofertas laborales, filtrado de contenido sensible.

Si tu proyecto responde **“no”** a todas, probablemente estés en una zona de baja exposición; aun así, conviene al menos revisar T&Cs y políticas básicas de datos y consumidor. Si respondés **“sí”** a **una o dos de estas preguntas**, el semáforo pasa a **amarillo**: es momento de una consulta puntual para identificar riesgos y buenas prácticas mínimas.

Si respondes **“sí”** a **tres o más**, el árbol te pone en **modo rojo**: lanzar sin asesoría legal/regulatoria no es “ahorrar”, es **patear una bomba** más adelante. En ese caso, la decisión estratégica no es sólo “consulta o no consulta”, sino:

- ¿Qué tipo de asesoría necesito (sectorial, generalista, local, regional)?
- ¿Cómo la integro en el diseño del modelo de negocio, y no como corrector posterior?
- ¿Puedo apalancar **IA-unificada y human augmented AI** para hacer el trabajo de mapeo y documentación previo, y aprovechar mejor el tiempo del especialista?

Este árbol se puede pegar como página única al final de [*"El ecosistema emprendedor"*](#) y también sirve para equipos de producto que están ampliando el alcance de una plataforma ya existente, como contamos en *La implementación de los modelos Unified & Collaborative Commerce*: cada nuevo módulo (fintech, logística, publicidad, IA) cambia la cantidad de "sí" en este árbol y, con ello, el nivel de riesgo que hay que gestionar.

Mapa de stakeholders regulatorios

El tercer instrumento aborda una verdad incómoda: **el riesgo regulatorio no se gestiona sólo leyendo boletines oficiales**. Se gestiona construyendo relaciones, confianza y capacidad de interlocución con un conjunto amplio de actores que influyen en cómo se interpretan y aplican las normas.

En los distintos libros de *Génesis de un Futuro Digital* aparece una y otra vez la idea de **ecosistema**: ecosistema

emprendedor, ecosistema de datos, ecosistema de Unified & Collaborative Commerce, ecosistema de Retail Media. Este mapa de stakeholders regulatorios traslada esa idea al plano de la gobernanza. Visualmente, lo podés imaginar como tres anillos concéntricos:

□ **Núcleo (centro del radar):**

- Reguladores directos: autoridades de datos, defensa del consumidor, competencia, banca central, reguladores de telecomunicaciones, fiscalidad.
- Son quienes emiten normas, supervisan, inspeccionan y sancionan.

□ **Anillo medio:**

- Legisladores y equipos técnicos de Congreso/ Parlamento.
- Cámaras y asociaciones empresarias sectoriales (como las que recorro en *El boom del comercio electrónico* y en *La implementación de los modelos Unified & Collaborative Commerce*).
- Organismos internacionales y multilaterales (OCDE, BID, CEPAL, ONU, bancos de desarrollo).
- ONGs y organizaciones de consumidores.

□ **Anillo externo:**

- Medios de comunicación tradicionales y nativos digitales.
- Opinión pública organizada en redes sociales.
- Big Tech globales que fijan estándares de facto

(tiendas de apps, proveedores de nube, grandes plataformas).

- Comunidad académica y think tanks especializados.

El ejercicio consiste en **dibujar ese mapa con nombres y apellidos** para tu país, tu sector y tu modelo de negocio:

- ☐ ¿Qué agencias realmente te pueden regular?
- ☐ ¿En qué cámaras y espacios ya estás sentado... y en cuáles deberías estar?
- ☐ ¿Qué ONGs, universidades o centros de estudio marcan agenda en temas de datos, IA, competencia, inclusión financiera?
- ☐ ¿Quiénes son los periodistas y medios que amplifican (o distorsionan) la conversación?

En "[El desarrollo del retail media network](#)" mostramos que, cuando un retailer decide transformarse en medio, entra a un juego donde participan agencias, anunciantes, reguladores de publicidad, autoridades de datos, plataformas de medición. Este mapa permite entender que algo similar ocurre en lo regulatorio: cambiar de rol (por ejemplo, de retailer a marketplace, o de plataforma a player fintech) no sólo cambia el modelo de negocio; **cambia el mapa de stakeholders con los que tenés que dialogar.**

Para un policy maker, este mismo mapa se puede leer al revés: ¿con quién estoy hablando hoy cuando diseño normas para el ecosistema digital? ¿Estoy escuchando sólo a incumbentes o también a startups, a organizaciones de derechos digitales, a academia? ¿Qué tan conectados estoy con lo que está pasando en países vecinos que enfrentan los mismos dilemas?

Integrado con IA-Unificada, este mapa de stakeholders puede convertirse en algo más que una foto estática:

- Se puede alimentar con información pública sobre consultas abiertas, proyectos de ley, comunicados de autoridades o pronunciamientos de cámaras.
- Se pueden detectar patrones (“este regulador cita sistemáticamente a tal organismo internacional”, “esta ONG influye mucho en la agenda de datos”).
- Se puede anticipar cuándo es el momento de participar en un debate y con qué argumentos, conectando este libro con los hallazgos y datos de [*“El boom del comercio electrónico”*](#), [*“El arribo de las tecnologías exponenciales”*](#) y [*“El ecosistema emprendedor”*](#).

El mensaje de fondo es simple: **no hay estrategia regulatoria sostenible sin estrategia de relaciones en red**. El mapa de stakeholders convierte esa intuición en una hoja de trabajo concreta.

Checklist de regulatory readiness para proyectos digitales

La meta de este checklist no es convertir a nadie en abogado exprés, sino ofrecer una **lista mínima de preguntas incómodas** que todo proyecto digital debería hacerse antes de escalar. Si el *Radar de riesgos regulatorios* y el *Risk-Impact Canvas* te ayudan a ver el mapa completo, este checklist es el equivalente a mirar tu propia mochila y preguntarte: “¿con qué estoy saliendo a la ruta?”.

En otros libros de la colección *Génesis de un Futuro Digital* fuimos desarmando las piezas de la experiencia digital, de los modelos colaborativos y de las tecnologías exponenciales. Aquí las miramos desde un solo ángulo: **¿qué necesito tener como mínimo en orden para no estrellarme con el regulador... o con mi propio usuario?**

La propuesta es sencilla: usar este checklist como **ritual de proyecto**. Cada vez que vas a lanzar, escalar o cambiar algo importante —un nuevo país, una nueva vertical, una nueva funcionalidad, una nueva integración de IA— sentarte con tu equipo (negocio, producto, datos, legal/compliance, tecnología) y recorrer estos bloques:

- ☐ Datos personales y privacidad.
- ☐ Derechos del consumidor digital.
- ☐ Pagos y fintech.
- ☐ Operaciones *cross-border* y aduanas/fiscalidad.

- Uso de IA y decisiones automatizadas.
- Cultura interna y gobierno del riesgo regulatorio.

No se trata de marcar todo “sí” como si fueran casilleros de auditoría; se trata de **hacer visibles los huecos** y decidir conscientemente qué vas a abordar ahora, qué en seis meses y qué requiere ayuda externa.

1. Datos personales y privacidad:

Del “llenar casilleros” al data trust flywheel

En [*“La revolución de los datos”*](#) y en [*“El arribo de las tecnologías exponenciales”*](#) mostramos que la materia prima del ecosistema digital ya no son sólo productos o servicios, sino **datos en movimiento**. El problema: esos datos no son neutros, ni infinitos, ni “gratis”. Vienen con derechos, expectativas y reglas de juego.

Checklist mínimo para datos y privacidad:

□ **Inventario de datos**

- ¿Sabemos qué datos recolectamos en cada punto de contacto? (registro, navegación, compra, servicio posventa, programas de fidelidad, apps, sensores, etc.)
- ¿Distinguimos entre datos personales, datos sensibles y datos meramente técnicos/operativos?
- ¿Tenemos claro qué datos son realmente necesarios para el servicio y cuáles son “nice to have” que podríamos no recolectar?

□ Base legal y propósito

- Para cada gran flujo de datos, ¿podemos responder con una frase clara: *para qué* los recolectamos y *en base a qué* (consentimiento, contrato, obligación legal, interés legítimo, etc.)?
- ¿Esa base legal se condice con lo que decimos en nuestra política de privacidad y con la experiencia real de usuario? (lo que prometemos en papel tiene que dialogar con la interfaz, como trabajamos en [*“El consumidor, la experiencia del usuario y el enfoque en la interfaz y usabilidad”*](#)).

□ Gobernanza y acceso

- ¿Quién decide internamente qué nuevos usos se hacen de los datos? ¿Existe algún comité o al menos una “ventanilla” donde se discutan usos no previstos originalmente?
- ¿Sabemos quién tiene acceso a qué datos (internamente y a nivel de proveedores/partners) y con qué controles?

□ Gestión de incidentes y derechos del titular

- ¿Tenemos un proceso por escrito —aunque sea simple— para responder a solicitudes de acceso, rectificación, eliminación u oposición de usuarios?
- ¿Sabemos qué hacer si hay una brecha de seguridad? ¿Quién lidera, a quién avisamos, en qué plazos?

Si en este bloque la mayoría de las respuestas es “no sé” o “lo vemos con IT”, el data trust flywheel del que hablamos en *El arribo de las tecnologías exponenciales*

simplemente no tiene de dónde arrancar. El mensaje del checklist es claro: **sin un mínimo de gobernanza de datos, no hay ni confianza ni escalabilidad.**

2. Derechos del consumidor digital: Prometer menos, cumplir más

En *El boom del comercio electrónico* y en la saga *#RetailReset* aparece una tensión recurrente: la tentación de prometer todo en la landing y luego negociar con la realidad en operaciones. Desde la perspectiva regulatoria, eso se traduce en **riesgo de prácticas engañosas, cláusulas abusivas y experiencias que erosionan la confianza.**

Checklist mínimo de consumidor:

□ Términos y condiciones claros y legibles

- ¿Nuestros T&Cs están redactados en lenguaje comprensible para un humano promedio, o parecen escritos sólo para un juez?
- ¿Las cláusulas más sensibles (limitaciones de responsabilidad, plazos de retracto, restricciones particulares) están destacadas o escondidas?
- ¿Coinciden lo que dicen los T&Cs con lo que muestra la interfaz en cada paso del proceso de compra? (Esto conecta directamente con las discusiones de UX que trabajamos en *El consumidor, la experiencia del usuario...*).

❑ **Política de cambios, devoluciones y retracto**

- ¿Hay una política clara, visible y fácil de encontrar sobre cambios y devoluciones?
- ¿Respetas los mínimos legales del país donde operamos (plazos de retracto, productos excluidos, condiciones de devolución)?
- ¿Los equipos de atención al cliente conocen esa política y tienen herramientas para aplicarla?

❑ **Información precontractual y durante la experiencia**

- ¿El usuario sabe cuánto va a pagar, qué incluye el precio, qué costos adicionales puede haber (envío, impuestos, fees)?
- ¿Las promesas de stock, plazos y cobertura logística están alineadas con la capacidad real de la operación?

❑ **Canales de reclamo y resolución de conflictos**

- ¿Existe un canal claro para reclamos (más allá de redes sociales) y un proceso interno para darles seguimiento?
- ¿Tenemos criterios mínimos de respuesta (tiempos, compensaciones, escalamiento de casos)?

Si este bloque es débil, no sólo sube el riesgo de conflictos con autoridades de consumo; también se resiente la **recurrencia y recomendación**, dos piezas clave del flywheel que trabajamos en *El boom del comercio electrónico* y *Quantum/Flywheel Retail*.

3. Pagos y fintech: Dinero ajeno, reglas serias

Cuando un proyecto digital toca dinero de terceros, el nivel de exigencia sube varios escalones. En *La implementación de los modelos Unified & Collaborative Commerce* mostramos cómo, al sumar billeteras, *checkout* propio o crédito al consumo, un retailer deja de ser “sólo retailer” y entra al terreno financiero.

Checklist mínimo para pagos/fintech:

- ❑ **Modelo claro de rol en la cadena de pagos**
 - ¿Somos meros integradores de un gateway externo, agregadores, emisores de valor, proveedores de crédito, o todo a la vez?
 - ¿Entendemos qué rol jurídico tiene cada actor (banco, procesador, fintech, marketplace) y qué regulador lo mira?
- ❑ **Licencias y registros**
 - ¿Nuestro modelo requiere licencia específica (institución de pago, emisor de dinero electrónico, proveedor de crédito, etc.) o podemos operar bajo licencias de terceros?
 - Si usamos licencias de partners, ¿hay contratos sólidos que definan quién responde por qué?
- ❑ **KYC/AML y prevención de fraude**
 - ¿Tenemos políticas mínimas de conocimiento del cliente (KYC) y prevención de lavado (AML), aunque las implemente un tercero?

- ¿Qué mecanismos usamos para detectar transacciones sospechosas, suplantación de identidad, usos fraudulentos?

□ **Gestión de contracargos y disputas**

- ¿Tenemos reglas claras para manejar *chargebacks* y disputas? ¿Quién asume el costo en cada tipo de ticket?
- ¿Nuestros términos reflejan esa asignación de responsabilidades?

Aquí el checklist se cruza directamente con el **marco 4R de regulación adaptativa** que proponemos en este libro: los modelos fintech mal entendidos disparan riesgo sistémico y reacción regulatoria dura; los bien diseñados, con pilotos y reglas claras, terminan convertidos en regulación habilitante, como contamos en varias experiencias del capítulo de sandboxes y en diálogo con *El arribo de las tecnologías exponenciales*.

4. Operaciones cross-border y aduanas/fiscalidad: El mundo no es una sola jurisdicción

En *"El boom del comercio electrónico"* ya vimos cómo el sueño del ecommerce *cross-border* chocaba con la realidad de aduanas, impuestos y normas inconsistentes. Hoy, con marketplaces, plataformas SaaS y servicios totalmente digitales, el problema es más fino: **¿dónde se considera que "ocurre" la operación y quién quiere cobrar qué?**

Checklist mínimo *cross-border*:

□ **Mapa de jurisdicciones relevantes**

- ¿En qué países tenemos usuarios, clientes, proveedores o infraestructura (almacenes, servidores, oficinas)?
- ¿Entendemos qué implica eso en términos de legislación aplicable (consumo, datos, impuestos)?

□ **Umbral de minimis y tratamiento aduanero**

- Si vendemos productos físicos *cross-border*, ¿sabemos cuál es el umbral de minimis para envíos en cada país (valor por debajo del cual hay exenciones o tratamiento simplificado)?
- ¿Informamos a los consumidores sobre posibles cargos de aduana, impuestos locales o tiempos de retención?

□ **Esquema impositivo**

- ¿Sabemos dónde se considera que se presta el servicio (origen/destino) y qué IVA/impuestos aplican?
- ¿Hay riesgo de doble imposición o estamos usando estructuras diseñadas hace años y que ya no conversan con los nuevos marcos de fiscalidad digital?

□ **Contratos y atención al cliente *cross-border***

- ¿Nuestros T&Cs indican claramente qué ley aplica y qué jurisdicción es competente?
- ¿Tenemos capacidad real de atender reclamos desde otros países (idioma, canales, tiempos)?

5. Uso de IA y decisiones automatizadas: Del experimento al accountability

Checklist mínimo para IA:

☐ Mapa de dónde usamos IA hoy

- ¿Sabemos en qué procesos ya hay modelos de IA (generativa o no) tomando decisiones o influyendo en ellas? (recomendaciones, scoring, precios, moderación de contenidos, segmentación, validación de identidad, etc.)
- ¿Hay un responsable claro de cada caso de uso?

☐ Tipo de decisión e impacto en personas

- ¿La IA influye en decisiones que afectan acceso a crédito, trabajo, educación, salud, servicios esenciales o precios diferenciados?
- ¿Podemos explicar, al menos en términos generales, cómo se toma esa decisión? (Si la respuesta es “no”, estamos en zona roja).

☐ Datos de entrenamiento y sesgos

- ¿Tenemos alguna visibilidad sobre qué datos se usaron o se usan para entrenar los modelos más críticos?
- ¿Hemos hecho pruebas internas para detectar sesgos evidentes o efectos discriminatorios?

☐ Supervisión humana y mecanismos de revisión

- ¿Existe la posibilidad de que una persona revise y corrija decisiones

automatizadas en casos sensibles?

¿Los usuarios pueden cuestionar o apelar decisiones tomadas por sistemas automatizados?

☐ Documentación y principios

- ¿Tenemos al menos en borrador una política interna sobre el uso responsable de IA (aunque no se llame así), alineada con principios como los que trabajan la OCDE y la UNESCO y que analizamos en *El arribo de las tecnologías exponenciales*?

Si aquí abundan los “no sé”, estás básicamente montando una **caja negra regulatoria**. El aprendizaje de los últimos déjà vu que recorre este libro es simple: lo que hoy parece “innovación imparable” puede ser mañana un caso emblemático de abuso algorítmico.

6. Cultura interna y gobierno del riesgo regulatorio

Por último, un bloque transversal: **no hay checklist que aguante si la organización vive en modo “cumplamos lo justo para no tener multas”**. En toda la colección *Génesis de un Futuro Digital* aparece el mismo patrón: los ecosistemas que mejor funcionan son los que tienen **criterio y propósito**, no sólo procesos.

Checklist mínimo cultural:

- ☐ ¿Existe al menos una vez al año una conversación estratégica sobre riesgos legales/regulatorios en el comité ejecutivo

- ❑ ¿Hay alguien con mandato claro para coordinar temas regulatorios (legal, compliance, asuntos públicos, risk officer) y para dialogar con cámaras y reguladores?
- ❑ ¿Usamos herramientas como el radar de riesgos, el risk-impact canvas y este checklist como insumo periódico, o sólo cuando hay crisis?
- ❑ ¿Formamos a líderes de producto, datos, marketing y operaciones para que entiendan el marco regulatorio básico de su rol? (aquí se cruzan las iniciativas formativas que contamos en [*"El ecosistema emprendedor..."*](#) y en [*"El boom del comercio electrónico"*](#)).
- ❑ ¿Estamos explorando el uso de IA-unificada y human augmented AI como soporte para monitorear cambios normativos, sintetizar información y preparar escenarios, como desarrollamos en este libro y en [*"El arribo de las tecnologías exponenciales"*](#)?

Si la mayoría de las respuestas es "no" o "todavía no", el problema ya no es jurídico: es de **gobernanza**. El resto de las herramientas del libro —radar, matrices, marcos 4R, casos cortos— están justamente pensadas para ayudarte a mover estas respuestas hacia "sí" de manera gradual y consciente.

Preguntas que deberías hacerle a tu abogada o abogado antes de lanzar

Las startups y compañías digitales suelen caer en dos extremos: o no consultan nunca con abogados (“total, después se ve”), o los consultan tarde, cuando ya hay conflicto, sanción o pérdida de reputación. Entre ambos extremos existe una tercera vía —más madura, más estratégica— que encaja con el espíritu de toda la colección *Génesis de un Futuro Digital*: **usar el criterio jurídico como herramienta de diseño de negocio.**

No se trata de juridificar la innovación, sino de integrarla con inteligencia al proceso de desarrollo, como una capa más del *Human Augmented Management* que atraviesa esta saga: la combinación de criterio humano, inteligencia colectiva y datos para tomar decisiones con conciencia de impacto.

Por eso, antes de lanzar o escalar un proyecto digital, conviene sentarse con el equipo legal o con una asesora/asesor externo y recorrer este conjunto de preguntas. No son un examen: son disparadores que ayudan a detectar vacíos, incoherencias o riesgos que todavía pueden corregirse sin costo reputacional ni sanciones.

1. ¿Qué regula realmente mi modelo de negocio?

La pregunta más básica suele ser la más ignorada. Muchas veces, el equipo fundador o directivo **no tiene**

claro bajo qué ley o régimen opera su producto. En *El boom del comercio electrónico* vimos que los pioneros confundían “estar en internet” con “estar fuera del comercio tradicional”. Hoy pasa algo parecido con IA, cripto, tokenización o retail media: se asume que la novedad tecnológica cambia el marco jurídico, cuando en realidad lo expande.

Preguntale a tu abogada/o:

- ☐ ¿Qué leyes o autoridades me miran realmente (consumo, datos, fintech, competencia, publicidad, fiscalidad)?
- ☐ ¿Mi producto es “nuevo” o una versión digital de algo que ya existía y por tanto tiene jurisprudencia previa?
- ☐ ¿Existen reglas implícitas o prácticas de mercado (soft law, autorregulación, códigos de cámaras) que me conviene adoptar preventivamente?

2. ¿Qué podría salir mal en la relación con mis usuarios o clientes?

Toda relación comercial tiene zonas de fricción: información incompleta, expectativas incumplidas, logística fallida, cobros duplicados, errores de precio o publicidad confusa.

Preguntale a tu abogada/o:

- ☐ ¿Qué escenarios de conflicto son más probables según mi tipo de usuario y producto?
- ☐ ¿Mis Términos y Condiciones realmente me protegen

en esos escenarios?

- ☐ ¿Qué obligaciones mínimas de información y transparencia tengo que cumplir para evitar reclamos recurrentes?
- ☐ ¿Qué tipo de evidencia necesito conservar para demostrar que informé correctamente?

3. ¿Dónde empiezo a asumir responsabilidad aunque nadie me la exija aún?

Cuando un negocio se vuelve plataforma, deja de ser una relación uno-a-uno para convertirse en un sistema donde las responsabilidades se distribuyen entre actores. Aunque la ley no sea clara todavía, hay deberes de diligencia mínima que conviene asumir voluntariamente.

Preguntale a tu abogada/o:

- ☐ ¿Qué responsabilidades emergentes podría tener aunque no estén expresas (por ejemplo, corresponsabilidad de tratamiento de datos, curaduría de contenido, retención de impuestos)?
- ☐ ¿Existen precedentes en otros países que anticipen hacia dónde se moverá la interpretación local?
- ☐ ¿Cómo puedo documentar que la empresa actúa de buena fe y con diligencia razonable, aunque la regulación todavía no lo exija?

4. ¿Cómo manejo datos e IA sin abrir una caja de Pandora?

El manejo de datos y la adopción de IA ya no son temas técnicos: son vectores de riesgo reputacional y normativo. En *El arribo de las tecnologías exponenciales* hablamos del *Data Trust Flywheel*: la confianza en los datos como activo central.

Preguntale a tu abogada/o:

- ☐ ¿Qué categorías de datos manejo y bajo qué base legal los proceso?
- ☐ ¿Estoy aplicando modelos de IA en decisiones que podrían ser impugnadas (precios, crédito, empleo, moderación, scoring)?
- ☐ ¿Existe política interna o lineamiento de “uso responsable de IA”?
- ☐ ¿Qué debo documentar para demostrar trazabilidad y posibilidad de explicación si alguien cuestiona una decisión automatizada?

5. ¿Qué obligaciones tengo en materia fiscal, laboral y de competencia?

En *“El boom del comercio electrónico”* y en los capítulos sobre fiscalidad digital mostramos que buena parte del “caos regulatorio” regional se debe a errores de diagnóstico: empresas que creen no estar alcanzadas por ciertos tributos, startups que no clasifican correctamente a sus colaboradores, o

plataformas que desconocen que están adquiriendo posición dominante en nichos específicos.

Preguntale a tu abogada/o:

- ☐ ¿Mi modelo genera obligaciones de retención o percepción de impuestos?
- ☐ ¿Estoy clasificado correctamente ante los fiscos locales y ante las aduanas si opero *cross-border*?
- ☐ ¿Qué implica tener contratos con freelancers o repartidores? ¿Podría recalificarse como relación laboral?
- ☐ ¿Hay riesgo de concentración o abuso de posición dominante en alguno de mis segmentos?

6. ¿Qué acuerdos necesito (o conviene) documentar desde el inicio?

No todos los acuerdos requieren un contrato formal de 40 páginas, pero todo negocio necesita **definir por escrito los mínimos con sus socios críticos**.

Preguntale a tu abogada/o:

- ☐ ¿Qué acuerdos o políticas necesito antes de escalar (socios fundadores, partners estratégicos, marketplace, proveedores de pago, influencers)?

- ☐ ¿Qué puedo manejar con políticas internas o términos estandarizados, y qué requiere contrato a medida?
- ☐ ¿Dónde necesito cláusulas de confidencialidad o propiedad intelectual específicas?
- ☐ ¿Qué aspectos conviene revisar si me estoy integrando en una red de Unified & Collaborative Commerce o en un esquema de Retail Media?

7. ¿Estoy preparado para hablar con el regulador si aparece?

En *Los déjà vu regulatorios* vimos que el gran salto cualitativo en los ecosistemas maduros es pasar del miedo al regulador a **la cooperación inteligente**. La clave: estar listo para explicar tu modelo de negocio con transparencia y datos.

Preguntale a tu abogada/o:

- ☐ ¿Qué relato institucional voy a usar si el regulador me convoca?
- ☐ ¿Tengo material explicativo que muestre mis mecanismos de cumplimiento?
- ☐ ¿Puedo ofrecer ejemplos de buenas prácticas del sector o de autorregulación que adopto?
- ☐ ¿Quién debe ser la cara visible de la empresa ante autoridades o cámaras (GC, CEO, asuntos públicos)?

8. ¿Cómo mantengo esta conversación viva?

Finalmente, el mayor error es creer que la regulación es una “foto” que se revisa una vez por año. En realidad, es una película que cambia todos los meses. En el marco de *Human Augmented AI* que recorre esta colección, tu equipo legal y tu IA-Unificada pueden convertirse en un **copiloto permanente**: monitorea boletines, clasifica cambios por tema, alerta al equipo, y ayuda a priorizar.

Preguntale a tu abogada/o:

- ☐ ¿Podemos establecer un *radar regulatorio* trimestral para revisar novedades?
- ☐ ¿Qué alertas tempranas deberíamos automatizar?
- ☐ ¿Cómo integramos IA-Unificada al seguimiento de normas y jurisprudencia?
- ☐ ¿Qué instancias externas (cámaras, asociaciones, foros) vale la pena frecuentar para anticipar cambios y participar en su diseño?

El valor de preguntar bien

Las respuestas cambiarán según el tamaño de la organización y la madurez regulatoria del país, pero las preguntas —estas ocho— deberían ser universales. En el fondo, son una forma de ponerle criterio humano al vértigo tecnológico, de conectar lo jurídico con lo estratégico, y de convertir al derecho en aliado de la innovación, no en freno.

Como recuerda la cita que abre *El arribo de las tecnologías exponenciales*: “no hay progreso sin reglas, ni reglas que sobrevivan sin progreso”. Preguntar a tiempo es, en sí mismo, una forma de innovar.

GÉNESIS

DE UN FUTURO DIGITAL

GÉNESIS

DE UN FUTURO DIGITAL



Agradecimientos

Cada libro de esta colección es un puente entre generaciones de innovadores, académicos, reguladores y soñadores digitales. Pero este volumen, en particular, nació del diálogo constante entre quienes creyeron que el ecosistema no puede madurar sin reglas claras, éticas y compartidas.

Quiero agradecer, en primer lugar, a todos los líderes que, con su tiempo y generosidad, nos permitieron escuchar la historia desde dentro. Por compartir sus visiones sobre la responsabilidad de las plataformas y el equilibrio entre libertad e institucionalidad, por haber tendido los primeros puentes entre la innovación y la regulación, por recordarnos que la confianza digital se construye colaborando, no compitiendo; y por su compromiso con la creación de entornos regulatorios que promuevan la innovación sin limitarla con ello.

Agradezco también al equipo editorial de ***Génesis de un Futuro Digital***, que hizo posible que este libro —y los veinticuatro que lo acompañan— se transformen en un

relato colectivo del ecosistema iberoamericano. A cada investigador, diseñador, editor y productor que participó en este proceso, gracias por su talento, su paciencia y su convicción.

A mis compañeros de camino en el **eCommerce Institute** y a todos los líderes del ecosistema digital regional, por seguir impulsando la conversación pública sobre los desafíos éticos y normativos que nos interpelan como sociedad.

A quienes, desde los organismos públicos, los congresos o la academia, están trabajando día a día para que la regulación del futuro sea un instrumento de inclusión y no una barrera.

Y, sobre todo, a los pioneros que se animaron a innovar cuando no existían leyes, manuales ni garantías. Ellos —y ellas— demostraron que el progreso no espera permisos: los crea.

Este libro es para ellos. Para quienes se animan a construir el futuro digital, sabiendo que regularlo también es una forma de soñarlo.

Gracias de corazón a todos los que lo hacen posible.

Marcos Pueyrredon

GÉNESIS

DE UN FUTURO DIGITAL

Disclaimer:

Nuestros conceptos se sustentan en análisis recientes y testimonios de expertos que fueron entrevistados para esta edición y reservados en una playlist en YouTube y en Spotify que se puede consultar dentro de la web oficial de Génesis de un Futuro Digital o en nuestros canales, dentro de cada plataforma. También se han rescatado testimonios de expertos que se publicaron en otros medios, en cuyo caso, se cita debidamente la fuente. También recuperamos estudios de mercado latinoamericanos de diversas fuentes de autoridad, previamente curados por el área eContentLAB del eCommerce Institute. Cada sección de este libro viviente integra estas evidencias para ofrecer un panorama riguroso y reflexivo, en primera persona, que cumple las normas APA al final de cada obra de la colección.

A continuación, compartimos las debidas referencias.

Ante cualquier consulta u observación por las mismas, contáctenos por correo electrónico: econtentlab@ecommerce.institute

Algunas imágenes de este libro fueron generadas con herramientas de inteligencia artificial. Son utilizadas exclusivamente con fines ilustrativos y conceptuales. Cualquier semejanza con personas, marcas o lugares reales es mera coincidencia.

GÉNESIS

DE UN FUTURO DIGITAL



Referencias

1. Cramer-Flood, E. (2024, 06 de septiembre). *Worldwide Retail Ecommerce Forecast 2024 Midyear Update*. eMarketer <https://content-naf.emarketer.com/worldwide-retail-ecommerce-forecast-2024-midyear-update>
2. Ceurvels, M. (2021, 14 de julio). *Latin America Ecommerce Forecast 2021*. Insider Intelligence (eMarketer) <https://www.emarketer.com/content/latin-america-ecommerce-forecast-2021>
3. Daza Jaller, L.; Gaillard, S. & Molinuevo, M. (2020). *The regulation of digital trade: Key policies and international trends*. World Bank <https://documents1.worldbank.org/curated/en/998881578289921641/pdf/The-Regulation-of-Digital-Trade-Key-Policies-and-International-Trends.pdf>
4. Federal Reserve Bank of St. Louis (2024, 19 de septiembre). *Internet users: All income levels for Latin America and Caribbean* <https://fred.stlouisfed.org/series/ITNETUSERP2LCN>

5. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). (1996). *Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) con su nuevo artículo 5 bis aprobado en 1998*. Naciones Unidas https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_commerce
6. eLíderes Podcast x25 (2024, 18 de diciembre). Entrevista a Eugenio Sánchez - *La regulación de la comunicación y la tecnología en Colombia* [Video] YouTube <https://www.youtube.com/watch?v=WoFLhz3ixOU>
7. Ministerio de Transportes y Telecomunicaciones (2023, 19 de abril). *Ley N.º 21.553: Regula las aplicaciones de transporte remunerado de pasajeros y los servicios que a través de ellas se presten*. Biblioteca del Congreso Nacional de Chile <https://www.bcn.cl/leychile/navegar?idNorma=1191380>
8. Melo, L. (2014, 28 de noviembre). *Maquiagem de preços lidera reclamações na Black Friday*. Exame <https://exame.com/negocios/maquiagem-de-precos-lidera-reclamacoes-na-black-friday/>
9. Vilela, V. (2013, 08 de noviembre). *Black Friday brasileira ganha Código de Ética para proteger consumidor*. Ecommerce Brasil <https://www.ecommercebrasil.com.br/noticias/black-friday-brasileira-ganha-codigo-etica-protoger-consumidor>

10. eLíderes Podcast x25 (2025, 28 de enero). Entrevista a Ludovino Lopes – *La creación de un marco regulatorio para el ecosistema digital* [Video] YouTube <https://www.youtube.com/watch?v=khuBa5p8iVo>
11. Borges Vieira, F. (2013, 22 de mayo). *Nuevas reglas para contratación en el comercio electrónico*. TI Inside <https://tiinside.com.br/es/22/05/2013/novas-regras-para-contratacao-no-comercio-eletronico/>
12. Pereira, P. & Jungblut, C. (2014, 25 de marzo). *Câmara aprova Marco Civil da Internet e projeto segue para o Senado*. O Globo <https://oglobo.globo.com/politica/camara-aprova-marco-civil-da-internet-projeto-segue-para-senado-11984559>
13. Congreso de la Nación Paraguaya (2013, 26 de febrero). *Ley N° 4868/2013 de Comercio Electronico, Paraguay* <https://www.wipo.int/wipolex/es/legislation/details/22955>
14. DocuSign (2025, 20 de junio). *NOM 151: qué es y cómo se relaciona con las firmas electrónicas* <https://www.docuSign.com/es-mx/blog/nom-151>
15. argentina.gb.ar (2024, 15 de enero). *Argentina logró la nueva adecuación por parte de la Unión Europea para el flujo internacional de datos personales* <https://www.argentina.gob.ar/noticias/argentina-logro-la-nueva-adecuacion-por-parte-de-la-union-europea-para-el-flujo>

16. Congreso de la Nación Argentina (2001, 14 de diciembre). *Ley 25.506* <https://www.argentina.gob.ar/normativa/nacional/ley-25506-70749>
17. Güisa Díaz, C. & Ramírez Cubillos, K. (2022, 05 de septiembre). *Comercio electrónico transfronterizo: un dinamizador de la economía global y nacional*. Cámara Colombiana de Comercio Electrónico <https://ccce.org.co/noticias/comercio-electronico-transfronterizo-un-dinamizador-de-la-economia-global-y-nacional>
18. European Union (2022, 19 de octubre). *Reglamento de Servicios Digitales* <https://eur-lex.europa.eu/ES/legal-content/summary/digital-services-act.html#:~:text=DOCUMENTO%20PRINCIPAL,1-102>
19. eLíderes Podcast x25 (2025, 25 de febrero). Entrevista a Alejandro Prince - *La creación de la CACE, institucionalizar el ecommerce* [Video] YouTube <https://www.youtube.com/watch?v=hdghurCLB6o>
20. eLíderes Podcast x25 (2025, 27 de febrero). Entrevista a Jacobo Cohen Imach - *Argentina pionera en protección de datos personales* [Video] YouTube <https://www.youtube.com/watch?v=ALKoH0ro-Wc>
21. Diario TAG (2022, 28 de junio). *La Aduana denunció a Mercado Libre por “infracciones en importaciones” de posnet* <https://www.diariotag.com/140410-la-aduana-denuncio-a-mercado-libre-por-infracciones-en-importaciones-de-posnet>

22. Media Auditors (2025, 02 de octubre). Influencer marketing en LATAM: cifras, oportunidades y claves para anunciantes <https://www.mauditors.com/influencer-marketing-en-latam-cifras-oportunidades-y-claves-para-anunciantes/>
23. SociallyIn (n.d.). Influencer marketing statistics: 2025 ROI & engagement benchmarks <https://sociallyin.com/influencer-marketing-statistics/>
24. Goldfish (2025, 08 de abril). Estado de marketing de influencers 2025 <https://www.goldfish.com.co/en-us/post/estado-de-marketing-de-influencers-2025>
25. Pel (2025, 15 de julio). Tendencias de influencer marketing en México para 2025 <https://pel.com.mx/tendencias-de-influencer-marketing-en-mexico-para-2025/>
26. Federal Trade Commission (2023, 29 de junio). Federal Trade Commission announces updated advertising guides to combat deceptive reviews and endorsements <https://www.ftc.gov/news-events/news/press-releases/2023/06/federal-trade-commission-announces-updated-advertising-guides-combat-deceptive-reviews-endorsements>
27. Federal Trade Commission (2019, noviembre). Disclosures 101 for social media influencers <https://www.ftc.gov/business-guidance/resources/disclosures-101-social-media-influencers>

28. Procuraduría Federal del Consumidor (n.d.). *Guía de publicidad para influencers* <https://www.profeco.gob.mx/influencers/doc/Profeco-GuiadePublicidadparaInfluencers.pdf>
29. Banco Mundial (n.d.). *Account ownership at a financial institution or with a mobile-money-service provider (% of population ages 15+) - Latin America & Caribbean* <https://data.worldbank.org/indicator/FX.OWN.TOTL.ZS?locations=ZJ&>
30. Servicio de Administración Tributaria (n.d.). *Plataformas tecnológicas: Personas físicas* https://www.sat.gob.mx/minisito/PlataformasTecnologicas/PersonasFisicas/personasfisicas_inicio.html
31. Ayres, M. (2024, 02 de abril). *Brazil's Pix payments are killing cash. Are credit cards next?* Reuters <https://www.reuters.com/business/finance/brazils-pix-payments-are-killing-cash-are-credit-cards-next-2024-04-02/>
32. Ipsos (2024, 11 de julio). *Estudio Medios de Pago en Latinoamérica – 2º edición, 2024* <https://www.ipsos.com/es-ar/estudio-medios-de-pago-en-latinoamerica-2024>
33. Comisión Europea (n.d.). *About the Digital Markets Act. Digital Markets Act.* Recuperado el 10 de octubre de 2025, de https://digital-markets-act.ec.europa.eu/about-dma_en

34. Levy-Carciente, S.; Leonardi, A.; Bongiovanni, J.; Beltramone, F.; Velarde, J.; Siles, L.; Lenhart, W.; Resende, P.; Piaia Abreu, M.; Horst, B.; Durán, N.; Chacón, C.; Calle, A.; Torrealba, O.; Loría, L.; Méndez, E.; Andrade, J.; Verdecia, G.; Vélez, D.;... & Eilender, D. (2025). *Índice de Burocracia 2025*. Adam Smith Center for Economic Freedom, Florida International University <https://freedom.fiu.edu/wp-content/uploads/2025/09/Indice-de-Burocracia-2025-Digital-Final-compressed.pdf>
35. Crowell (2025, 28 de enero). *Latin American Data Privacy* <https://www.crowell.com/en/insights/publications/latin-american-data-privacy>
36. Enforcement Tracker (n.d.). *Fines statistics*. Recuperado el 10 de octubre de 2025, de <https://www.enforcementtracker.com/?insights>
37. eLíderes Podcast x25 (2025, 18 de febrero). Entrevista a Yerka Yukich - *Código de buenas prácticas: fundamental para la autorregulación del ecosistema* [Video] YouTube <https://www.youtube.com/watch?v=pKdhF4uMxOI>
38. Good Discuss (2025, 20 de septiembre). *How blockchain is revolutionizing ePayment security and reducing international transaction fraud* <https://www.gooddiscuss.com/en/financial-information/673881.html>

39. Saldaña, S. (2024, 02 de abril). *Mercado Libre elimina millones de productos por violar las reglas; en México el principal motivo es claro: los productos falsos*. Xataka México <https://www.xataka.com/comercio-electronico/mercado-libre-elimina-millones-productos-violar-reglas-mexico-principal-motivo-claro-productos-falsos>
40. Oficina Española de Patentes y Marcas (OEPM). (n.d.). *Amazon - Informe de Protección de Marca 2024*. Recuperado el 10 de octubre de 2025, de <https://stopfalsificaciones.oepm.es/novedades-y-publicaciones/novedades/617a78c8-0ae5-11f0-898c-005056bb6786/>
41. Mercado Libre (2022, 21 de octubre). *Mercado Libre rebuttal 2022 Special 301 out-of-cycle review of notorious market* https://downloads.regulations.gov/USTR-2022-0010-0047/attachment_1.pdf
42. Oficina Española de Patentes y Marcas (OEPM). (n.d.). *Amazon - Informe de Protección de Marca 2024*. Recuperado el 10 de octubre de 2025, de <https://stopfalsificaciones.oepm.es/novedades-y-publicaciones/novedades/617a78c8-0ae5-11f0-898c-005056bb6786/>
43. Wirth, G. (2020, 05 de noviembre). *For Mercado Libre's GC, the goal of enabling business keeps his legal team focused & innovating*. Thomson Reuters <https://www.thomsonreuters.com/en-us/posts/legal/forum-fall-2020-jaco-mercadolibre-gc/>

44. Meza, C. & Durán, L. (2025, 14 de julio). *The impact that digital service taxes have had on Latin America*. Bloomberg <https://news.bloombergtax.com/tax-management-international/do-not-publish-63>
45. eLíderes Podcast x25 (2025, 04 de agosto). Entrevista a Verónica Pinazo - *Democratización de internet: la primera gran ola* [Video] YouTube <https://www.youtube.com/watch?v=FotVDIQMqVU>
46. Pino, M. (2025, 10 de junio). Yerka Yukich: “El CyberDay contribuye al profesionalismo del comercio electrónico”. Agenda Logística. Recuperado el 13 de octubre de 2025, de <https://www.agendalogistica.cl/camara-de-comercio-comercio-electronico-cyberday/yerka-yukich-el-cyberday-contribuye-al-profesionalismo-del-comercio-electronico/1950680>
47. Microjuris (2022, 18 de mayo). Fallos: “Falso Hot Sale”. Se multa a la firma que consignó un precio anterior más elevado al que ofrecía en los días previos al Hot Sale, informando un porcentaje de descuento que no era tal, lo que induce al engaño y error en los consumidores <https://aldiaargentina.microjuris.com/2022/05/18/fallos-falso-hot-sale-se-multa-a-la-firma-que-consigno-un-precio-anterior-mas-elevado-al-que-ofrecia-en-los-dias-previos-al-hot-sale-informando-un-porcentaje-de-descuento-que-no-era-tal-lo-que/>

48. Errepar (2024, 14 de noviembre). *Multan a una empresa de electrodomésticos por publicidad engañosa durante el Hot Sale*. <https://documento.errepar.com/actualidad/multan-a-empresa-de-electrodomesticos-por-publicidad-enganosa-durante-el-hotsale-20241114175609613>
49. León, S. (2024, 14 de mayo). *Hot Sale 2024: ¿Cuáles son las empresas con más quejas ante Profeco?* Vanguardia <https://vanguardia.com.mx/informacion/hot-sale-2024-cuales-son-las-empresas-con-mas-quejas-ante-profeco-GPI1960464>
50. Servicio Nacional del Consumidor (SERNAC). (2025, 06 de octubre). *El SERNAC ha recibido más de 100 reclamos en la primera jornada del Cyber Monday*. Recuperado el 13 de octubre de 2025, de <https://www.sernac.cl/portal/604/w3-article-87381.html>
51. Olmedo Neri, R. A. (2024). *Influencers y publicidad. Implicaciones y regulación en América Latina*. Avatares de la Comunicación y la Cultura (28). Facultad de Ciencias Sociales UBA <https://publicaciones.sociales.uba.ar/index.php/avatares/article/view/9816>
52. Talip Pinarbasi, A. (2025, 07 de julio). *Requisitos de la FTC para los influencers: Directrices y normas*. Termly. Recuperado el 13 de octubre de 2025, de <https://termly.io/es/recursos/articulos/ftc-requirements-for-influencers/>

53. Cárdenas, L. (2025, 27 de febrero). *Mercado Libre gana demanda de A3D: Tribunal concluye que “no es el vendedor, distribuidor o comercializador de los productos”*. La Tercera. Recuperado el 13 de octubre de 2025, de <https://www.latercera.com/pulso-pm/noticia/mercado-libre-gana-demanda-de-a3d-tribunal-concluye-que-no-es-el-vendedor-distribuidor-o-comercializador-de-los-productos/FG3MH2LKNFEBNAJIQTM5E4KV74/>
54. Estadão Conteúdo (2024, 13 de octubre). *Mercado Livre passa de vilão a aliado do MP no combate à pirataria*. CNN Brasil. Recuperado el 13 de octubre de 2025, de <https://www.cnnbrasil.com.br/economia/negocios/mercado-livre-passa-de-vilao-a-aliado-do-mp-no-combate-a-pirataria/>
55. Sánchez Onofre, J. (2017, 28 de marzo). *Amazon y Mercado Libre operan con prácticas abusivas en México*. El Economista <https://www.eleconomista.com.mx/empresas/Amazon-y-MercadoLibre-operan-con-practicas-abusivas-en-Mexico-20170328-0111.html>
56. Soto Galindo, J. (2020, 19 de marzo). *Los conejos de Profeco: El caso de Amazon*. Recuperado el 13 de octubre de 2025, de <https://economicon.mx/blog/los-conejos-de-profeco-el-caso-de-amazon/>

57. Valencia, A. (2018, 05 de diciembre). *La SIC sanciona por cuarta vez a Linio Colombia, esta vez por más de \$350 millones*. Asuntos Legales. Recuperado el 13 de octubre de 2025, de <https://www.asuntoslegales.com.co/actualidad/la-sic-sanciona-por-cuarta-vez-a-linio-colombia-esta-vez-por-mas-de-350-millones-2802351>
58. Cifuentes Quintero, S. (2025, 09 de mayo). *Mercado Libre Colombia recibió millonaria multa: SIC la encontró responsable de uso indebido de datos sensibles de los usuarios*. Infobae <https://www.infobae.com/colombia/2025/05/09/sic-multa-a-mercado-libre-colombia-por-uso-indebido-de-datos-sensibles-la-sancion-supera-los-200-millones/>
59. Valora Analitik (2023, 21 de marzo). *Rappi responde a la millonaria sanción de la SIC por incumplimiento a consumidores*. Yahoo Finanzas. Recuperado el 13 de octubre de 2025, de <https://es-us.finanzas.yahoo.com/noticias/rappi-responde-millonaria-sancion-sic-023000428.html>
60. Carey, G. & Hara, K. (2023, 09 de agosto). *Interpretaciones del SERNAC sobre garantía legal, derecho a retracto y el ejercicio de otros derechos*. Carey. Recuperado el 13 de octubre de 2025, de <https://www.carey.cl/interpretaciones-del-sernac-sobre-garantia-legal-derecho-a-retracto-y-el-ejercicio-de-otros-derechos/>

61. Bojalil, P. & Vela-Treviño, C. (2019, 12 de febrero). *Despuntan las reformas en materia de protección de datos en América Latina*. Banco Interamericano de Desarrollo (BID). Recuperado el 13 de octubre de 2025, de <https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/>
62. Infobae (2014, 18 de diciembre). *La Justicia porteña avaló el impuesto a Netflix* <https://www.infobae.com/2014/12/18/1615919-la-justicia-portena-avalo-el-impuesto-netflix/>
63. León Pinedo, S. (2017, abril). *Tributación de la economía digital, ¿hacia un nuevo paradigma de establecimiento permanente (EP)?* Revista del Instituto Peruano de Derecho Tributario (62), 227–246 https://www.ipdt.org/uploads/docs/08_Rev62_SLP.pdf
64. Martínez, M.L. (2022, 28 de abril). *La Justicia Federal ordenó a Mercado Libre que embargue activos digitales de un demandado en una causa de seguridad social*. Palabras del Derecho. Recuperado el 13 de octubre de 2025, de <https://palabrasdelderecho.com.ar/articulo/3579/La-Justicia-Federal-ordeno-a-Mercado-Libre-que-embargue-activos-digitales-de-un-demandado-en-una-causa-de-seguridad-social>
65. iProfesional (n.d.). *AFIP y un fallo histórico para embargo de cuentas digitales: ¿Puede retener dinero de Mercado Pago o Ualá?* Tristán & Asociados <https://tristanyasociados.com/2022/09/afip-y-un-fallo-historico-para-embargo-de-cuentas-digitales-puede-retener-dinero-de-mercado-pago-o-uala/>

66. Red en Defensa de los Derechos Digitales (R3D). (2024, 31 de julio). *Suprema Corte de Estados Unidos protege a plataformas de redes sociales de la regulación estatal*. <https://r3d.mx/2024/07/31/suprema-corte-de-estados-unidos-protege-a-plataformas-de-redes-sociales-de-la-regulacion-estatal/>
67. Ámbito (2023, 09 de noviembre). *Alianza y Mercado Libre se unen para avanzar en la lucha contra la piratería audiovisual*. Recuperado el 13 de octubre de 2025, de <https://www.ambito.com/negocios/alianza-y-mercado-libre-se-unen-avanzar-la-lucha-contra-la-pirateria-audiovisual-n5868961>
68. ECIJA México (2023, 25 de agosto). *Influencers: Mexican consumer protection agency establishes advertising guidelines*. Recuperado el 13 de octubre de 2025, de <https://www.ecija.com/actualidad-insights/influencers-mexican-consumer-protection-agency-establishes-advertising-guidelines/>
69. Delgado Tong, A. (2025, 05 de abril). *El Zein y Samahara Lobatón multados: Indecopi revela lista completa de influencers sancionados por publicidad encubierta*. Infobae <https://www.infobae.com/peru/2025/04/05/el-zein-y-samahara-lobaton-multados-indecopi-revela-lista-de-completa-de-influencers-sancionados-por-publicidad-encubierta/>

70. Prensa Mercosur (2025, 17 de julio). *Pagos digitales e integración regional: ¿Puede Mercado Pago impulsar el comercio intra-Mercosur?* Recuperado el 13 de octubre de 2025, de <https://www.prensamercosur.com.ar/pagos-digitales-e-integracion-regional-puede-mercado-pago-impulsar-el-comercio-intra-mercotur.html>
71. Ceurvels, M. (2025, 23 de marzo). *The Future of Digital 2025: Latin America*. Recuperado el 13 de octubre de 2025, de <https://www.emarketer.com/content/future-of-digital-2025-latin-america>
72. Statista (2024, 31 de enero). *El comercio electrónico sigue creciendo en América Latina* <https://es.statista.com/grafico/22835/boom-del-e-commerce-en-latinoamerica/>
73. Comisión Económica para América Latina y el Caribe (2002, 08 de mayo). *Brecha digital podría ampliarse en América Latina* <https://www.cepal.org/es/comunicados/brecha-digital-podria-ampliarse-america-latina>
74. Ulloa, M. (n.d.). *Avances en la regulación de la inteligencia artificial en América Latina*. Observatorio de Riesgos Catastróficos Globales. Recuperado el 13 de octubre de 2025, de <https://orcg.info/articulos/avances-en-la-regulacin-de-la-inteligencia-artificial-en-amrica-latina>

75. Bijkerk, W. (2021, abril). *Sandboxes regulatorios, hubs de innovación y más innovaciones regulatorias en América Latina y el Caribe: una aproximación*. Banco Interamericano de Desarrollo (BID). Recuperado el 13 de octubre de 2025, de <https://publications.iadb.org/es/sandboxes-regulatorios-hubs-de-innovacion-y-mas-innovaciones-regulatorias-en-america-latina-y-el>
76. Lloreda Camacho & Co (2025, 02 de julio). *Fintech Laws and Regulations: Colombia 2025*. International Comparative Legal Guides (ICLG). Recuperado el 13 de octubre de 2025, de <https://iclg.com/practice-areas/fintech-laws-and-regulations/colombia>
77. Singla, A.; Sukharevsky, A.; Yee, L.; Chui, M. & Hall, B. (2025, 12 de marzo). *El estado de la IA: Cómo se transforman las organizaciones para capturar valor*. McKinsey & Company. Recuperado el 13 de octubre de 2025, de <https://www.mckinsey.com/locations/south-america/latam/hispanoamerica-en-potencia/el-estado-de-la-ia-como-se-renuevan-las-organizaciones-para-capturar-valor/es-CL>
78. Usercentrics (2024, 26 de diciembre). *Diferencias principales entre la Ley de Mercados Digitales (DMA) y la Ley de Servicios Digitales (DSA)*. Recuperado el 13 de octubre de 2025, de <https://usercentrics.com/es/knowledge-hub/diferencias-ley-mercados-digitales-y-ley-servicios-digitales/>

79. Alianza del Pacífico (2021). *Hoja de ruta para el Mercado Digital Regional de la Alianza del Pacífico* <https://alianzapacifico.net/wp-content/uploads/2021/06/HOJA-DE-RUTA-PARA-EL-MERCADO-DIGITAL-REGIONAL-DE-LA-ALIANZA-DEL-PACIFICO.pdf>
80. eLíderesPodcastx25 (2024, 20 de noviembre). Sebastián Bellagamba: *De los primeros días de internet en Argentina al futuro del comercio digital* [Video] YouTube <https://www.youtube.com/watch?v=mfl7nUvDOFY>
81. LACNIC Blog (2017, 12 de septiembre). Sebastián Bellagamba: *“LACNIC sirve como amalgama de los espacios de la región”*. Recuperado el 13 de octubre de 2025, de <https://blog.lacnic.net/sebastian-bellagamba-lacnic-sirve-como-amalgama-de-los-espacios-de-la-region/>
82. eCommerce Institute (2024, 19 de julio). *eLíderes Podcastx25 - Sergio Candelo y el camino del CD a la nube* [Video]. YouTube <https://www.youtube.com/watch?v=3lCVZN2ffNE>
83. Federal Reserve Bank of St. Louis (2024, 19 de septiembre). *Internet users: All income levels for Latin America and Caribbean* <https://fred.stlouisfed.org/series/ITNETUSERP2LCN>

84. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). (1996, 12 de junio). *Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) con su nuevo artículo 5 bis aprobado en 1998*. Naciones Unidas https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_commerce
85. Badillo, M. & Imran, M. (2024, mayo). *Regulatory strategies and priorities of data protection authorities in Latin America: 2024 and beyond*. Future of Privacy Forum https://fpf.org/wp-content/uploads/2024/05/Final_-LatAm-DPA-Report_-2024.pdf
86. Melo, L. (2014, 28 de noviembre). *Maquiagem de preços lidera reclamações na Black Friday*. Exame <https://exame.com/negocios/maquiagem-de-precos-lidera-reclamacoes-na-black-friday/>
87. Vilela, V. (2013, 08 de noviembre). *Black Friday brasileira ganha Código de Ética para proteger consumidor*. E-commerce Brasil <https://www.ecommercebrasil.com.br/noticias/black-friday-brasileira-ganha-codigo-etica-protoger-consumidor>
88. Comisión Europea (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de IA).

Podcast y entrevistas

No te pierdas las entrevistas con algunos de los líderes más influyentes del comercio digital de Iberoamérica: visionarios, pioneros y artistas que comparten sus historias y secretos. Prepárate para disfrutar de conversaciones inspiradoras con quienes están definiendo el futuro digital de nuestra región.



**Eugenio
Sánchez**



**Ludovino
Lopes**



**Alejandro
Prince**



**Jacobo
Cohen Imach**



**Yerka
Yukich**



**Verónica
Pinazo**

Falta link



**Sebastián
Bellagamba**

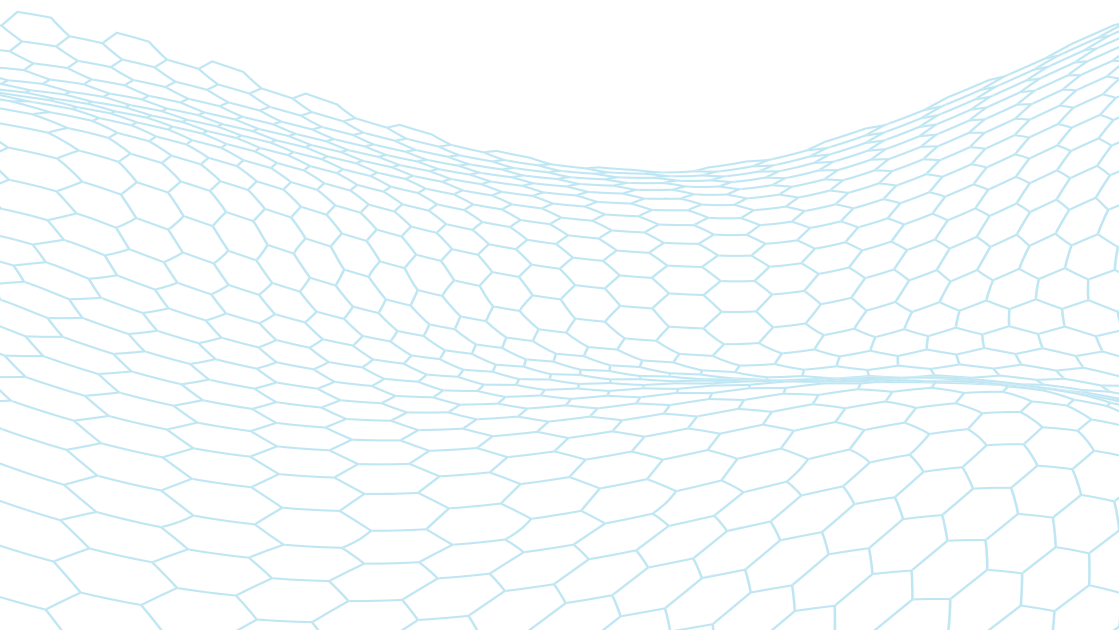


**Enrique
Dans**



**Sergio
Candelo**

GÉNEROS DE UN FUTURO DIGITAL



GÉNESIS

DE UN FUTURO DIGITAL



Sobre las **dimensiones** del libro vivo

En ***Génesis de un Futuro Digital***, los lectores son invitados a una travesía multidimensional donde cada capítulo se convierte en un portal hacia un mundo lleno de conocimiento, historia y visión que podrán explorar por medio de una experiencia única de aprendizaje. A continuación, les presento las distintas dimensiones que conforman este universo:



Dimensión Gráfica



Dimensión textual



Dimensión multimedia



Dimensión aumentada

Dimensión Gráfica



En esta dimensión encontrarán un mapa detallado de las líneas de tiempo que marcan los hitos más significativos en la evolución del comercio electrónico hasta la conformación del ecosistema digital. Esta línea temporal sirve como guía para comprender la gestación y desarrollo del ecosistema digital. Además, se destacan las personalidades, emprendimientos y empresas que han dejado una huella indeleble en este paisaje en constante cambio, como también los recursos gráficos que se utilizan en cada *momentum* para ilustrar y comprender la gestación y desarrollo del ecosistema digital.



Dimensión Textual



Por medio de esta dimensión tienen acceso a una vasta biblioteca de documentos en formato ebook, estudios y análisis estadísticos que han sido la columna vertebral de la investigación detrás de este *libro vivo*. Cada palabra, cada dato, se presenta como un ladrillo en la construcción del conocimiento, proporcionando una base sólida para comprender la trama real del mundo digital.

De la A a la Z ¿Quiénes participan en los **libros vivos**?

A B C D E F G H I J K L M N Ñ O P Q R S T U V X Y Z



Justo
Abón



José
Acosta



Pablo
Altamira



Ricardo
Alonso

De la A a la Z, ¿de qué hablamos en los **libros vivos**?

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

Algoritmos de Recomendación: Sistemas que sugieren productos o contenido basado en el comportamiento del usuario.

Análisis de Sentimientos: Evaluación de opiniones y emociones en textos mediante tecnología.

Análisis Predictivo: Uso de datos y algoritmos para predecir futuros eventos.

Análisis Web: Medición y análisis del tráfico de un sitio web.

Asistentes por Voz: Dispositivos que responden a comandos de voz.

Automatización de Marketing: Uso de software para automatizar procesos de marketing.

Automatización de Procesos Robóticos (RPA): Uso de software para automatizar tareas repetitivas.

Dimensión Multimedia



Esta dimensión es un tesoro de experiencias audiovisuales, con más de 200 entrevistas en video y audio realizadas a visionarios, pioneros, pilotos y artistas del comercio digital en Iberoamérica. Desde testimonios inspiradores hasta análisis profundos, estas entrevistas ofrecen una ventana única a las mentes que han dado forma al panorama digital en la región.

Los déjã vu de las regulaciones
y de los desafíos legales



PLAYLIST DE SPOTIFY



PLAYLIST DE YOUTUBE

Dimensión Aumentada



Esta dimensión utiliza la inteligencia artificial aumentada y la realidad aumentada para llevar la experiencia de lectura a nuevas alturas. A través de Delphy AI, los lectores pueden explorar información adicional, profundizar los conceptos presentados en los capítulos e incluso comparar datos entre diferentes secciones del libro. Esta interacción dinámica entre el contenido y el lector redefine los límites de la exploración y el aprendizaje.

¿Existe otro portal disponible para explorar una nueva dimensión de este contenido? Todavía no lo sabemos, pero lo que sí tenemos muy claro mi equipo y yo es que estamos realizando el primer libro vivo de la historia editorial, un concepto que nos enseña a medida que damos cada paso sobre el mismo y que, estamos seguros, representará una nueva modalidad omnicanal de leer el origen de este ecosistema y poder explorarlo atravesando las barreras del tiempo.

GÉNESIS

DE UN FUTURO DIGITAL



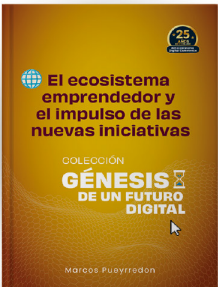
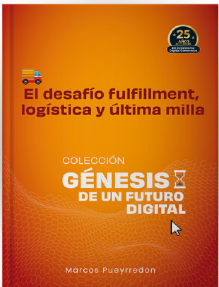
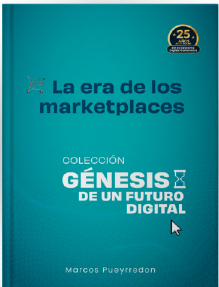
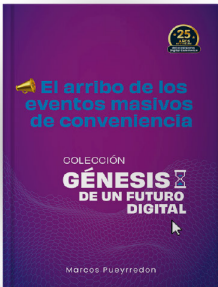
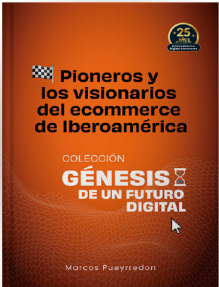
Próximos Momentums

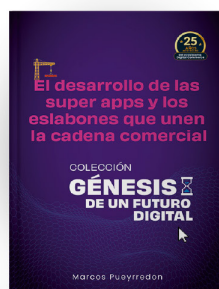
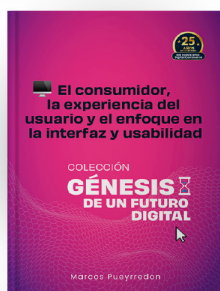
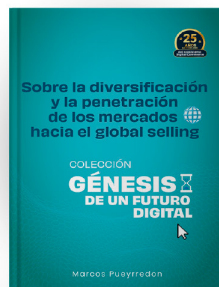
Génesis de un Futuro Digital no es simplemente un libro, es un testamento vivo de los momentos y las participaciones de los pioneros clave que han dado forma al ecosistema digital en Iberoamérica. A través de testimonios vividos en primera persona y una profunda investigación, este proyecto registra los 25 momentums que han marcado la evolución del comercio electrónico desde sus inicios hasta la actualidad.

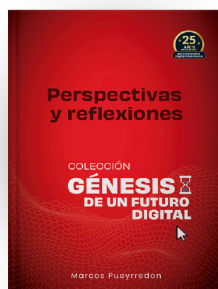
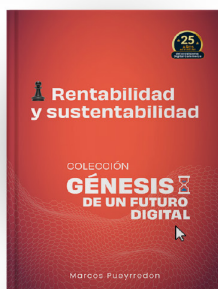
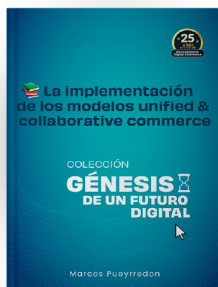
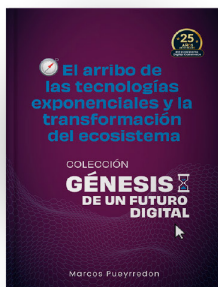
Cada momentum es una invitación para navegar el océano digital en constante cambio y evolución, atravesando las olas y el eTsunami que marcaron un antes y un después para el ecosistema, reconociendo cada uno de los pasos dados por los visionarios y pioneros que dieron forma a la industria del comercio electrónico y descubriendo hasta las últimas innovaciones tecnológicas.

El *libro vivo* es una experiencia única de aprendizaje y descubrimiento que brinda una perspectiva completa del pasado, presente y futuro del ecosistema digital en nuestra región.

Explora los próximos momentums que revelan los secretos, desafíos y triunfos detrás del mundo del Digital Commerce en Iberoamérica:







Interactúa con Delphy AI

Accede a genesisfuturo.digital y explora los libros vivos de esta colección, donde el contenido evoluciona con cada interacción.

Explora:

- ➔ Temáticas profundas relacionadas al digital commerce.
- ➔ Anécdotas y datos únicos que enriquecen tu experiencia.
- ➔ Perfiles de entrevistados y entrevistadas con historias inspiradoras.

Cada pregunta que realices:

- ➔ Expande la capacidad de la tecnología.
- ➔ Contribuye a un ecosistema de conocimiento único.
- ➔ Ayuda a otros usuarios con nueva información en constante evolución.



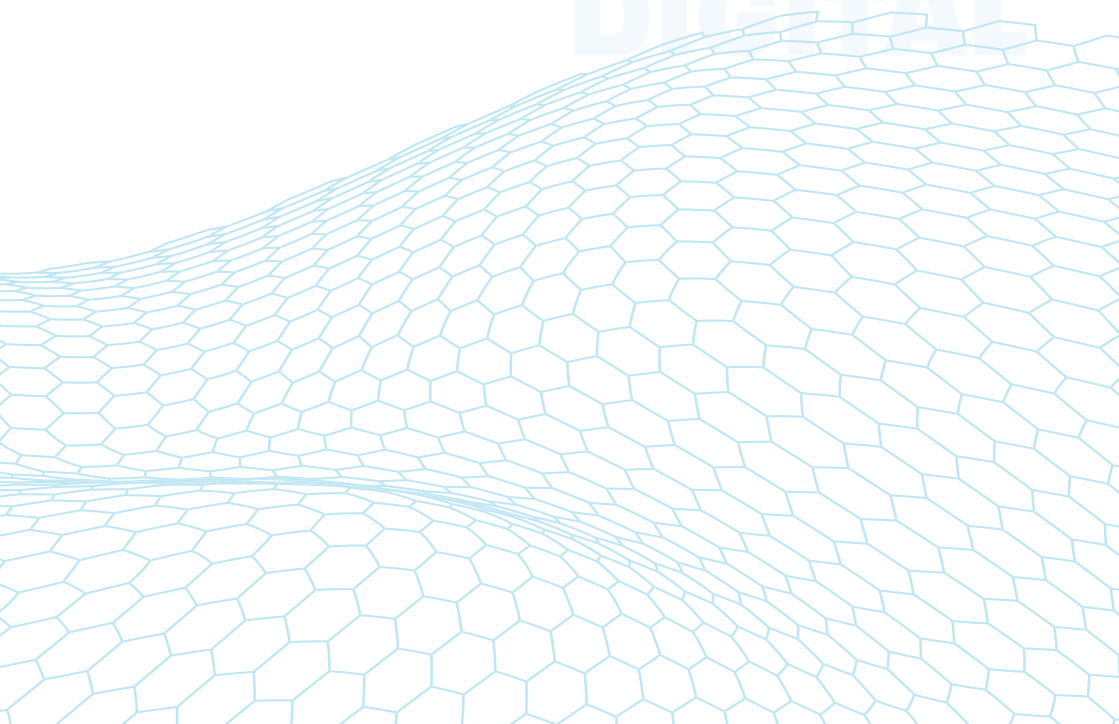
Comienza ahora

Vive el digital commerce
como nunca antes

Este *libro vivo* es parte de la colección Génesis de un futuro digital. Cada *momentum* captura un instante significativo de nuestra evolución.

Gracias por ser parte de este viaje.

¡Nos encontraremos en la próxima edición!





Los déjà vu de las regulaciones y de los desafíos legales

Cada ola de innovación digital trae consigo un déjà vu regulatorio. Las tensiones entre tecnología y ley, entre avance y control, entre lo posible y lo permitido han acompañado al ecosistema digital iberoamericano desde sus inicios.

Los déjà vu de las regulaciones y de los desafíos legales explora ese ciclo histórico que se repite —con nuevos actores y escenarios— cada vez que la transformación tecnológica se adelanta a la capacidad del Estado de regularla.

Este libro, parte de la colección Génesis de un Futuro Digital, analiza cómo los vacíos normativos, la sobreregulación improvisada y la falta de armonización jurídica condicionaron el crecimiento del comercio electrónico, las fintech, los marketplaces y las plataformas digitales en América Latina y el mundo.

Desde los primeros años del ecommerce, cuando la ley apenas reconocía las transacciones electrónicas, hasta los debates contemporáneos sobre inteligencia artificial, soberanía de datos, identidad digital y ética algorítmica, esta obra recorre más de dos décadas de evolución jurídica y tecnológica.

A través de casos emblemáticos se muestra cómo la jurisprudencia y la práctica empresarial fueron moldeando las reglas en ausencia de legislación específica. La narrativa se enriquece con los testimonios de los líderes que vivieron estos procesos desde adentro.

Con un enfoque prospectivo, este libro propone una nueva visión de la regulación: no como límite, sino como palanca de desarrollo y confianza digital. Porque regular el futuro no es detenerlo sino diseñarlo con propósito, equidad y visión compartida.

