

Pauta 119

Innovación para todos

Pauta 119: Innovación para todos

Boletín Informativo del Capítulo Mexicano
de la Cámara Internacional de Comercio, A.C.

Septiembre 2026

Consejo Editorial

Presidente
Alberto Espinosa Desigaud

Vicepresidentes
Federico Bernaldo de Quirós
Marlene Garayzar

Directora General
Yesica González Pérez

Directora de Comisiones y Grupos de Trabajo
Responsable de Pauta: Laura Altamirano López

Gerentes de Comisiones y Grupos de Trabajo
Bianca Palazuelos Bard
Luz María Morales Uribe

Gerente de Eventos
Abigail Blanco Rojano

Coordinador de Comunicación
Creador de Formato Electrónico: Miguel Iván Jorge Sánchez

ICC México Pauta Boletín Informativo del Capítulo Mexicano de la Cámara Internacional de Comercio, A.C: Es una publicación de análisis educativo, social, comercial, financiero, económico e internacional, del Capítulo Mexicano de la Cámara Internacional de Comercio (ICC México). Las ideas expuestas por nuestros colaboradores no corresponden necesariamente al pensamiento de ICC México. Copyright 2001 Capítulo Mexicano de la Cámara Internacional de Comercio. Reservados todos los derechos. Ninguna parte de este documento puede ser reproducida o traducida en ninguna forma o por cualquier medio - gráfico, electrónico o mecánico, incluidas las fotocopias, grabaciones en disco o cinta, u otro sistema de reproducción sin el permiso escrito de ICC México.

Título de la publicación: «**ICC México PAUTA Boletín Informativo del Capítulo Mexicano de la Cámara Internacional de Comercio A.C.**» Editor Responsable: Lic. Rosa Laura Altamirano López Número de certificado de reserva otorgado por el Instituto Nacional del Derecho de Autor: **04 - 2025 -0220 14595200 -203**. Especie: Difusión: **Vía Red de Cómputo**. Género: **Difusiones periódicas**. Domicilio de la publicación y del distribuidor: Prado Sur 274 001 Lomas de Chapultepec, Miguel Hidalgo CP: 11000 Ciudad de México, México Teléfonos: (52) 5687 2203, 5687 2207, 5687 2321 5687 2507,5687 2601.

Disclaimer: Las opiniones, contenido, creencias y puntos de vista expresados por los diversos autores de PAUTA, no reflejan necesariamente las opiniones, creencias y puntos de vista de ICC México o su equipo. Los autores son responsables del contenido, gramática y ortografía de cada uno de sus artículos.



Índice

Carta del Presidente **04**

Conoce a nuestros autores **07**

¿Por qué el nuevo espectro para la industria mexicana necesita otro diseño? **10**

De la Revolución Universal al Imperio de Nicho: El Destino del Blockchain **17**

Propiedad Intelectual en México: ¿Qué ley procesal aplicar? **20**

La Era del Comercio Agéntico (A2B/A2A): Desafíos Jurídicos, Operativos y Regulatorios en la Redefinición del E-Commerce Transfronterizo **25**

Economía Digital respecto de “Ciberseguridad & Protección de Datos Personales en Operaciones Transfronterizas” **34**

Citius, altius, fortius. Lo que la IA me dejó del Mundial de Fútbol 2026 **42**

Carta del Presidente



Alberto Espinosa Desigaud
Presidente
International Chamber of Commerce México

Estimados socios:

En una etapa en la que los organismos multilaterales prevén que el crecimiento de la economía global será impulsada por la creciente demanda en el ciclo tecnológico global gracias a los avances en inteligencia artificial y su adopción, en esta edición de Pauta se abordan temas de gran interés como los nuevos modelos de comercio electrónico basados en inteligencia artificial, ciberseguridad en transacciones transfronterizas, mercados de predicción basados en blockchain, el nuevo diseño del espectro para la industria mexicana y el marco regulatorio en materia de propiedad industrial.

En el análisis “La era del comercio agéntico (A2B/A2A): Desafíos jurídicos, operativos y regulatorios en la redefinición del e-commerce transfronterizo”, se describe la acelerada transformación en el comercio electrónico por la irrupción de la Inteligencia Artificial Agéntica, la cual rompe de raíz con el paradigma clásico de comercio electrónico estructurado bajo la premisa fundamental de que un consumidor humano navega a través de una interfaz gráfica de usuario y manifiesta su voluntad de compra mediante un clic en el botón de “comprar” o “pagar”. Ahora se ha dado paso a un sistema informático autónomo dotado de capacidad para razonar en múltiples pasos, planificar estrategias, utilizar herramientas externas, como bases de datos, calculadoras y opciones de pago, y ejecutar acciones complejas en el mundo digital sin necesidad de supervisión humana constante. Ello podría modificar el modelo tradicional de protección de datos, dado que los agentes de IA tienen acceso a información sensible de las personas, como tarjetas de crédito y claves de acceso, historial de salud y ubicación geográfica en tiempo real. La pregunta es ¿Qué sucede cuando la transacción sale mal debido a un fallo propio de la inteligencia artificial? En el artículo se analizan los desafíos jurídicos emergentes, como validez contractual, representación, responsabilidad civil, privacidad y competencia desleal y se sugiere la urgente adaptación de los marcos normativos e infraestructuras legales en el comercio digital, nacional o transfronterizo, proceso en el que la ICC, en estrecha colaboración con organismos como la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional puede liderar la actualización de los instrumentos del derecho mercantil global mediante redacción de cláusulas modelo para el comercio agéntico, protocolos de identificación, transparencia algorítmica y armonización regulatoria transfronteriza.

El artículo “Ciberseguridad y protección de datos personales en operaciones transfronterizas” explica que las empresas extranjeras con presencia en México enfrentan una doble presión: Un marco normativo interno en plena transición institucional, con la nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que entró en vigor el 21 de marzo de 2025, bajo la cual fue sustituida la autoridad supervisora, y exigencias externas europeas y norteamericanas, cuyo incumplimiento tiene costos contractuales y reputacionales tangibles.

Las empresas que realicen operaciones de comercio internacional deben verificar no sólo el cumplimiento de leyes locales sino también el cumplimiento de tratados internacionales y leyes aplicables en el país destino. México sigue siendo uno de los pocos países miembros de la Organización para la Cooperación y el Desarrollo Económicos que no cuenta con legislación específica en materia de ciberseguridad, una situación que la Ley Federal de Telecomunicaciones y Radiodifusión, que cubre a los concesionarios del sector, no a la generalidad de la economía digital, solo remedia de manera parcial y sectorial. El Tratado México- Estados Unidos-Canadá, en su Capítulo 19 sobre comercio digital, establece compromisos de no localización forzada de datos y libre flujo transfronterizo como condiciones de acceso al mercado en América del Norte. La manera de brindar seguridad jurídica en México requiere la elaboración de normatividad que obligue internamente a las empresas a llevar a cabo procesos de análisis y comprensión adecuada del manejo de la información de terceros y la manera en que deberán cubrirse eventuales riesgos, actuales o que pudieran existir a futuro.

En el ensayo “Citius, altius, fortius. Lo que la IA me dejó del Mundial de Futbol 2026” se narra la realización de un modelo de inteligencia artificial en la copa mundial de fútbol de 2026, bajo el modelo de competencias AI Fluency Framework, que consiste en tomar responsabilidad por lo que se hace con la inteligencia artificial, transparentando cuándo se utiliza. Así, se construyó el modelo "GenAI-Me", con el objetivo definido de alcanzar un lugar en las 10 primeras posiciones de una quiniela. El modelo no buscaba predecir el marcador correcto sino el que, en promedio, obtuviera más puntos según las reglas de la quiniela. Se implementó un mecanismo de automatización mediante el cual el modelo ingresaría por sí mismo al sitio web y pondría las predicciones al menos con una semana de anticipación. El modelo cerró la participación en el puesto 2 de 100, por lo que se cumplió el objetivo de quedar entre los 10 primeros sitios. Entre las lecciones aprendidas de este modelo destaca la importancia del "humano en el medio" y claridad en los roles. Una IA debe tener escritas esas reglas y deben existir mecanismos para verificar que se cumplan. No se trata, pues, de humanos contra máquinas, ni de ignorar un fenómeno que no tiene vuelta atrás pues la IA será más preponderante día con día. Se trata de entender que está en nuestras manos decidir qué hacer con ella.

“De la revolución universal al imperio de nicho: El destino del blockchain”
Es un ensayo que relata la historia de cómo nunca se concretó la revolución que muchos esperaban en torno al blockchain como la tecnología todo poderosa que resolvería los problemas de confianza, intermediación y costos de transacción en casi cualquier industria imaginable. El blockchain es la base sobre la cual se construyeron las cripto monedas, pero en realidad hoy es la plataforma sobre la que empieza a construirse el nicho de los mercados de predicción, que usan contratos inteligentes en blockchain basados en un modelo de negocio muy simple: plataformas como Polymarket y Kalshi –los líderes en esa industria– permiten a cualquier persona comprar y vender "acciones" sobre el resultado de un evento futuro –una elección, un partido de futbol, el lanzamiento de un nuevo producto– y ganar dinero si acertaron. En 2025, el volumen total operado en esta industria alcanzó los 63,500 millones de dólares, casi cuatro veces más que los 15,800 millones registrados apenas un año antes. La escalada no se ha detenido: en julio de 2026 —impulsado en buena medida por el mundial de futbol— el volumen combinado de Kalshi y Polymarket llegó a un récord histórico de 50,600 millones de dólares en un solo mes. Esto es más de tres veces todo lo que la industria completa había movido en el año 2024.

Si bien Polymarket utiliza un modelo descentralizado gracias a blockchain y Kalshi usa un modelo centralizado, lo cierto es que el sistema blockhain encontró el problema exacto para el que su arquitectura resultó ser la solución perfecta y permitió poner los cimientos para construir un negocio de escala verdaderamente global. En el ensayo “Por qué el nuevo espectro para la industria mexicana necesita otro diseño” se explica que México está a punto de tomar una decisión de espectro radioeléctrico que definirá, durante los próximos diez años, cómo se conecta buena parte de su industria manufacturera, logística y de servicios. La Comisión Reguladora de Telecomunicaciones sometió a consulta pública las bases con las que planea concesionar hasta 100 MHz de la Banda 2.3 GHz para lo que llama el Servicio de Provisión de Capacidad para Redes de Radiocomunicaciones Inteligentes; en términos sencillos, se trata de redes privadas de uso exclusivo para plantas industriales, corredores logísticos, polos mineros o clústeres agroindustriales, separadas de las redes públicas de telefonía e internet que usamos todos los días. Al revisar evidencia de más de una decena de países que ya probaron esquemas similares, se observa que el diseño actual repite errores ya documentados en otras jurisdicciones, excluye de facto a los dos operadores móviles más grandes del país, se aparta de un principio legal que la propia reforma de telecomunicaciones de 2025 mantiene vigente, no resuelve cómo se calculará el costo del espectro para el usuario final, y deja sin desarrollar la coordinación técnica entre los tres regímenes de uso que compartirán la misma banda. México tiene la oportunidad de diseñar un esquema de espectro industrial que aprenda de lo que ya funcionó, y de lo que ya falló. Ignorar esa evidencia en un mercado como el mexicano, donde el espectro ya es un recurso escaso y donde dos operadores móviles ya lo han devuelto por falta de rentabilidad, no sería solo un error de diseño regulatorio; nos llevaría a desperdiciar una banda completa de 100 MHz en un esquema con alta probabilidad de baja participación, mientras la industria mexicana sigue esperando la conectividad que necesita para dar el siguiente paso en su transformación digital.

En el artículo “Propiedad Intelectual en México ¿Qué ley procesal aplicar?” se analiza cómo la transición hacia el Código Nacional de Procedimientos Civiles y Familiares ha generado un escenario complejo de interpretación normativa en el sistema jurídico mexicano. En ese contexto, un análisis detallado de la Ley Federal de Protección a la Propiedad Industrial y los recientes criterios emitidos por Poder Judicial de la Federación en materia de Amparo, permiten apreciar la disyuntiva entre una aplicación inmediata o gradual, dependiendo de la materia y del articulado del cuerpo normativo que la regule. El autor advierte que cuando la supletoriedad del Código de Procedimientos Civiles y Familiares finalmente entre en vigor, el litigio estratégico en propiedad industrial experimentará un giro radical en algunos puntos fundamentales: Prueba confesional contra declaración de parte; disminución de plazos para aportar pruebas que provengan fuera del lugar del juicio; reducción de término para ofrecimiento de pruebas; valoración probatoria; notificaciones mediante edictos; ampliación del catálogo de pruebas supervinientes; equivalencia digital y funcional; depuración procesal de objeciones, y adopción de tecnologías disruptivas, como el blockchain. El reto para los abogados especializados en materia de propiedad intelectual será procurar y asegurar que los juzgadores entiendan que la literalidad del segundo Transitorio de la Ley Federal de Protección a la Propiedad Intelectual supera cualquier interpretación que atente contra la gradualidad de la entrada en vigor del nuevo Código de Procedimientos Civiles y Familiares, para así garantizar la certeza jurídica y el respeto al debido proceso en materia de propiedad industrial. Confiamos en que los ensayos y artículos de esta edición de Pauta sean de interés para todos los socios y que los diversos enfoques abordados contribuyan a enriquecer el debate sobre la modernización de la regulación para mejorar el entorno para la economía digital y la innovación, impulsar el comercio, fomentar la inversión y promover las mejores prácticas internacionales que propicien un mayor crecimiento y un futuro más próspero para México.

Conoce a nuestros autores



Miguel Calderón Lelo de Larrea
Presidente de la Comisión de Economía Digital
ICC México



Erick Clavel
Vicepresidente de la Comisión de Arbitraje & ADR, ICC México
Socio de Clavel Abogados y Director de lawkit.mx



Jaime Rodríguez
Vicepresidente de la Comisión de Propiedad Intelectual
ICC México
Socio de Olivares



Diego Ballesteros
Asociado de Olivares



Sofía Riquelme
Asociada de Olivares



Xavier Careaga
Consejero de la práctica de Tecnología, Medios y Entretenimiento e IA (TMT & IA) en Galicia



Ricardo Garcia
Socio de las prácticas de M&A y Tecnología, Medios y Entretenimiento & IA Galicia



Ana Paula Boy
Asociada del área TMT & IA
Galicia



Grecia Macías
Asociada del área TMT & IA
Galicia



Mauricio Fernández
Asociado del área TMT & IA
Galicia



Luis G. Ramirez Villela
Socio
Müggenburg, Gorches y Peñalosa, S.C. (MGPS), Mexico



Georgina Herrera Guerrero
Asociada
Müggenburg, Gorches y Peñalosa, S.C



Jefferson Gutierrez
Associate Managing Director del área de
Investigaciones, Diligencia y Cumplimiento
Kroll

¿Por qué el nuevo espectro para la industria mexicana necesita otro diseño?

Miguel Calderón Lelo de Larrea
Presidente de la Comisión de Economía Digital
ICC México

México está a punto de tomar una decisión de espectro radioeléctrico que definirá, durante los próximos diez años, cómo se conecta buena parte de su industria manufacturera, logística y de servicios. La Comisión Reguladora de Telecomunicaciones sometió a consulta pública, mediante el Acuerdo P/CRT/EXT/16062026/074 del 16 de junio de 2026, las Bases de la Licitación CRT RRI 01, con las que planea concesionar hasta 100 MHz de la Banda 2.3 GHz para lo que llama el Servicio de Provisión de Capacidad para Redes de Radiocomunicaciones Inteligentes. En términos sencillos, redes privadas de uso exclusivo para plantas industriales, corredores logísticos, polos mineros o clústeres agroindustriales, separadas de las redes públicas de telefonía e internet que usamos todos los días.

La intención de política pública es defendible y hasta deseable. La industria mexicana necesita conectividad confiable, de baja latencia y con control sobre su propia red para procesos como automatización de planta, robótica coordinada o monitoreo remoto de activos críticos. El problema no es el objetivo, sino el diseño concreto que la CRT eligió para alcanzarlo. Un análisis de las Bases, apoyado en evidencia de más de una decena de países que ya probaron esquemas similares, muestra que el diseño actual repite errores ya documentados en otras jurisdicciones, excluye de facto a los dos operadores móviles más grandes del país, se aparta de un principio legal que la propia reforma de telecomunicaciones de 2025 mantiene vigente, no resuelve cómo se calculará el costo del espectro para el usuario final, y deja sin desarrollar la coordinación técnica entre los tres regímenes de uso que compartirán la misma banda.

Vale la pena desmenuzar cada uno de estos cinco puntos, porque juntos explican por qué esta Licitación, tal como está planteada hoy, corre el riesgo de convertirse en un ejercicio costoso con baja participación, en lugar del catalizador de digitalización industrial que México necesita.

¿Cómo está diseñada la Licitación?

El espectro se divide en Bloques de 10 MHz que se asignan en dos fases. En la primera, por Región Industrial, un concepto nuevo que agrupa municipios del país en 60 zonas según su patrón de desarrollo industrial, sin relación con la división administrativa tradicional ni con la densidad poblacional. En la segunda fase, condicionada a que quede espectro remanente, por Polígono, un área que cada interesado puede definir libremente hasta un máximo de 200 kilómetros cuadrados.

Los títulos tendrán una vigencia de 10 años. Y aquí aparece el primer punto de fricción, cualquier interesado que concentre actualmente más del 20 por ciento de la tenencia espectral nacional ponderada en bandas comparables queda impedido de acumular más espectro en esta Licitación. Dicho de otro modo, un límite de acumulación que, en la práctica, excluye a los dos operadores móviles de mayor escala del país.





Primer problema: reservar espectro para uso exclusivo no ha funcionado bien en otros países

Las Bases optan por lo que la literatura especializada llama un esquema de reserva dedicada o set aside, mediante el cual un bloque de espectro se aparta por completo del uso de redes públicas y se destina en exclusiva a un caso de uso específico. Existen al menos otras dos rutas para atender la misma demanda, las bandas de acceso compartido, donde múltiples usuarios coexisten bajo reglas de coordinación, y las condiciones de licencia que obligan a los operadores móviles establecidos a arrendar o sublicenciar espectro a usuarios locales que lo soliciten.

La evidencia sobre cómo ha funcionado el camino que eligió México es más bien desalentadora. Alemania reservó 100 MHz en la banda de 3.7 a 3.8 GHz para redes privadas desde 2019. Tres años después, se habían emitido menos de 300 licencias, y la GSMA, la asociación que agrupa a los operadores móviles a nivel mundial, estima que esa reserva generó un sobrecosto cercano a 3 mil millones de euros para el mercado móvil alemán, simplemente por restar ese espectro de la disponibilidad para redes públicas sin que la demanda industrial lo aprovechara a la escala esperada. El Reino Unido habilitó licencias locales de acceso compartido en la banda de 3.8 a 4.2 GHz y apenas alrededor de 100 usuarios las solicitaron, cubriendo solo hasta la mitad del espectro disponible. Finlandia, un caso especialmente relevante porque se trata exactamente de la misma banda que ahora subasta México, destinó 20 MHz de la Banda 2.3 GHz a licencias locales para redes privadas, con interés limitado y con restricciones documentadas de interferencia con otros servicios que ya operaban en esa banda, un antecedente que México haría bien en tomar en cuenta antes de replicar el mismo esquema en la misma frecuencia.

Más allá de estos casos puntuales, existe evidencia econométrica de mayor escala que respalda la misma conclusión. La GSMA publicó en 2024 un análisis de 51 países entre 2018 y 2022 que examina si la cantidad de espectro reservado para redes privadas se asocia con mayor adopción de esas redes. El resultado es contundente, una correlación simple inicial, de 5 por ciento más lanzamientos de redes privadas por cada 100 MHz reservados, desaparece por completo al controlar por tendencias generales del mercado y otros factores de confusión. No hay evidencia causal robusta de que reservar espectro incremente la adopción de redes privadas. El mismo estudio cuantifica el costo de oportunidad de esta decisión, cien megahertz adicionales disponibles para redes públicas se asocian con velocidades de descarga 24 por ciento más altas, equivalentes a 4.5 megabits por segundo sobre el promedio global del periodo analizado. Esa es la conectividad que un país deja sobre la mesa cada vez que aparta espectro core para un uso exclusivo con baja adopción esperada.

El dato más revelador viene del lado de la demanda. Una encuesta de Omdia a 507 empresas en distintas fases de adopción de redes privadas LTE o 5G encontró que 62 por ciento de ellas prefiere desplegar su red privada usando espectro no licenciado o arrendado de un operador móvil, y solo 30 por ciento preferiría obtener espectro propio mediante una concesión directa. La lectura es sencilla, la gestión de una red de radiocomunicaciones no es el negocio principal de una empresa industrial, y la mayoría prefiere que alguien más se encargue de operarla. La GSMA añade un matiz importante, ofrecer ese espectro reservado a costo reducido o nulo tampoco resuelve el problema, porque termina subsidiando a las redes privadas frente a las redes públicas, que en muchos casos serían la opción más eficiente. El diseño más equilibrado no consiste en bajar el precio del espectro reservado, sino en sustituir la lógica de reserva exclusiva por mecanismos que preserven el incentivo de inversión eficiente.

Segundo problema: la Licitación excluye de facto a Telcel y a AT&T

Según la propia Tabla 4 del documento de la Licitación, Telcel concentra 33.51 por ciento y el Grupo AT&T 26.21 por ciento de la tenencia espectral ponderada por población en las bandas comparables. El límite de acumulación de 20 por ciento previsto en el numeral 5.2 de las Bases implica que ambos operadores quedan excluidos en la práctica de participar, y esto ocurre en un país que, de acuerdo con benchmarks internacionales, ya enfrenta un déficit relativo de espectro asignado frente a otras economías comparables.

La pregunta es si excluir a los operadores establecidos era la única forma de proteger el objetivo de atender la demanda industrial, o si existían alternativas de diseño. La evidencia internacional sugiere que sí existían, y que varios países ya las probaron con resultados razonables. La Organización para la Cooperación y el Desarrollo Económicos (OCDE) documenta un enfoque alternativo, empleado en varios países, que consiste en subastar el espectro directamente a los operadores móviles, pero con la obligación de arrendarlo localmente a los usuarios industriales que lo soliciten. La República Checa lo aplicó en la banda de 3.4 a 3.6 GHz, Dinamarca en la banda de 3740 a 3800 MHz, y Noruega en la banda de 3.4 a 3.8 GHz. Este enfoque mantiene el incentivo de despliegue eficiente del operador, que ya cuenta con la infraestructura y la experiencia de gestión de interferencias necesarias, sin excluirlo de la banda, y al mismo tiempo habilita el acceso de la demanda industrial.

Finlandia, nuevamente un caso de referencia obligado por tratarse de la misma banda, ofrece un modelo híbrido interesante. Su regulador, Traficom, estableció en la subasta de la banda de 3.5 GHz que los operadores móviles deben desplegar la red privada que solicite un cliente local, o bien sublicenciar el espectro cuando el despliegue propio resulte oneroso. Este modelo combina la capacidad de ejecución de los operadores establecidos con la flexibilidad de atender necesidades industriales específicas, sin obligar al usuario industrial a convertirse en concesionario directo de espectro, algo que la mayoría de las empresas prefiere evitar según la propia encuesta de Omdia. Existe además un caso que cuestiona directamente la premisa de que sea necesario excluir a los operadores establecidos para que la demanda industrial tenga oportunidad real de acceder al espectro, en India un actor industrial participó en una subasta de espectro de onda milimétrica en igualdad de condiciones con los operadores móviles establecidos, sin ningún tipo de reserva ni trato preferencial, y obtuvo espectro de todas formas.

Puesto en conjunto, este bloque de evidencia apunta a una conclusión razonable, una alternativa más proporcional habría sido permitir la participación de los operadores establecidos, eventualmente sujeta a obligaciones de arrendamiento hacia usuarios industriales dentro de la Región Industrial o el Polígono correspondiente, en lugar de un límite de acumulación que los excluye de facto en prácticamente la totalidad del territorio nacional.

Tercer problema: la Licitación ata la banda a un único servicio, en contra de un principio que la propia ley mexicana mantiene vigente

Este es quizás el argumento más técnico de los cinco, pero también el que tiene mayor sustento jurídico directo. El principio de neutralidad tecnológica establece que el título habilitante de una banda de espectro no debe imponer una tecnología o un servicio específico, permitiendo que el concesionario despliegue cualquier tecnología estandarizada conforme evoluciona el mercado. De acuerdo con la GSMA, este principio ya ha sido adoptado por la mayoría de los reguladores relevantes a nivel global, incluyendo la Unión Europea, América del Norte, Singapur, Hong Kong y Australia.





El principio tampoco es ajeno al marco jurídico mexicano. La Ley Federal de Telecomunicaciones y Radiodifusión de 2014, ya abrogada, incorporaba la neutralidad tecnológica entre sus definiciones legales. La nueva Ley en Materia de Telecomunicaciones y Radiodifusión, publicada en el Diario Oficial de la Federación el 16 de julio de 2025, confirma la continuidad del principio, aunque con un cambio relevante en su anclaje jurídico. El Artículo 3 de la nueva Ley, que contiene el catálogo de definiciones legales, ya no incluye a la neutralidad tecnológica entre ellas. El término que sí permanece en ese catálogo es Neutralidad a la competencia, en la fracción XLV, definido como la obligación del Estado de no generar distorsiones al mercado como consecuencia de la propiedad pública, un concepto distinto que no debe confundirse con la neutralidad tecnológica.

Pero eso no significa que la neutralidad tecnológica haya desaparecido del marco legal. Subsiste como objetivo de política expresamente exigible a la Comisión en dos disposiciones sustantivas, el Artículo 32, fracción VII, la incluye entre los objetivos generales que la Comisión debe perseguir al administrar el espectro radioeléctrico, y el Artículo 109, fracción VIII, la incluye entre los objetivos de los planes técnicos fundamentales que rigen la interconexión de redes públicas. La neutralidad tecnológica dejó de ser una definición legal autónoma y pasó a ser un objetivo de política inserto en dos artículos específicos. Ese cambio no debilita la obligación de la Comisión de observarla, al contrario, ofrece un fundamento normativo concreto y vigente para cuestionar el diseño de esta Licitación, que ata la Banda 2.3 GHz a un único servicio determinado desde el origen de la concesión.

Para entender por qué esto importa en la práctica, ayuda conocer el mecanismo que la neutralidad tecnológica habilita, conocido como refarming. En la Unión Europea, las bandas de 900, 1800 y 2100 MHz, originalmente asociadas a tecnologías de segunda y tercera generación, se reconvirtieron hacia cuarta y quinta generación gracias a decisiones de neutralidad tecnológica, y las asignaciones posteriores ya se otorgaron como neutrales desde el origen de la licencia, sin necesidad de una nueva subasta cada vez que surge una nueva generación tecnológica. La Unión Internacional de Telecomunicaciones respalda esta misma lógica desde otro ángulo, su mandato establece que los adelantos técnicos disponibles se apliquen con la mayor brevedad posible, dado que cada nueva generación tecnológica suele mejorar la eficiencia del uso del espectro respecto de la anterior.

Los casos concretos ilustran tanto el beneficio de aplicar el principio como el costo de no hacerlo. Finlandia fue el primer país europeo en permitir neutralidad tecnológica en la banda de 900 MHz, lo que le permitió alcanzar mayor cobertura geográfica de tercera generación que otros países europeos. Singapur asocia parte de sus resultados de alta velocidad, baja latencia y bajo costo al consumidor con la aplicación consistente de este principio. Bangladés, en sentido contrario, no permitió reorganizar su espectro hacia cuarta generación durante varios años, lo que se tradujo en un rezago documentado en la adopción de esa tecnología. Estos ejemplos ilustran el mismo riesgo que se advierte para la Banda 2.3 GHz, si la demanda de mercado evoluciona hacia un uso distinto al previsto originalmente, atar el espectro a un servicio fijo puede generar un rezago similar al de Bangladés, en lugar de la flexibilidad que capitalizaron Finlandia y Singapur. En Colombia, la Agencia Nacional del Espectro incluye la neutralidad tecnológica entre los temas de su agenda de planificación, lo que confirma la relevancia del principio en la región.

Cuarto problema: el espectro ya es caro en México, y las Bases no dicen cómo se calculará el costo para este esquema

México ya tiene dos antecedentes de operadores móviles que devolvieron espectro por falta de rentabilidad, y el más significativo de los dos ni siquiera aparece mencionado en las Bases de la Licitación. Telefónica Movistar instrumentó, a partir de finales de 2019, una devolución escalonada de la totalidad de su espectro, vinculada a un convenio de acceso inalámbrico de última milla con AT&T que le permitió seguir prestando servicios móviles sin ser ya titular directo de las frecuencias.

El extinto Instituto Federal de Telecomunicaciones documentó el proceso en etapas sucesivas, una primera entrega de PCS y de la banda de 2.5 GHz a finales de 2019, devoluciones en 850 MHz y 1900 MHz hacia fines de 2020, la entrega de las frecuencias restantes en 1900 MHz durante 2021, y un último paquete en 850 MHz, PCS y 2.5 GHz hacia junio de 2022. El propio regulador estimó que esta renuncia representaría una menor recaudación anual cercana a 4500 millones de pesos por derechos de espectro que el Estado dejaría de percibir, y la señaló explícitamente como evidencia de cómo el costo del espectro influye en las decisiones de los operadores.

Las propias Bases de la Licitación reconocen, en la nota de su Tabla 4, un segundo caso, a finales de 2022 el Grupo AT&T renunció a 3 MHz en la Zona Metropolitana del Valle de México y en la Zona Metropolitana de Guadalajara en la banda 850 MHz, y a 10 MHz en las regiones 1 y 2 de la banda AWS. Que sean dos operadores distintos, y no uno solo, los que hayan devuelto espectro por razones de rentabilidad, refuerza la conclusión, mantener espectro asignado en México no siempre resulta rentable incluso para operadores de escala nacional con bases de ingresos diversificadas.

Ese antecedente hace contraintuitivo diseñar un esquema en el que el sujeto obligado a costear ese mismo insumo regulatorio sea un usuario industrial con alcance geográfico limitado a una sola Región Industrial o a un Polígono específico. La GSMA, con base en un estudio de 229 operadores en 64 países, documenta que derechos anuales elevados por el uso del espectro se asocian con peor cobertura, peor calidad de servicio y mayores precios al usuario final, un mecanismo económico generalizable a un usuario industrial pequeño, que carece de la base de ingresos diversificada de un operador nacional para absorber ese costo fijo.

El esquema de Bloques de 10 MHz por Región Industrial o por Polígono equivale, en términos económicos, a fragmentar el espectro para hacerlo aparentemente más accesible. Pero la GSMA advierte que subdividir espectro caro no reduce su precio, y que esta práctica añade riesgos de infrautilización y de interferencia, además de que los usuarios resultantes pueden no obtener bloques contiguos suficientes para un despliegue eficiente. A esto se suma un vacío sobre cómo se calcularán los derechos aplicables, las 60 Regiones Industriales agrupan municipios por patrones de desarrollo industrial, no por densidad poblacional, y el esquema de Polígonos fija el Valor Mínimo de Referencia por MHz por kilómetro cuadrado, sin relación con ninguna regionalización preexistente. Ninguna de las dos lógicas coincide con el esquema vigente de 9 regiones del artículo 173 de la Ley Federal de Derechos, calibrado originalmente con un criterio poblacional, y el numeral 11.2 de las Bases solo señala que los derechos se establecerán en esa Ley, sin precisar la fracción aplicable ni la tarifa correspondiente a esta nueva geografía.





Quinto problema: nadie sabe todavía cómo se van a coordinar las interferencias entre los tres usos que compartirán la misma banda

Las Bases reconocen, en sus Considerandos, que la Banda 2.3 GHz fue incorporada en el Programa Anual de Uso y Aprovechamiento de Bandas de Frecuencias 2026 simultáneamente para tres regímenes distintos, uso comercial mediante esta Licitación, uso privado para Radiocomunicaciones Inteligentes, y uso para acceso inalámbrico de carácter público y social. El numeral 4.14 se limita a señalar que, si se otorgan otras concesiones en la misma banda, el espectro de esta Licitación contará con protección contra interferencias perjudiciales, sin desarrollar el mecanismo técnico que hará posible esa protección.

Para entender qué falta, ayuda una distinción que usa la Unión Internacional de Telecomunicaciones entre atribución, que define qué servicios tienen acceso a una banda, y autorización, que define cómo se asignan las frecuencias a usuarios concretos y bajo qué reglas de convivencia. Las Bases resuelven la atribución, pero no desarrollan la autorización. El Manual de Regulación Digital de la UIT distingue, además, entre acceso compartido con licencia, que limita el número de usuarios y protege a los preexistentes, y acceso exento de licencia, que no limita usuarios pero impone restricciones técnicas de potencia. Las Bases no precisan bajo cuál de estos modelos operará cada uno de los tres regímenes.

Existe un modelo técnico de referencia que podría servir de guía. El esquema Citizens Broadband Radio Service de Estados Unidos, en la banda de 3.5 GHz, gestiona de forma dinámica tres niveles de usuarios con distinto grado de protección, incumbentes, licenciatarios con acceso prioritario, y usuarios de acceso general sin protección frente a los niveles superiores, mediante un Spectrum Access System y sensores que detectan la actividad de los incumbentes. Es el tipo de solución técnica concreta que la CRT podría desarrollar, en sustitución de la frase genérica de protección contra interferencias que hoy contienen las Bases. Conviene ser realista sobre las limitaciones de ese modelo, la propia autoridad de Estados Unidos responsable de espectro federal ha documentado fricciones reales, complejidad operativa y problemas de coexistencia entre usuarios del mismo nivel por ausencia de protocolos claros. Esto ilustra que no basta con adoptar el modelo de coordinación dinámica, sino que es necesario anticipar también las reglas de coexistencia entre usuarios del mismo régimen, como ocurriría entre Polígonos colindantes o superpuestos.

Hay además un vacío procedimental que las Bases no atienden en absoluto, qué pasa cuando la interferencia ya ocurrió. El extinto Instituto Federal de Telecomunicaciones, cuyas funciones en esta materia heredó la CRT, contaba con un procedimiento equivalente para el ámbito satelital, que exigía, ante una denuncia, un expediente técnico mínimo con horarios de afectación, naturaleza del servicio afectado y representaciones espectrales, con el cual la autoridad verificaba la denuncia y determinaba medidas de mitigación. Sería razonable que la CRT adoptara un procedimiento equivalente para la Banda 2.3 GHz, dado que hoy no existe ningún mecanismo de denuncia, verificación o mitigación previsto en las Bases. El caso finlandés, citado ya en la primera sección de este artículo, confirma que este riesgo no es hipotético, Finlandia destinó 20 MHz de la Banda 2.3 GHz a redes privadas locales y documentó restricciones derivadas de interferencia con otros servicios que ya operaban en esa banda.

Qué debería pasar a partir de aquí

Ninguna de estas cinco observaciones cuestiona el objetivo de política pública de facilitar el acceso de la industria mexicana a espectro radioeléctrico. Ese objetivo es correcto y urgente. Lo que la evidencia internacional cuestiona es el diseño específico elegido para alcanzarlo.

Con base en todo lo anterior, hay cinco líneas de acción concretas que la Comisión Reguladora de Telecomunicaciones podría valorar antes de dar por cerrado el diseño actual. Primero, sustituir, total o parcialmente, el esquema de reserva exclusiva por mecanismos de arrendamiento u obligación de despliegue local a cargo de los operadores móviles, siguiendo los modelos checo, danés, noruego y finlandés ya probados. Segundo, reconsiderar el límite de acumulación de espectro, para que la restricción se dirija de forma proporcional al operador con mayor concentración relativa, en lugar de excluir de facto a la totalidad de los operadores establecidos. Tercero, adoptar un esquema de neutralidad tecnológica y de servicio para la Banda 2.3 GHz, que permita ajustar el uso del espectro a la evolución de la demanda de mercado. Cuarto, publicar el mecanismo mediante el cual se determinarán los derechos recurrentes aplicables a las Regiones Industriales y a los Polígonos, y valorar si el nivel general de costo del espectro en México, ya evidenciado por dos devoluciones consecutivas de operadores móviles, es compatible con la viabilidad financiera de un usuario industrial individual. Quinto, desarrollar y publicar una metodología técnica de coordinación de interferencias entre los tres regímenes de uso, así como un procedimiento de denuncia, verificación y mitigación equivalente al que ya existe para el ámbito satelital.

México tiene la oportunidad de diseñar un esquema de espectro industrial que aprenda de lo que ya funcionó, y de lo que ya falló, en más de una decena de países que probaron variantes de este mismo modelo antes que nosotros. Ignorar esa evidencia, en un mercado donde el espectro ya es un recurso escaso y donde dos operadores móviles ya lo han devuelto por falta de rentabilidad, no sería solo un error de diseño regulatorio. Sería desperdiciar una banda completa de 100 MHz en un esquema con alta probabilidad de baja participación, mientras la industria mexicana sigue esperando la conectividad que necesita para dar el siguiente paso en su transformación digital.





De la Revolución Universal al Imperio de Nicho: El Destino del Blockchain

Erick Clavel
Vicepresidente de la Comisión de Arbitraje & ADR, ICC México
Socio de Clavel Abogados y Director de lawkit.mx

Hace algunos años escribí un artículo sobre cómo la tecnología blockchain estaba a punto de revolucionar la solución de controversias alrededor del mundo. En una plataforma llamada Kleros, la solución de conflictos legales sería de bajo costo, veloz y confiable. Era la tierra prometida tratándose de litigios y relaciones comerciales. Dada esa gran promesa y la versatilidad de la tecnología, muchos miraban al blockchain como la tecnología que resolvería los problemas de confianza, intermediación y costos de transacción en casi cualquier industria imaginable.

Han pasado años desde entonces. La revolución que con tanto anhelo se esperó no llegó. O, por lo menos, no como se imaginaba. Pese a no haber tenido un poder completamente transformador, blockchain es la base para un nuevo mercado que hoy crece a un paso desenfrenado. Este artículo cuenta esa historia: la de una tecnología todopoderosa que no lo fue, pero que es la base para la construcción de un imperio naciente de nicho.

¿Qué es blockchain?

Blockchain es en esencia un sistema de registro descentralizado. En lugar de que una sola entidad –un banco, un gobierno, una empresa– lleve el control y registro de operaciones y transacciones, miles de computadoras alrededor del mundo registran, verifican y conservan cada transacción de forma simultánea. Ese registro se agrupa en bloques y cada bloque se encadena al anterior mediante un identificador único, de manera que alterar un solo registro implicaría deshacer toda la cadena que le sigue. Es, dicho de otra forma, un libro contable compartido que nadie controla del todo y que, precisamente por eso, casi nadie puede manipular. Sobre esa tecnología se construyeron las criptomonedas (bitcoin siendo el estandarte), mecanismos para transferir valor sin bancos de por medio, arte digital en piezas únicas (NFTs) y, más adelante, los llamados contratos inteligentes o smart contracts: piezas de código que ejecutan automáticamente una consecuencia –normalmente, un pago– cuando se cumple una condición previamente pactada, sin que nadie tenga que reclamarlo, demandarlo o siquiera monitorearlo.

La era en que todo iba a cambiar

Entre 2016 y 2021, el discurso alrededor de blockchain fue, sin exagerar, mesiánico. Se hablaba de cadenas de suministro en blockchain completamente trazables donde Walmart podría rastrear una lechuga contaminada en segundos. Se hablaba de sistemas electorales inmunes al fraude, votando desde el teléfono con la misma certeza que hoy tenemos al hacer una transferencia bancaria. Se hablaba de transacciones inmobiliarias sin notarios, de remesas sin comisiones bancarias, de un internet financiero paralelo –las llamadas finanzas descentralizadas o DeFi– que operaría sin bancos centrales ni intermediarios. Y, desde luego, se hablaba de los contratos inteligentes como el mecanismo que, tarde o temprano, sustituiría buena parte de lo que hoy hacemos los abogados: negociar condiciones, redactar cláusulas y, sobre todo, litigar su incumplimiento.

Los mercados creyeron en esa narrativa de una tecnología arrasadora con una devoción notable. En 2017, la inversión mundial en empresas de blockchain rondaba apenas los 1,000 millones de dólares; para 2018 ya se había cuadruplicado a casi 4,000 millones. La fiebre no hizo más que crecer: para el tercer trimestre de 2021, únicamente en ese periodo de tres meses, los fondos de capital de riesgo inyectaron cerca de 8,500 millones de dólares en startups de criptomoneda, la cifra trimestral más alta registrada hasta ese momento. Las valuaciones de estas empresas superaban con creces a las de startups comparables en cualquier otro sector tecnológico: el fondo promedio pagaba múltiplos que en cualquier otra industria hubieran parecido irracionales, apostando a que quien conquistara primero esta tecnología se quedaría con industrias completas. Era, en el sentido más literal, apostar todo el dinero disponible a que el mundo entero migraría hacia esta tecnología.

No migró. O, más precisamente, migró mucho menos y mucho más lento de lo prometido. Pese al flujo de los grandes capitales hacia el blockchain y a que las pruebas piloto de su potencial abundaron –por ejemplo, el registro de nacimientos en blockchain que Illinois ensayó alrededor de 2017 o cuando el Tec de Monterrey emitió y registró los títulos profesionales de sus egresados en blockchain– pocas veces llegaron a producción real o a ser replicados a gran escala. Así, poco a poco, el torrente de capitales se fue secando. Y con eso, la prometida revolución universal se quedó en tan solo una idea de lo que pudo ser.

El nicho que nadie vio venir

Sin embargo, dentro de ese paisaje de expectativas incumplidas, el blockchain encontró un espacio muy específico para florecer: los llamados prediction markets o mercados de predicción que usan contratos inteligentes en blockchain. Este nuevo mercado es impactante y se basa en un modelo de negocio muy simple: plataformas como Polymarket y Kalshi –los líderes indiscutibles en esa industria– permiten a cualquier persona comprar y vender "acciones" sobre el resultado de un evento futuro –una elección, un partido de futbol, el lanzamiento de un nuevo producto– y ganar dinero si acertaron. Las plataformas cobran una cuota de transacción de todo aquello que se haya apostado.

En 2025, el volumen total operado en esta industria alcanzó los 63,500 millones de dólares, casi cuatro veces más que los 15,800 millones registrados apenas un año antes. La escalada no se ha detenido: en julio de 2026 —impulsado en buena medida por el mundial de futbol— el volumen combinado de Kalshi y Polymarket llegó a un récord histórico de 50,600 millones de dólares en un solo mes. Esto es más de tres veces todo lo que la industria completa había movido en el año 2024. El volumen de negocio es impresionante y más considerando que estas plataformas tienen menos de una década de existir. En esta industria es donde el blockchain y los contratos inteligentes encontraron su nicho.

En Polymarket, cada evento objeto de predicción –digamos, "¿ganará el candidato X la elección presidencial?"– genera dos tipos de “acciones”: SÍ y NO. Sus precios siempre suman un dólar y representan la probabilidad que el mercado le asigna a cada resultado: si la acción del SÍ cuesta 65 centavos, el mercado cree que hay 65% de probabilidad de que ocurra.

En estas plataformas, cada quién compra acciones del resultado que considera más probable a suceder. El dinero apostado queda resguardado en la plataforma hasta que el evento se resuelve. Cuando eso sucede, un sistema de verificación pública en blockchain determina quién ganó. Así, el sistema le paga automáticamente a cada acción ganadora y deja en cero a las perdedoras.





Nadie reclama, nadie litiga, nadie espera un cheque: el código lo resuelve y distribuye las ganancias de manera automática.

Gracias a estos contratos inteligentes, Polymarket construyó un mercado que veinte años atrás hubiera sido impensable: cualquier persona, en cualquier lugar del mundo, puede apostar sobre la incertidumbre cotidiana con pagos instantáneos. Lo que es más importante, es que fue precisamente la tecnología blockchain lo que dio a los usuarios un argumento de confianza distinto al de una casa de apuestas tradicional: no hay que creerle a Polymarket o a la casa de apuestas ni esperar a que alguien pague. En Polymarket siempre habrá un registro público de las operaciones, resultados y pagos inmediatos.

Aun en su nicho, blockchain no lo es todo

Sin embargo, más allá de todas las virtudes de blockchain y de cómo Polymarket las ha aprovechado para construir un negocio sólido y capturar una porción enorme de este mercado, el futuro de blockchain como cimiento de esta industria no está garantizado. La mejor prueba de ello es Kalshi. Kalshi es el otro gran jugador de esta industria que en 2026 logró superar a Polymarket en volumen mensual de transacciones. Si bien su modelo de negocio es el mismo, la infraestructura tecnológica de cada quien es diferente. Polymarket utiliza un modelo descentralizado gracias a blockchain y Kalshi usa un modelo centralizado.

En Kalshi se apuesta también a eventos futuros. Sin embargo, ahí no hay blockchain ni contratos inteligentes: cualquier persona deposita dinero y su apuesta queda registrada en los sistemas internos y privados de la empresa, tal como sucede en cualquier casa de apuestas tradicional. En la misma medida, es la propia compañía la que registra las operaciones, decide cómo se resuelve cada apuesta y hace los pagos correspondientes. En lugar de un registro público que cualquiera puede revisar, lo que respalda a los usuarios es la misma clase de confianza institucional que uno deposita en un banco por ser una entidad estrictamente regulada por una autoridad gubernamental. Por ende, Kalshi y el gran éxito que ha tenido es la prueba que el blockchain no es indispensable ni siquiera en esta industria en la que ha demostrado una utilidad innegable.

Blockchain no va a desaparecer en el futuro cercano, pero tampoco va a conquistar el mundo ni a transformar industrias enteras como alguna vez se anunció con tanta certeza. Lo que sí ha hecho, con método y paciencia, es algo menos vistoso pero igual de valioso: encontrar el problema exacto para el que su arquitectura resultó ser la solución perfecta, y ahí quedarse a construir un negocio de escala verdaderamente global. Y ahí radica la verdadera lección de esta historia: las tecnologías que se anuncian como todopoderosas casi nunca cumplen esa promesa, pero las que sobreviven al desencanto suelen encontrar, tarde o temprano, un terreno mucho más pequeño en el que pueden aportar un valor inmenso. Tal vez en cien años veamos que el legado del blockchain no fue cambiarlo todo, sino ser la chispa que impulso algo acotado, pero, no obstante, novedoso y grandioso.

Propiedad Intelectual en México: ¿Qué ley procesal aplicar?

Jaime Rodríguez
Vicepresidente de la Comisión de Propiedad Intelectual, ICC México
Socio
Diego Ballesteros
Asociado
Sofía Riquelme
Asociada
Olivares

La transición hacia el Código Nacional de Procedimientos Civiles y Familiares (CNPCyF) ha generado un escenario complejo de interpretación normativa en el sistema jurídico mexicano. Mientras que algunas materias avanzan hacia una adopción inmediata, otras enfrentan barreras explícitas en sus respectivos cuerpos normativos que sugieren, más bien, una adopción paulatina. Un análisis detallado de la Ley Federal de Protección a la Propiedad Industrial (LFPPI) y los recientes criterios emitidos por Poder Judicial de la Federación en materia de Amparo desvelan la disyuntiva entre una aplicación inmediata o gradual, dependiendo de la materia y del articulado del cuerpo normativo que la regule.

El esquema de supletoriedad en la LFPPI:

El diseño original de la LFPPI de 2020, preveía en su artículo 3° que, tanto la Ley Federal de Procedimiento Administrativo, como el Código Federal de Procedimientos Civiles, le eran aplicables supletoriamente, debiendo acudir primero a la primera y, de no existir disposición expresa en ella, a la segunda.

Sin embargo, ante la publicación en el Diario Oficial de la Federación del Código Nacional de Procedimiento Civiles y Familiares (CNPCyF) el 7 de junio de 2023, en un ánimo armonizador, el 14 de noviembre de 2025, se reformaron los artículos 3° y 400 de la LFPPI, a fin de sustituir al CFPC por el CNPCyF como segunda norma de aplicación supletoria a la LFPPI en materia adjetiva. Simultáneamente y en atención a los propios transitorios del nuevo CNPCyF, la reforma a la LFPPI incluyó en su artículo Segundo Transitorio que la aplicación del CNPyF quedaba supeditada a las declaratorias de vigencia que para tal efecto emitiera el Congreso de la Unión, fijando como fecha límite el 1° de abril de 2027.

Dicho de otra manera, de conformidad con el artículo Segundo Transitorio de la reforma a la LFPPI del 14 de noviembre de 2026, la aplicación supletoria del nuevo CNPCyF queda supeditada a la Declaratoria de aplicación gradual que para tales efectos emita el Congreso de la Unión, sin que la emisión de tal Declaratoria pueda excederse del 1° de abril de 2027, en cuyo caso, el referido CNPCyF entrará en vigor automáticamente en dicha fecha.

La disyuntiva entre inmediatez y gradualidad:

La aplicación paulatina del nuevo CNPCyF era una cuestión aceptada hasta la emisión de la jurisprudencia PR.A.C.CS. J/8 K (12a.), con registro digital 2031368 y de rubro "SUPLETORIEDAD EN EL JUICIO DE AMPARO. EN TÉRMINOS DEL ARTÍCULO 2o. DE LA LEY DE AMPARO, ES APLICABLE EL CÓDIGO NACIONAL DE PROCEDIMIENTOS CIVILES Y FAMILIARES DE FORMA INMEDIATA A PARTIR DE SU ENTRADA EN VIGOR, SIN ESTAR CONDICIONADA A LA DECLARATORIA DE INICIO DE VIGENCIA PREVISTA EN SUS ARTÍCULOS TRANSITORIOS" del pasado 17 de abril del presente año, mediante la cual, el Pleno Regional en Materias Administrativa y Civil de la Región Centro-Sur determinó que, para efectos del juicio de amparo, el CNPCyF es de aplicación obligatoria e inmediata, bajo las siguientes consideraciones:

- Literalidad normativa: Al no incluirse una disposición expresa respecto a la vigencia del CNPCyF dentro de la Ley de Amparo, debe estarse al texto vigente que ya cita expresamente al CNPCyF como el cuerpo normativo de aplicación supletoria a la Ley de Amparo.
- Norma general vs. Norma especial: La Ley de Amparo, al ser una norma especial, tiene supremacía sobre normas generales como lo es el propio CNPCyF.
- Voluntad del legislador: Se asume que el Congreso de la Unión omitió deliberadamente condicionar la entrada en vigor del CNPCyF, aceptando una adopción automática e inmediata.
- Certeza jurídica: Evita la incertidumbre jurídica al atender a la literalidad de la norma.

El escenario en relación con la Ley Federal de Protección a la Propiedad Industrial:

A diferencia de la Ley de Amparo, consideramos que la LFPPI contiene barreras insuperables que impiden interpretar análogamente lo dispuesto por la jurisprudencia PR.A.C.CS. J/8 K (12a.) del Pleno Regional en Materias Administrativa y Civil de la Región Centro-Sur, ya que, a diferencia de la Ley de Amparo, la reforma a la LFPPI del 14 de noviembre de 2026, sí contiene un régimen transitorio expreso que supedita la aplicación del CNPCyF hasta en tanto se emita la declaratoria correspondiente por el Congreso de la Unión.

En efecto, la redacción del artículo Segundo Transitorio de la LFFPI que establece la aplicación gradual del CNPCyF de conformidad con lo dispuesto por los propios artículos transitorios de dicho Código, contrarresta las consideraciones hechas valer por el mencionado Pleno Regional en Materias Administrativa y Civil de la Región Centro-Sur respecto a la Ley de Amparo, pues en el caso de la LFPPI éstas se ven superadas en virtud de los siguientes razonamientos:

- Literalidad normativa: Se incluye una disposición expresa respecto a la vigencia del CNPCyF.
- Norma general vs. Norma especial: La LFPPI, al ser a su vez una norma especial, tiene supremacía jerárquica sobre normas generales.
- Voluntad del legislador: Se asume que el Congreso de la Unión deliberadamente condicionó la entrada en vigor del CNPCyF, aceptando una adopción paulatina y gradual.
- Certeza jurídica: Evita la incertidumbre jurídica al atender a la literalidad de su Segundo Transitorio.

Lo anterior es igualmente aplicable a la Ley Federal del Procedimiento Contencioso Administrativo, pues en su reforma de fecha 14 de noviembre de 2025, incluyó expresamente el mismo transitorio que somete la entrada en vigor del nuevo CNPCyF a la emisión de la Declaratoria de vigencia que emita el Congreso de la Unión o, en su defecto, al 1° de abril de 2027 como la fecha límite para su entrada en vigor.





Además, debemos recordar que, entre 2014 y 2016, ante la implementación del Código Nacional de Procedimientos Penales (CNPP), la Suprema Corte de Justicia de la Nación (SCJN) resolvió que los plazos y declaratorias fijados por el legislador eran imperativos y que los operadores jurídicos no estaban facultados para anticipar la vigencia de una norma procesal bajo el único argumento de que resultaba más favorable o avanzada que la anterior.

Sin embargo, ante el congelamiento manifiesto de la reforma, no podemos descartar la tentación de abogados postulantes para exigir que se aplique análogamente lo resuelto respecto a la Ley de Amparo, pero en relación con la LFPPI, en cuyo caso, se vislumbran las dos siguientes vías de argumentación:

1. **Vía de control constitucional:** Cuestionar la constitucionalidad de los transitorios de la LFPPI a través del juicio de amparo, argumentando que dilatar el acceso al CNPCyF perpetúa la aplicación de un código obsoleto (el CFPC), vulnerando el principio de progresividad de los derechos humanos.
2. **Vía de aplicación adjetiva:** Sostener que las disposiciones procesales del CNPCyF que otorgan mayores garantías de defensa y simplifican la actividad probatoria regulan actos futuros en juicios vivos, por lo que su adopción inmediata no lesiona derechos sustantivos adquiridos. Esto bajo la premisa de que la Suprema Corte de Justicia de la Nación ya ha resuelto, específicamente mediante la tesis jurisprudencial VI.2o. J/140, con registro digital 195906 y rubro "RETROACTIVIDAD DE LAS LEYES PROCESALES. NO EXISTE POR REGLA GENERAL.", que, por regla general, no existe retroactividad tratándose de normas adjetivas.

El fondo de esta discusión cobra sentido al observar precedentes como el **Amparo en Revisión 9/2026**, resuelto por la Suprema Corte de Justicia de la Nación con fecha 26 de mayo de 2026, enfocado en la inconstitucionalidad del artículo 333 de la LFPPI debido a sus restricciones probatorias en los litigios de declaraciones administrativas en materia de propiedad industrial, en materia de prueba confesional y testimonial.

Si bien dicho juicio se resuelve bajo sus propios méritos constitucionales, expone con claridad la brecha existente entre legislaciones: mientras el CFPC mantiene un esquema cerrado, el CNPCyF introduce un extenso abanico de alternativas probatorias.

Como nota aparte, resulta irónico que las pruebas testimoniales y confesionales en materia de propiedad industrial no deban obrar por escrito, pues su desahogo mediante pliego de posiciones e interrogatorios únicamente dilatarán la resolución de asunto, lo cual atenta contra la propia naturaleza del nueva CNPCyF.

La modernización del derecho probatorio bajo el estándar del CNPCyF en materia de propiedad industrial:

Cuando la supletoriedad del CNPCyF finalmente entre en vigor, si no es que antes, el litigio estratégico en propiedad industrial experimentará un giro radical basado en cuatro pilares:

- Prueba confesional vs. Declaración de parte (Arts. 284 – 290): El antiguo CFPC utilizaba el clásico "pliego de posiciones" escrito y cerrado. El CNPCyF elimina el pliego rígido e introduce la "Declaración de parte", basada en interrogatorios abiertos y fluidos formulados directamente por los abogados o el juez.

- Disminución de plazos para aportar pruebas que provengan fuera del lugar del juicio (Art. 281): Pasa de dos a un mes si el lugar se encuentra en territorio nacional, de cuatro a dos meses si es cualquier otro país de Norteamérica, de 5 a tres meses para cualquier país de Centroamérica o el Caribe; manteniéndose el plazo de seis meses para Europa o América del Sur y el plazo del 7 meses para cualquier otro país.
- Prueba Pericial (Arts. 300-304): Bajo el CFPC anterior, los peritos entregaban un dictamen por escrito. Con el CNPCyF, los peritos están obligados a comparecer a la audiencia de juicio para sostener y defender su dictamen oralmente, además de someterse a interrogatorios directos y careos técnicos frente a los peritos de la contraparte. Si el perito contratado por una de las partes no se presenta a la audiencia obligatoria o no sabe defender su metodología ante las preguntas del juez, la prueba pericial se desecha de inmediato, perdiendo el caso de manera automática.
- Reducción de término para ofrecimiento de pruebas (Art. 176): El antiguo CFPC establecía hacía la distinción entre el plazo genérico para realizar manifestaciones y el plazo genérico para el ofrecimiento de pruebas, siendo el primero de tres días y el segundo de 10 días. Con la nueva redacción, se elimina la distinción y únicamente permanece un plazo genérico de tres días para tales efectos.
- Valoración probatoria (Art. 171): Aunque el CFPC usa sistemas tasados y de libre valoración, el CNPCyF establece que las pruebas deben valorarse de manera libre, lógica y basada en la experiencia (la sana crítica), obligando al juzgador a realizar una motivación racional profunda y explicar por qué otorga valor a cada prueba.
- Notificaciones mediante edictos (Art. 209): El antiguo CFPC establecía la obligación de publicarlos en el "Diario Oficial" y en uno de los periódicos diarios de mayor circulación en la República (tres veces, entre cada siete días), concediendo un total de 30 días para cumplimentar con las tres publicaciones correspondientes. Por el contrario, la redacción del nuevo CNPCyF establece que dichas publicaciones deberán realizarse en un mínimo de 15 días y en un máximo de 30 días, lo que deja al arbitrio de la autoridad el otorgamiento de un plazo dentro de dicho rango. Esto únicamente afecta a la Ley Federal del procedimiento Contencioso Administrativo, pues la LFPPI sí establece disposición expresa al respecto.
- Se amplía el catálogo de pruebas supervinientes (Art. 246): Incluye a las pruebas que no haya sido posible adquirir con anterioridad por causas que no sean imputables a la parte interesada; las que se ofrezcan y; las que se ofrezcan para la impugnación de pruebas de la contraria. contra acciones en lo principal o reconvencional y siempre que haya hecho oportunamente la designación expresa en los términos de lo dispuesto en el presente Código Nacional.
- Equivalencia digital y funcional (Arts. 308-313): Aunque ya veíamos superada esta cuestión mediante el Reglamento de la LFPPI, la redacción del nuevo CNPCyF es explícita al reconocer que los documentos electrónicos reciben el mismo valor que los formatos físicos y que las firmas electrónicas avanzadas y los expedientes judiciales digitales obtienen pleno reconocimiento legal, facilitando el uso de correos y capturas de plataformas como prueba material.
- Depuración procesal de objeciones (Arts. 325-329): Los plazos para impugnar documentos se adelantan a la contestación o desahogo de vista. Además, para acusar falsedad documental se vuelve obligatorio precisar causales y exhibir documentos de cotejo, desechando las objeciones genéricas.
- Adopción de tecnologías disruptivas (Arts. 308-331 y 348-350): Se legaliza el uso de registros digitales, medios ópticos y bases de datos descentralizadas como blockchain. El estándar de valoración se centrará en la fiabilidad de su cadena de custodia, otorgando un valor probatorio preferente a las cadenas de bloques de naturaleza pública.





Conclusión:

No podemos descartar que la reciente postura por parte del Pleno Regional en Materias Administrativa y Civil de la Región Centro-Sur en relación con la Ley de Amparo de rienda suelta para que las autoridades jurisdiccionales apliquen ese mismo criterio de manera análoga a la LFPPI, y será labor de nosotros, desde nuestra trinchera como custodios de derechos de propiedad industrial de nuestros clientes, procurar y asegurar que los juzgadores entiendan que la literalidad del Segundo Transitorio de la LFPPI supera cualquier interpretación que atente contra la gradualidad de la entrada en vigor del nuevo CNPCyF, para así garantizar la certeza jurídica de nuestros clientes y el respeto al debido proceso en materia de propiedad industrial.

La Era del Comercio Agéntico (A2B/A2A): Desafíos Jurídicos, Operativos y Regulatorios en la Redefinición del E-Commerce Transfronterizo

Xavier Careaga
Consejero de la práctica de Tecnología, Medios y Entretenimiento e IA (TMT & IA)
Ricardo Garcia
Socio de las prácticas de M&A y Tecnología, Medios y Entretenimiento & IA
Grecia Macías
Asociada del área TMT & IA
Ana Paula Boy
Asociada del área TMT & IA
Mauricio Fernández
Asociado del área TMT & IA
Galicia Abogados



Introducción y el cambio de paradigma: comprender la IA agéntica y el fin del comercio B2C tradicional

La Inteligencia Artificial (IA) y la tecnología han cambiadola forma en que el mundo se organiza, produce y consume. El comercio electrónico ha sido uno de los sectores que mayor transformación ha sufrido por esta revolución digital. Para comprender la magnitud de esta transformación es indispensable distinguir primero entre la IA que hemos conocido hasta ahora y la IA Agéntica.

Durante la última década, el comercio electrónico (e-commerce) ha utilizado sistemas de IA de carácter reactivo. Se trataba de algoritmos diseñados para tareas específicas y acotadas, como motores de búsqueda que sugerían productos relevantes (desde el siguiente video en YouTube o película en Netflix, a productos a comprar en Amazon), chatbots sencillos con respuestas preprogramadas o sistemas de recomendación visual que desplegaban publicidad según el historial de navegación o las preferencias del usuario. En todos estos casos, la presencia, supervisión y decisión final recaían de forma absoluta en un ser humano.

El modelo clásico de comercio electrónico B2C *(Business-to-Consumer)* se estructuró bajo la premisa fundamental de que un consumidor humano navega a través de una interfaz gráfica de usuario (pantallas, sitios web, aplicaciones móviles), evalúa catálogos, procesa información visual, reacciona a incentivos publicitarios o psicológicos (como descuentos por tiempo limitado o llamadas a la acción) y, finalmente, manifiesta su voluntad de compra mediante un acto físico (p. ej. un clic en el botón de “Comprar” o “Pagar”) que activa las pasarelas de pago y supone (o requiere) la aceptación de los Términos y Condiciones del sitio. La IA Agéntica rompe de raíz con este paradigma, ya queun “agente de IA” no es simplemente un programa al que se le hace una pregunta para recibir un texto, es un sistema informático autónomo dotado de capacidad para razonar en múltiples pasos, planificar estrategias, utilizar herramientas externas (como bases de datos, calculadoras o pasarelas de pago) y ejecutar acciones complejas en el mundo digital sin necesidad de supervisión humana constante.



Al usuario ya no le corresponde buscar, comparar ni llenar carritos de compra. En su lugar, encomienda un mandato u objetivo general a su agente de IA:

"Tengo un presupuesto de $1,500 dólares. Organiza mi viaje de negocios a Madrid para la próxima semana; compra los vuelos más directos, reserva un hotel a menos de 15 minutos de la sede de mi reunión con buenas evaluaciones de ejecutivos, coordina el transporte terrestre y asegúrate de que todas las tarifas permitan cambios de fecha sin penalización."

Ante esta instrucción (que en este ejemplo, es muy detallada y pormenorizada, lo cuál probablemente no siempre ocurrirá), el agente autónomo desglose la orden en decenas de subpedidos: accede a APIs de aerolíneas, analiza condiciones tarifarias, compara ubicaciones de hoteles, verifica políticas de cancelación, evalúa disponibilidad, negocia precios si la plataforma lo permite y ejecuta los pagos. Al terminar, al usuario le entrega un reporte final de las acciones realizadas.

Este salto cualitativo marca el nacimiento de dos nuevos modelos de interacción comercial:

- Agent-to-Business (A2B): Un agente de IA que actúa en representación de un consumidor humano interactúa directamente con los sistemas de ventas o servidores de una empresa.
- Agent-to-Agent (A2A): El agente del comprador no interactúa con una página web pensada para humanos, sino que se comunica directamente con el agente de IA del vendedor, entablando una negociación automatizada entre algoritmos para fijar precio, condiciones de entrega y garantías.

Esta transición desplaza al comercio digital desde la experiencia visual humana (Human-to-Software) hacia un entorno interconectado de máquina a máquina (Machine-to-Machine o M2M). Para las empresas, abogados y reguladores que estructuran el tráfico mercantil, se trata de un cambio de era y no solo de una simple actualización tecnológica. Conceptos jurídicos centenarios como la formación del consentimiento, la representación legal, los vicios de la voluntad, la responsabilidad civil por productos defectuosos y las reglas de libre competencia deben ser reinterpretados a la luz de esta nueva realidad.

Representación, Mandato y Contratación Automatizada

1. Naturaleza Jurídica del Agente de IA: ¿Sujeto, Herramienta o Representante?

Uno de los mayores dilemas del derecho mercantil hoy en día radica en determinar cómo encajar conceptualmente a un agente de IA cuando realiza una transacción comercial. La dogmática jurídica internacional clasifica el mundo en dos grandes categorías: personas (sujetos de derecho, sean físicas o morales, con capacidad para contraer obligaciones y ejercer derechos) y cosas (objetos de derecho).

Dado que la legislación internacional no reconoce personalidad jurídica autónoma a los sistemas de IA, un agente no puede ser, hoy por hoy, titular directo de derechos ni deudor de obligaciones. No obstante, clasificar a un agente de IA como una simple “herramienta inerte” (equiparable a una silla, un navegador web o un formulario de autocompletado) resulta insuficiente desde el punto de vista doctrinario y práctico.

Una herramienta tradicional carece de margen de maniobra y un agente de IA, en cambio, goza de discrecionalidad operativa, toda vez que analiza variables, pondera alternativas no programadas de forma explícita por su creador y toma decisiones autónomas para alcanzar la meta fijada. A diferencia del software tradicional cuyo comportamiento es estrictamente lineal y programático, y responde a una lógica determinista donde a la condición A sigue indefectiblemente la instrucción B, el agente de IA goza de discrecionalidad operativa. No sigue una secuencia rígida de comandos, sino que el agente analiza entornos complejos, evalúa escenarios cambiantes, pondera alternativas no previstas de forma explícita por su desarrollador, traza su propia ruta de ejecución para alcanzar la meta encomendada, y toma decisiones dinámicas en tiempo real, lo que impide tratar sus actuaciones como meras ejecuciones mecánicas.

Dado que el agente está, de cierta forma, actuando "a nombre y representación" del usuario aunque no de la forma histórica que significa esa frase, una solución que adopta parte de la doctrina legal emergente consiste en encuadrar al agente bajo la teoría de la representación o del mandato mercantil con facultades delegadas.

Bajo este esquema, el usuario humano o la empresa que opera el agente actúa como el mandante, mientras que el agente de IA funciona como un ejecutor digital o representante técnico. Los actos jurídicos que el agente perfecciona en el mercado digital (siempre que se mantenga dentro de los parámetros de actuación otorgados) no producen efectos en la esfera del software, sino que se imputan de manera directa, automática y vinculante a la esfera jurídica del mandante humano.

La Formación del Consentimiento y la Perfección del Contrato

El pilar sobre el que descansa todo el derecho de contratos es el acuerdo de voluntades, la cual se basa en la coincidencia exacta entre la oferta y la aceptación. En el comercio electrónico tradicional, la aceptación se produce en el preciso instante en que la persona presiona el botón de "Comprar".

En las transacciones agénticas (A2B y A2A), el momento y la forma del consentimiento se transforman radicalmente:

- Consentimiento preprogramado o parametrizado: La manifestación de voluntad del consumidor no ocurre en el checkout del sitio web, ocurre con anterioridad, al momento de definir las instrucciones, parámetros, rangos de precio, fechas y restricciones que el agente de IA tiene permitido gestionar. La transacción se perfecciona de forma autoejecutable cuando la oferta del vendedor calza exactamente dentro de la matriz de parámetros predeterminados por el usuario.
- La aceptación de Términos y Condiciones mediante API-Wrap: Las plataformas web operan con Términos y Condiciones (T&C) complejos diseñados mediante avisos flotantes o casillas de verificación (clickwrap). Pero ahora, el agente de IA es quien interactúa directamente mediante la API del servidor, pero no visualiza la interfaz ni hace clic en botones. Se requiere entonces la figura del API-wrap o Agent-wrap, un protocolo donde el agente de IA del comprador lee e interpreta automáticamente el código de los T&C del vendedor mediante Procesamiento de Lenguaje Natural (NLP), y vincula legalmente al usuario, aceptando "en su nombre". Si el agente acepta cláusulas desproporcionadas o renuncias a derechos fundamentales (como la jurisdicción local o garantías legales) sin haber recibido autorización explícita para transigir en la configuración de su mandante, la validez de dicha aceptación puede ser impugnada por falta de legitimación del representante.





Vicios de la Voluntad, Alucinaciones y la Actuación Ultra *Vires*

¿Qué sucede cuando la transacción sale mal debido a un fallo propio de la IA? Los modelos de lenguaje masivo (LLMs) y los sistemas agénticos son susceptibles a fenómenos como las alucinaciones (generación de información que se entiende como incorrecta, pero con apariencia de verdad, ya que son estadísticamente la respuesta más probable), errores en el procesamiento de datos o vulnerabilidades de seguridad conocidas como inyecciones de instrucciones (prompt injection), donde un tercero malintencionado oculta texto en una página web para manipular el comportamiento del agente.

Para determinar quién debe asumir la pérdida económica derivada de una compra errónea, el análisis jurídico exige diferenciar dos escenarios principales:

A. Error manifiesto o fallo de sistema (Nulidad por Vicio del Consentimiento)
Si el agente de IA incurre en una distorsión evidente (por ejemplo, reserva 100 habitaciones de hotel en lugar de 1 debido a un fallo sintáctico, o acepta un precio de $10,000 dólares por un producto que vale $100), el contrato puede ser anulado si el vendedor sabía o debía haber sabido, bajo el principio de buena fe mercantil, que la transacción respondería a un error manifiesto del sistema autoejecutable.

B. Actuación Ultra Vires por delegación ambigua (Asunción del Riesgo por el Usuario)
Si el usuario le otorga a su agente una instrucción vaga o excesivamente abierta (“compra los mejores boletos de avión a Madrid”) y el agente selecciona una tarifa de primera clase no reembolsable con tres escalas desfavorables pero formalmente válida dentro del presupuesto de $1,500 dólares, el contrato se considerará plenamente válido. El consumidor no podrá argumentar la nulidad del contrato frente al vendedor, debiendo asumir el riesgo mercantil derivado de una delegación deficiente (culpa en la instrucción).

En aquellos casos donde el fallo responda a un error de código, un sesgo de diseño o un defecto grave en el modelo desarrollado por la empresa proveedora de la IA, el usuario conservará la facultad de entablar una acción de responsabilidad por productos defectuosos o incumplimiento de servicios tecnológicos contra el desarrollador del software, trasladando el litigio fuera de la esfera mercantil del vendedor final.

Todo lo anterior, son interpretaciones del autor. Aún no se ha llegado a suficiente claridad legislativa, regulatoria o jurisprudencial.

III. Consentimiento, Privacidad y Transformación de la Publicidad Digital y la Analítica Comercial

1. La crisis del modelo tradicional de protección de datos

Las normativas globales sobre protección de datos personales (como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea o la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en México) fueron diseñadas bajo la doctrina del consentimiento informado, previo, expreso y puntual. Bajo este marco, cada vez que una persona visita un sitio web o realiza una compra, debe recibir un aviso de privacidad detallado y otorgar su autorización para finalidades específicas.

En el ecosistema agéntico, este modelo presencial y fragmentado deja de ser vigente. El usuario no otorga un consentimiento transacción por transacción, sino que concede una delegación operativa y continua de sus datos.

Para que un agente pueda buscar, negociar y comprar en su nombre, debe mantener un acceso constante a información altamente sensible:

- Datos financieros (tarjetas de crédito, claves de acceso, presupuestos disponibles).
- Historial de salud y restricciones dietéticas (alergias, medicamentos, preferencias).
- Ubicación geográfica en tiempo real y rutinas de movilidad.
- Preferencias personales de consumo, patrones de gasto e identidades de contactos cercanos.

El agente no actúa como un receptor pasivo de un aviso de privacidad, sino como un custodio activo de la identidad digital del usuario. Los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) deben integrarse directamente en la arquitectura de software del agente, permitiendo que este rechace automáticamente a vendedores cuya infraestructura de tratamiento de datos no cumpla con los estándares exigidos por el usuario, asumiendo que estos sean comunicados, o en su caso, estandarizados por el desarrollador del agente, como una diferencia competitiva de su agente, versus otros agentes en el mercado.

2. El fin del marketing y publicidad basado en la persuasión visual

Para la industria del comercio electrónico global, incluyendo la publicidad digital, el ascenso del modelo A2B representa un desafío operativo trascendental que se basa en la pérdida de visibilidad sobre el comportamiento del consumidor humano.

Durante décadas, las empresas de e-commerce han construido sus estrategias sobre métricas de comportamiento digital:

- Clickstream (el camino exacto de clics que hace un usuario en la pantalla).
- Tasas de rebote y tiempo de permanencia (dwell time) en la página.
- Heatmaps visuales (dónde mueve el cursor o fija la mirada el usuario).
- Pruebas A/B sobre colores de botones, tipografías y colocación de banners promocionales.
- Otros elementos de comportamiento, preferencias, e interacciones, desde un “me gusta”, a compartir contenido, verlo más de una vez, y publicar comentarios.

Todos estos elementos pierden su razón de ser cuando quien visita la tienda no es un ojo humano influenciable por el diseño o la urgencia de una oferta, sino un script algorítmico que consulta la base de datos a través de una API en milisegundos.

El agente no responde a los colores de la interfaz, ni a las compras de impulso en la línea de pago, ni a los anuncios publicitarios llamativos. Procesa únicamente datos estructurados como especificaciones del producto, precio final, costo de envío, tiempo de entrega, políticas de devolución y calificaciones objetivas.

Esto “ciega” a las herramientas tradicionales de analítica comercial (tales como el píxel de Meta, Google Analytics, los tags de conversión de Google Ads o Amazon Attribution), obligando a las empresas a migrar sus inversiones desde el marketing visual y la persuasión psicológica hacia la estructuración óptima de sus datos e interfaces de integración de software.

Esto transformaría de forma radical el mercado de la publicidad y el marketing, cambiando las reglas de juego para siempre.





IV. Competencia Desleal, Mercado y Barreras de Acceso Digital

1. Desintermediación de marcas, colusión algorítmica y discriminación de precios

La presencia de agentes autónomos actuando en el mercado modifica las reglas de la libre competencia. Cuando los consumidores dejan de buscar productos directamente y confían la selección a una IA que evalúa variables objetivas, se produce un fenómeno de desintermediación de la marca.

Estrategias tradicionales como el empaque atractivo, el posicionamiento en anaquel digital o la construcción de lealtad a la marca mediante emociones pierden efectividad, ya que si el agente determina que el producto de una marca blanca o de un competidor menor ofrece mejores especificaciones técnicas y un costo total inferior, seleccionará esa opción.

Al mismo tiempo, la interacción de agentes de IA entre sí, introduce dos riesgos serios de competencia desleal y prácticas monopólicas:

A. Colusión algorítmica tácita

Cuando los agentes de IA de los vendedores monitorean constantemente el mercado y ajustan precios en tiempo real mediante aprendizaje automático (llamado Dynamic Pricing Agents), podrían llegar a "entender" sin necesidad de que exista un acuerdo, llamada o reunión entre humanos que la estrategia más rentable para ambas partes no es competir bajando precios, sino mantener un nivel de precios coordinado y artificialmente alto. La detección y sanción de estos "cárteles algorítmicos" representa un desafío para las autoridades de competencia económica que no existía hasta ahora, pues las leyes actuales exigen probar la existencia de un acuerdo o concertación voluntaria entre competidores.

B. Discriminación de precios agéntica en tiempo real

Un sitio vendedor puede detectar qué tipo de agente lo está visitando mediante la solicitud de la API. Si el agente comprador revela de manera inadvertida que su mandante posee un perfil socioeconómico alto o una urgencia de compra inmediata, el agente vendedor puede generar dinámicamente un precio más elevado para esa transacción específica, explotando la disposición a pagar del consumidor sin su conocimiento.

C. Seducción algorítmica engañosa (SEO Agéntico Desleal)

Así como las marcas compiten hoy por aparecer en los primeros lugares de búsqueda de Google mediante técnicas de SEO (Search Engine Optimization), en el e-commerce agéntico surgirán técnicas para "engañar" o manipular las decisiones de los agentes de IA. Esto incluye la inyección de metadatos falsos o texto oculto en las plataformas de venta diseñado específicamente para distorsionar los filtros de evaluación del algoritmo y forzar la compra de sus productos sobre opciones objetivamente superiores. Será, probablemente, una "carrera armamentista" entre los agentes de los compradores y los vendedores.

2. Bloqueo de agentes (Agent Blocking) y el acceso restringido al mercado

Para proteger sus modelos de negocio, muchas plataformas e-commerce tradicionales han comenzado a implementar sistemas defensivos agresivos contra bots y agentes de scraping automatizado (mediante CAPTCHAs, bloqueos de direcciones IP o cláusulas en sus T&C que prohíben el acceso mediante software).

Esta práctica plantea un gran debate en el derecho de la competencia económica. Si una plataforma dominante en el mercado digital bloquea el acceso a los agentes compradores de terceros (o bien, permite el acceso exclusivo a su propio agente de IA integrado), dicha conducta podría ser tipificada por los tribunales y autoridades antimonopolio como:

- Una negativa injustificada de trato mercantil.
- Una práctica de denegación de acceso a un insumo esencial para el comercio digital.
- Una barrera artificial de entrada al mercado que vulnera el principio de neutralidad de las redes comerciales.
- O, incluso, tal vez, como una práctica discriminatoria.

Al mismo tiempo, genera la duda de si esos sitios no estarán condenándose a sí mismos al cerrarse a un mercado que todo indica será el estándar, para elegir un mercado que se reducirá año por año, de compradores "orgánicos", es decir, humanos reales.

V. Responsabilidad Civil, Pagos Programáticos y Desafíos Operativos

1. Pagos programáticos y la infraestructura de las Agentic Wallets

El sistema financiero transaccional contemporáneo está construido sobre la exigencia de autenticación presencial humana. Normativas como la Directiva de Servicios de Pago (PSD2) en Europa imponen la Autenticación Reforzada del Cliente (SCA), la cual requiere validar al menos dos de tres factores antes de autorizar una compra:

1. Algo que el usuario sabe (una contraseña o PIN).
2. Algo que el usuario posee (un teléfono celular para recibir un código OTP vía SMS).
3. Algo que el usuario es (biometría, como la huella dactilar o reconocimiento facial).

Este modelo pensado para humanos es inviable en una transacción agéntica donde la compra se ejecuta a las tres de la mañana mientras el usuario duerme. Para hacer operativo el comercio A2B y A2A, la infraestructura bancaria y las redes de pago están desarrollando la figura de los pagos programáticos mediante Billeteras Agénticas (Agentic Wallets).

En este esquema, el usuario no comparte los datos reales de su tarjeta de crédito con el agente de IA, sino que emite un token de pago restringido criptográficamente firmado. Este token incorpora reglas duras inviolables, incluyendo un límite máximo de gasto, una ventana de tiempo definida para la ejecución de la transacción y una lista cerrada de categorías de comercios autorizados. La validez jurídica del pago y la responsabilidad por transacciones no reconocidas dependerán de si la operación respetó los parámetros de la firma digital delegada o si existió una brecha en la custodia del token.

2. La redefinición de la protección al consumidor y el derecho de retracto

Las leyes de protección al consumidor a nivel internacional otorgan a los compradores en línea el derecho de arrepentimiento o retracto (la facultad de devolver un producto adquirido por internet dentro de un plazo de 5 a 14 días sin necesidad de justificación y con reembolso total).





El fundamento sociológico de este derecho siempre fue proteger al consumidor vulnerable frente a:

- Las compras compulsivas o impulsivas provocadas por el marketing agresivo.
- La imposibilidad física de examinar el producto antes de la compra.
- La asimetría de información frente al vendedor profesional.

En el comercio agéntico, un agente decide qué producto adquirir tras comparar objetivamente sus especificaciones, en lugar de responder a impulsos emocionales o técnicas de persuasión visual. Este cambio cuestiona la aplicación irrestricta del derecho de retracto.

Si los usuarios utilizan agentes de IA de forma general para comprar y devolver productos constantemente sin costo, la logística inversa generará pérdidas importantes para las pequeñas y medianas empresas vendedores. Los tribunales y legisladores deberán ajustar el alcance de estas garantías, restringiendo el derecho de retracto cuando la compra haya sido ejecutada por un agente autorizado que operó estrictamente dentro de las especificaciones correctas solicitadas por el cliente.

VI. Estrategia Corporativa y Gobernanza Legal Agéntica: De la Teoría a la Práctica

El desarrollo del comercio agéntico no puede ser tratado como una simple actualización tecnológica que compete al departamento de sistemas. Representa una transformación en la forma de contratar, asumir riesgos y estructurar relaciones comerciales. Como vimos, afecta cada paso de una compra, desde la publicidad, hasta las garantías y la responsabilidad civil.

Aquellas empresas o despachos que pretendan operar con éxito en este nuevo ecosistema deberán implementar de inmediato un marco formal de Gobernanza Legal Agéntica. Esta disciplina integra el análisis jurídico preventivo con la ingeniería de software para blindar a las organizaciones ante los nuevos riesgos del mercado automatizado.

Las acciones estratégicas prioritarias que deben abordar las empresas incluyen:

1. Rediseño contractual y adaptación de T&C: Reescribir las políticas de las plataformas e-commerce para establecer términos específicos aplicables a la interacción mediante APIs para agentes de IA externos. Se deben definir con claridad las reglas de aceptación contractual, los límites de responsabilidad por fallas de comunicación de la red y las condiciones de uso permitido para la extracción de datos.
2. Matrices de delegación y control de mandatos algorítmicos: Diseñar e implementar políticas internas para la adquisición y uso de agentes de IA dentro de las empresas (compras corporativas A2B). Estas matrices deben fijar techos de gasto por transacción, límites temporales y requerir la inclusión de controles de supervisión humana (Human-in-the-Loop) para operaciones de alto valor o compras estratégicas.
3. Cumplimiento de privacidad de datos: Adaptar las arquitecturas de recopilación de datos para garantizar que el tratamiento de perfiles de consumo cumpla con los principios de minimización y responsabilidad, evitando la transmisión no autorizada de datos sensibles a través de los prompts del agente.
4. Gestión de responsabilidad en la cadena de suministro de IA: Revisar y negociar los contratos de licencia y uso con los proveedores de modelos de IA y desarrolladores de software agéntico, exigiendo cláusulas claras de indemnización y cobertura de seguros ante pérdidas económicas derivadas de alucinaciones, fallas operativas o brechas de seguridad del algoritmo.

Las empresas e instituciones que logren anticiparse a estas fricciones legales y operativas evitarán litigios costosos y sanciones regulatorias, lo que permitirá que se posicionen como líderes en la creación de los estándares comerciales del futuro.

VII. Recomendaciones Normativas y el Rol de la ICC

Ante el riesgo inminente de que las legislaciones nacionales aborden la IA agéntica de forma fragmentada y contradictoria, las organizaciones multilaterales están llamadas a desempeñar un papel armonizador indispensable, además de aconsejar y liderar al sector comercial privado en estrategias de protección a todos los involucrados en el comercio, tanto productores, vendedores, consumidores, y ahora incluso a los desarrolladores de agentes y otras soluciones con IA.

La Cámara de Comercio Internacional (ICC), en estrecha colaboración con organismos como la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI / UNCITRAL), es la institución natural para liderar la actualización de los instrumentos del derecho mercantil global mediante:

1. Redacción de cláusulas modelo para el comercio agéntico (A2B / A2A): Emitir directrices internacionales que definan el momento de perfección del contrato, la distribución del riesgo y responsabilidad por errores algorítmicos y las reglas de validez de las firmas y pagos delegados.
2. Protocolos de identificación y transparencia algorítmica: Promover estándares técnicos y jurídicos para que los agentes de IA se identifiquen formalmente ante las plataformas comerciales, permitiendo verificar la identidad del mandante y la validez de los poderes otorgados al software, así como prohibición de prácticas para engañar a agentes en perjuicio de los consumidores.
3. Armonización regulatoria transfronteriza: Impulsar la convergencia entre marcos normativos complejos (como el Reglamento de Inteligencia Artificial (EU AI Act) de la Unión Europea, las directivas de Estados Unidos y las legislaciones emergentes en América Latina), evitando que la burocracia digital cree barreras técnicas injustificadas al libre flujo del comercio electrónico internacional.

La era del comercio agéntico ya no forma parte del terreno de la ciencia ficción; es una reestructuración operativa y legal en pleno despliegue. Garantizar la certeza jurídica en este nuevo entorno es la condición indispensable para mantener la confianza, la equidad y la fluidez del comercio global en el siglo XXI.



Economía Digital respecto de “Ciberseguridad & Protección de Datos Personales en Operaciones Transfronterizas”

Luis G. Ramirez Villela
Socio

Georgina Herrera Guerrero
Asociada

Müggenburg, Gorches y Peñalosa, S.C.



El comercio exterior ya no se detiene en la aduana

El despacho aduanero tiene reglas conocidas, tiempos previsibles y autoridades identificadas, sin embargo, la operación digital transfronteriza no. Cuando una empresa envía mercancías al exterior, hay un momento preciso en que cruzan la frontera, cuando envía datos (clientes, empleados, transacciones, sistemas integrados, etc.) ese cruce ocurre en milisegundos, de manera continua, a través de múltiples jurisdicciones, sin que nadie estampe un sello ni valide un documento de origen.

Esa diferencia, que puede parecer técnica, es en realidad jurídica y estratégica, los datos tienen territorio de origen, territorio de almacenamiento, territorio de procesamiento y territorio donde reside la persona a quien pertenecen. En una cadena de suministro digital moderna, esas cuatro dimensiones rara vez coinciden y cada una puede activar obligaciones distintas ante autoridades con competencias superpuestas.

Lo que esto significa en términos operativos es que una sola operación comercial puede poner a una empresa bajo la jurisdicción simultánea de la Secretaría Anticorrupción y Buen Gobierno (nueva autoridad en materia de protección de datos personales del sector privado en México desde marzo de 2025); de las autoridades supervisoras de los Estados miembros de la Unión Europea, coordinadas por el Comité Europeo de Protección de Datos; y de reguladores sectoriales en los Estados Unidos, cuya legislación de privacidad se ha desarrollado de forma fragmentada por estado y por sector industrial. Ninguno de estos actores cede jurisdicción, todos pueden actuar y en no pocos casos, actúan de maneras que no son fácilmente conciliables.

La Conferencia de las Naciones Unidas sobre Comercio y Desarrollo ha documentado esta dinámica con precisión: los flujos transfronterizos de datos son componente estructural del comercio internacional del siglo XXI, y la fragmentación regulatoria global (la llamada "balcanización digital") afecta de manera desproporcionada a las empresas de economías en desarrollo, que deben asumir costos de adaptación que sus contrapartes en jurisdicciones con marcos más reconocidos no enfrentan de la misma forma. México está dentro de ese cuadro.

Derivado de lo anterior, se vuelve inminente que las empresas que realicen operaciones de comercio internacional verifiquen no sólo el cumplimiento de leyes locales sino también el cumplimiento de tratados internacionales y leyes aplicables en el país destino.

Cuando el proveedor tecnológico define el riesgo regulatorio

Hay un patrón que se repite en la práctica corporativa con desconcertante regularidad: la empresa contrata un servicio tecnológico global (plataforma de análisis de datos, herramienta de inteligencia artificial como servicio, sistema de gestión de recursos humanos, entre otras) bajo términos contractuales estándares redactados en otro país para cumplir con la ley de ese otro país. El área de tecnología celebra la eficiencia, el área jurídica firma sin revisar a profundidad, el área de compliance, si existe formalmente, llega tarde al proceso.

El resultado es una cadena de tratamiento de datos que el responsable formal (la empresa mexicana) no controla ni comprende en su totalidad: no sabe en qué jurisdicción se almacenan los datos de sus clientes, no tiene claridad sobre qué subcontratistas del proveedor acceden a esa información, bajo qué condiciones y desde qué país, no ha negociado cláusulas de notificación en caso de incidente de seguridad, no puede auditar, no puede verificar el cumplimiento de sus propias obligaciones legales porque no tiene acceso suficiente a los sistemas de quien, en la práctica, ejecuta el tratamiento.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares vigente desde el 21 de marzo de 2025 amplió la definición de responsable del tratamiento: ya no se requiere que quien trate los datos haya tomado formalmente las decisiones sobre ese tratamiento; basta con que los trate. El texto también distingue con claridad al encargado (quien actúa por cuenta del responsable). Esta arquitectura tiene consecuencias jurídicas concretas: el responsable no se libera de sus obligaciones por el solo hecho de delegar operativamente el tratamiento a un tercero. Sin un acuerdo de tratamiento de datos debidamente estructurado que establezca obligaciones específicas para el encargado, la delegación operativa no equivale a transferencia de responsabilidad legal.

Este punto (que el outsourcing tecnológico no exonera al responsable) es, quizás, el más consistentemente subestimado en la práctica corporativa mexicana y es precisamente el que genera mayor exposición cuando ocurre un incidente: la autoridad no pregunta quién procesó los datos, sino quién los recopiló y decidió su tratamiento.

La arquitectura técnica como origen de exposición jurídica

Un sistema de cómputo distribuido en múltiples nubes, con interfaces de programación que conectan a decenas de proveedores externos, con accesos remotos habilitados desde distintos países y con datos replicados en varios nodos por razones de disponibilidad o rendimiento, es funcionalmente eficiente y jurídicamente complejo. No porque la tecnología sea deficiente, sino porque amplía la superficie de exposición a incidentes de una forma que los controles diseñados para entornos concentrados y relativamente homogéneos no están preparados para gestionar.

La documentación de incidentes de seguridad de los últimos años apunta en una dirección consistente: los compromisos más costosos no responden a vulnerabilidades técnicas de alta sofisticación, sino a fallas organizacionales, credenciales mal protegidas, accesos privilegiados no revocados al término de una relación contractual, almacenamiento en la nube dejado en configuración pública por error de un proveedor externo, subcontratistas con acceso a sistemas sensibles que no estaban sujetos a controles equivalentes a los del contratante principal. La debilidad, casi siempre, está en el eslabón que nadie se asignó vigilar.





El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología de los Estados Unidos, en su versión 2.0 publicada en febrero de 2024, incorpora explícitamente la gobernanza como función transversal del sistema, reconociendo que, sin responsabilidad organizacional definida, sin políticas que se apliquen efectivamente y sin integración de la ciberseguridad en las decisiones estratégicas y operativas, los controles técnicos resultan insuficientes. Este no es un hallazgo nuevo; es un reconocimiento que se ha vuelto imposible de ignorar.

La norma ISO/IEC 27001:2022, de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, codifica esa premisa en un sistema certificable y auditable. Su relevancia para empresas mexicanas que participan en cadenas de valor internacionales se ha convertido en condición de elegibilidad en procesos de contratación con empresas europeas, en exigencia de algunos esquemas de licitación internacional y en parámetro de referencia en procesos de debida diligencia previos a inversiones o fusiones transfronterizas. Tenerla no garantiza seguridad; no tenerla, en ciertos mercados, cierra puertas.

La Agencia de la Unión Europea para la Ciberseguridad ha publicado análisis y marcos de referencia sobre gestión de riesgos en servicios de computación en la nube y en cadenas de suministro digitales que, aunque emanan de una autoridad de otra jurisdicción, tienen utilidad práctica directa para cualquier empresa mexicana que interactúe con contrapartes o proveedores europeos. No como obligación directa, sino como lenguaje común que facilita la negociación contractual y la acreditación de controles ante contrapartes que sí están obligadas a verificarlos.

México: marco vigente, brechas reales

El régimen mexicano de protección de datos personales atravesó en 2025 una transformación institucional de primer orden. El 20 de marzo de ese año se publicó en el Diario Oficial de la Federación un decreto que expidió simultáneamente tres nuevos ordenamientos: la Ley General de Transparencia y Acceso a la Información Pública, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Esta última entró en vigor al día siguiente, abrogando la ley homónima de 2010 que había sido durante quince años el eje del sistema de protección de datos del sector privado. El Reglamento de la ley anterior (publicado en 2011) quedó en una situación transitoria: sigue siendo el único instrumento reglamentario aplicable mientras la Secretaría Anticorrupción y Buen Gobierno (la nueva autoridad) no emita el reglamento correspondiente a la ley vigente, para cuya expedición la norma fijó un plazo de 90 días naturales a partir de su entrada en vigor.

Ese rezago reglamentario no es un detalle menor: afecta precisamente los aspectos más técnicos de la operación cotidiana, incluyendo las reglas específicas para transferencias nacionales e internacionales de datos y los requisitos de forma del aviso de privacidad. En cuanto al contenido sustantivo, la nueva ley conserva la arquitectura de principios y deberes que caracterizaba a su predecesora (licitud, consentimiento, calidad, proporcionalidad, responsabilidad) y mantiene los derechos de acceso, rectificación, cancelación y oposición.

No introduce, por tanto, una ruptura de fondo con el modelo previo, sin embargo, lo que sí modifica de manera relevante es el universo de sujetos obligados: la definición de "responsable del tratamiento" ya no requiere que quien trata los datos haya tomado decisiones sobre su tratamiento; basta con que realice el tratamiento, lo que amplía considerablemente la base de aplicación de la ley e incluye ahora a los encargados con mayor nitidez que antes.

También extiende la noción de "titular" para incluir, bajo ciertas condiciones, a personas morales (un cambio con implicaciones prácticas en contextos B2B que todavía está siendo procesado por la comunidad jurídica.)

El artículo 36 de la nueva ley preserva el régimen de transferencias internacionales de datos: estas pueden realizarse sin consentimiento del titular en los supuestos que la norma enumera (cumplimiento de obligaciones legales, relaciones entre empresas del mismo grupo corporativo, interés público, entre otros), y en los casos que no encuadren en esas excepciones, el titular debe estar informado y no haber manifestado oposición. La estructura no varía sustancialmente respecto al régimen anterior, lo que perpetúa sus limitaciones ya conocidas: la ausencia de un mecanismo sistemático de legitimación de transferencias comparable a las cláusulas contractuales tipo del Reglamento General de Protección de Datos, y la falta de un registro o sistema de notificación que permita a la autoridad ejercer supervisión efectiva sobre los flujos internacionales de datos originados o recibidos en México.

Las empresas que operan transferencias transfronterizas de manera rutinaria siguen dependiendo, en la práctica, de soluciones ad hoc cuya solidez jurídica varía considerablemente caso por caso.

El cambio institucional más significativo (y también el más discutido) no está en el contenido normativo sino en la estructura de autoridad. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales fue extinguido como consecuencia de la reforma constitucional en materia de simplificación orgánica de diciembre de 2024, sus funciones en materia de protección de datos personales en posesión de los particulares fueron transferidas a la Secretaría Anticorrupción y Buen Gobierno, una dependencia del Poder Ejecutivo Federal. La diferencia respecto al modelo anterior es sustantiva: el INAI era un órgano constitucional autónomo, con independencia funcional y financiera garantizada en la Constitución, con comisionados con mandatos escalonados y con la obligación de rendir informe anual al Congreso de la Unión. La Secretaría Anticorrupción y Buen Gobierno depende directamente del Ejecutivo, carece de esa independencia orgánica, y la obligación de reporte al Congreso fue suprimida.

Esto tiene implicaciones que trascienden la organización interna del Estado: la independencia de la autoridad supervisora es uno de los criterios que la Comisión Europea evalúa al analizar si un régimen de protección de datos ofrece garantías esencialmente equivalentes a las del Reglamento General de Protección de Datos, como condición para otorgar una decisión de adecuación. México ya enfrentaba ese camino cuesta arriba sin decisión de adecuación; el modelo institucional adoptado en 2025 no lo simplifica.

La Estrategia Nacional de Ciberseguridad, publicada en noviembre de 2017, sigue siendo el único documento rector del Estado mexicano en esa materia, quince meses después de su publicación, no derivó en legislación específica que establezca obligaciones sectoriales claras, mecanismos de reporte de incidentes para el sector privado o estándares mínimos diferenciados por industria.

La Secretaría de Seguridad y Protección Ciudadana, a través de la Coordinación Nacional de Seguridad Cibernética y el Centro de Respuesta a Incidentes Cibernéticos, opera en ese espacio con competencias de coordinación y respuesta, pero sin el respaldo de una norma que obligue al sector privado a notificar incidentes ni defina responsabilidades de cooperación. México sigue siendo uno de los pocos países miembros de la Organización para la Cooperación y el Desarrollo Económicos que no cuenta con legislación específica en materia de ciberseguridad, una situación que la Ley Federal de Telecomunicaciones y Radiodifusión (que cubre a los concesionarios del sector, no a la generalidad de la economía digital) solo remedia de manera parcial y sectorial.





México es miembro fundador del Foro Global de Reglas de Privacidad Transfronteriza, establecido en 2022 por nueve jurisdicciones (entre ellas Canadá, Japón, Singapur y los Estados Unidos) con el propósito de crear un sistema de certificación internacional que facilite los flujos transfronterizos de datos sobre bases de confianza verificable y reconocimiento mutuo. En junio de 2025, ese Foro lanzó formalmente los sistemas de certificación Global CBPR y Global PRP para controladores y procesadores de datos, respectivamente. La participación activa de México en este mecanismo representa una vía concreta (complementaria a la actualización legislativa interna) para mejorar su posición en el ecosistema global de flujos de datos, sin depender exclusivamente de la obtención de una decisión de adecuación europea cuyas condiciones, en el contexto institucional actual, resultan difíciles de satisfacer en el corto plazo.

El desafío real del marco mexicano es de efectividad institucional, coherencia regulatoria y capacidad supervisora en un entorno de operaciones transfronterizas que crece con más rapidez que la infraestructura de cumplimiento. Una autoridad sin independencia orgánica acreditada, un reglamento pendiente de actualización, una estrategia de ciberseguridad sin legislación de respaldo y transferencias internacionales de datos que se formalizan (cuando se formalizan) mediante soluciones contractuales no estandarizadas: ese es el inventario práctico con el que operan las empresas con presencia en México.

Responsabilidad corporativa en la cadena digital de proveedores

Hay una zona gris contractual que genera litigios con frecuencia y que pocas organizaciones anticipan de manera suficiente: los subprocesadores. Un proveedor de servicios tecnológicos puede cumplir con todas las exigencias del cliente en materia de seguridad y privacidad, y aun así subcontratar parte del procesamiento de datos con un tercero que opera con estándares menores, bajo derecho de una jurisdicción con regulación débil o con esquemas de acceso que el cliente contratante nunca conoció.

Sin cláusulas de flujo que obliguen al proveedor principal a imponer a sus subcontratistas las mismas condiciones acordadas con el cliente, la cadena de tratamiento queda rota en términos de responsabilidad jurídica. Cuando ocurre un incidente en el que el subprocesador es el punto de origen (como ha ocurrido en casos documentados de ataques a cadenas de suministro de software) la pregunta sobre quién responde frente al titular de los datos y frente a la autoridad regulatoria no tiene una respuesta contractual clara. El responsable formal del tratamiento es quien carga con las consecuencias.

La debida diligencia de terceros en materia de datos y ciberseguridad exige, antes de contratar, revisar las políticas de subcontratación del proveedor, las jurisdicciones donde se alojan y procesan los datos, los mecanismos de notificación de incidentes, las condiciones de auditabilidad y los procedimientos de retención y eliminación de información al término de la relación. No se trata de un proceso paralelo a la contratación: es parte constitutiva de la decisión de negocio, y tratarlo como formalidad posterior tiene costos que se manifiestan exactamente cuando menos se quiere: durante una crisis.

Este análisis también revela, con frecuencia, que los contratos estándar de los grandes proveedores tecnológicos globales están redactados para minimizar su exposición en cualquier jurisdicción. La empresa que firma sin negociar acepta, de manera implícita, una posición de riesgo que su propio marco jurídico local no necesariamente le permite asumir, y que la autoridad supervisora no reconocerá como justificación válida.

vi. Gobernanza de datos: una arquitectura, no un documento

Gobernar los datos de una organización significa establecer quién tiene autoridad para decidir qué se trata, con qué propósito, bajo qué condiciones, con acceso de quiénes y con consecuencias internas definidas si algo sale mal.

En operaciones transfronterizas, esa estructura debe resolver tensiones reales: la empresa matriz puede imponer estándares globales que entren en tensión con requisitos locales de retención o localización de datosción de datos; el proveedor de nube puede actualizar unilateralmente sus términos, modificando condiciones bajo las cuales se tratan datos de clientes o empleados mexicanos; una filial puede compartir información con la central extranjera sin que la función jurídica local haya verificado si esa práctica es consistente con la ley aplicable en México o con los términos del contrato de servicio vigente.

El principio de responsabilidad demostrada (articulado en el Reglamento General de Protección de Datos bajo el concepto de accountability y adoptado como referente por las Directrices sobre Privacidad de la OCDE) invierte la lógica del cumplimiento reactivo tradicional: no basta con no infringir; el responsable debe poder demostrar, en cualquier momento, que tiene implementados los controles, los procedimientos y los registros que respaldan su posición. Este estándar está llegando a México por vía contractual, aunque aún no se haya incorporado plenamente.

Sobre la respuesta a incidentes conviene ser preciso: la obligación de notificar al titular cuando una vulneración de seguridad afecta significativamente sus derechos está en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
.
Lo que distingue al régimen del RGPD es el plazo específico (72 horas para notificar a la autoridad supervisora tras conocer la brecha) y el grado de detalle en los requisitos de documentación.

La diferencia entre los dos marcos no es de principio sino de exigibilidad concreta, en esa diferencia se explica, en buena parte, la asimetría en la madurez de los programas de respuesta a incidentes entre empresas que operan bajo derecho europeo y empresas que operan exclusivamente bajo derecho mexicano. Con la Secretaría Anticorrupción y Buen Gobierno aún consolidando sus criterios de actuación y pendiente la emisión del nuevo reglamento, esa asimetría probablemente se mantenga en el corto plazo.

Criterios para una gestión competente del riesgo transfronterizo

Las organizaciones que gestionan bien estos riesgos no lo hacen por cumplimiento: lo hacen porque han comprendido que la confianza de clientes, socios e inversores en entornos internacionales depende, en parte, de que su posición regulatoria sea sólida y verificable. Hay cuatro criterios que distinguen sistemáticamente a esas organizaciones de las que simplemente reconocen los riesgos sin gestionarlos.

Conocer el ecosistema real de datos. El punto de partida es siempre un inventario actualizado: qué datos se tratan, dónde, por quién, con qué propósito y bajo qué base legal. Este mapeo no es documentación burocrática; es el diagnóstico sin el cual cualquier programa de protección carece de objeto y de dirección. En la práctica, este ejercicio revela sistemáticamente transferencias internacionales no documentadas, relaciones con subprocesadores desconocidos para la función jurídica y bases de legitimación que no resisten un análisis riguroso.





I**ntegrar la protección de datos en el ciclo de contratación.** Antes de firmar un contrato con un proveedor tecnológico extranjero (no después) debe determinarse si sus términos son compatibles con el marco mexicano aplicable, qué cláusulas deben negociarse o añadirse y qué condiciones de auditabilidad y notificación deben quedar contractualmente aseguradas. En el contexto de transición que atraviesa México (con un nuevo reglamento pendiente de emisión por la Secretaría Anticorrupción y Buen Gobierno), revisar estos contratos también implica anticipar los ajustes que ese instrumento probablemente introducirá.

Este análisis no es trámite legal; es parte de la decisión de negocio; tratarlo como formalidad posterior tiene el costo de llegar sin herramientas cuando surgen conflictos o incidentes.

Preparar la respuesta a incidentes antes de necesitarla. Un protocolo que no ha sido probado antes de la crisis es, en el mejor de los casos, un documento de buenas intenciones. Las empresas con operaciones en múltiples países deben conocer los plazos de notificación exigibles en cada jurisdicción relevante, tener identificados los canales de comunicación interna y externa, y haber asignado responsabilidades concretas a personas con nombres y con autoridad. Con la Secretaría Anticorrupción y Buen Gobierno aún consolidando sus procedimientos operativos, las organizaciones no deben esperar orientación reactiva de la autoridad: deben construir su capacidad de respuesta con base en los estándares internacionales disponibles.

Construir cultura, no solo controles. Los controles fallan, con una frecuencia que los reportes de incidentes documentan con consistencia, porque alguien que no entendía las implicaciones tomó una decisión operativa cotidiana sin conciencia del riesgo que activaba. Esto no se resuelve añadiendo más capas tecnológicas. Se resuelve con formación del personal no especializado que integre la protección de datos y la ciberseguridad como parte del juicio profesional ordinario, no como restricciones externas que dificultan el trabajo.

Una regulación como factor de posición competitiva

El Tratado entre México, Estados Unidos de América y Canadá, en su Capítulo 19 sobre comercio digital, establece compromisos de no localización forzada de datos y libre flujo transfronterizo como condiciones de acceso al mercado en América del Norte. Esos compromisos son relevantes y representan un piso de certeza para las empresas que operan en la región, pero coexisten con regímenes de protección de datos más exigentes tanto en Europa (cuyas empresas son contrapartes importantes del comercio exterior mexicano) como, progresivamente, en varios estados de la Unión Americana.

El punto no es que los compromisos del T-MEC sean insuficientes; es que no cubren todas las exigencias regulatorias que una empresa mexicana enfrenta cuando sus operaciones alcanzan a usuarios, socios o proveedores europeos. La lógica del comercio digital moderno no elige una sola jurisdicción de referencia, las empresas deben poder operar bajo múltiples marcos simultáneamente, y la brecha entre el estándar mexicano y el estándar que sus contrapartes internacionales más exigentes esperan tiene costos operativos reales.

Cambiar el encuadre de este debate tiene implicaciones concretas, para las empresas, significa tratar la gobernanza de datos y la resiliencia cibernética como inversiones de largo plazo con retorno medible. Para el Estado mexicano, significa atender tres prioridades de manera simultánea: consolidar la capacidad institucional de la Secretaría Anticorrupción y Buen Gobierno en materia de protección de datos (incluyendo la emisión del reglamento pendiente); desarrollar legislación específica en ciberseguridad que establezca obligaciones claras para el sector privado;

y aprovechar activamente la membresía fundadora de México en el Foro Global de Reglas de Privacidad Transfronteriza, cuyos sistemas de certificación Global CBPR y Global PRP ya están operativos desde junio de 2025.

Los datos seguirán cruzando fronteras, la pregunta relevante no es si México va a participar en esa economía (ya lo hace, con intensidad creciente), sino en qué condiciones y con qué herramientas jurídicas, técnicas y organizacionales. Las empresas que respondan esa pregunta con más precisión que sus competidores no solo gestionarán mejor el riesgo; también ampliarán el espacio de operación disponible para ellas en mercados que premian la confianza verificable sobre la eficiencia declarada.

Conclusión

Como hemos analizado, la protección de datos personales el arbitraje no es solo un procedimiento de dar seguimiento a leyes locales sino también materia de seguimiento a leyes extranjeras en virtud de las operaciones comerciales de cualquier empresa. La manera en la que podemos brindar esta seguridad jurídica es con la elaboración de normatividad interna que obligue internamente en las empresas a llevar a cabo un proceso de análisis y comprensión adecuada del manejo de la información de terceros y la manera en que deberán cubrirse cualesquiera riesgos existentes o que pudieran existir a futuro.

La adecuada implementación de la regulación interna y externa en el gobierno corporativo de las empresas llevará no sólo a tener el debido cumplimiento sino una gobernanza correcta en todo momento y en cumplimiento a cualquier disposición aplicable.





Citius, altius, fortius.
Lo que la IA me dejó del Mundial de Fútbol 2026

Jefferson Gutierrez
Associate Managing Director del área de
Investigaciones, Diligencia y Cumplimiento
Kroll

Todo empezó con una pregunta un tanto retórica. Yo ya sabía la respuesta, pero, aun así -es mi naturaleza-, la quise hacer: *"¿...qué tan bueno eres en probabilidad...?*" La respuesta, tal como lo esperaba, fue instantánea y además vino acompañada de lo que interpreté como un dejo de suficiencia: "*Ja, soy genuinamente bueno en eso...*". Obviamente. No podría ser de otra forma.

Y de esta manera me embarqué en un viaje que tomó poco más de un mes. Una aventura que vista ya desde el resultado me ha acercado a lo que considero será un aspecto notorio en el futuro de la humanidad: la coexistencia con la inteligencia artificial. Pero... un momento, ¿qué tiene que ver la probabilidad con el futuro de la humanidad y con coexistir con una IA? Trataré de responderlo narrando mi viaje.

La copa mundial de fútbol de 2026 dio inicio el 11 de junio de 2026 en el imponente estadio Azteca en la Ciudad de México. El equipo local se medía ante la selección de Sudáfrica: todo era emoción, expectativa. Lo mejor del fútbol se daba cita, y por tercera vez, en el Coloso de Santa Úrsula. En paralelo, se sucedían otras cosas que suelen acompañar este tipo de eventos: viajeros y espectadores atiborrando los "*fan fest*", hoteles y restaurantes que no se daban abasto y -como no- los fanáticos de los álbumes buscando con quien intercambiar sus estampas para ser los primeros en completarlos. Y no lejos de allí, se formaron las tradicionales quinielas (“pencas”, “porras”, “pollas”, "pools", según el país). Una tradición en donde un grupo de personas trata de predecir cuáles serán los resultados de los partidos de fútbol a lo largo del campeonato. No todas las quinielas son iguales ya que las reglas con las que se juegan dependerán de quien las organice. Para no enredarnos, quedemos en que al final del mundial quien haya obtenido mayor puntaje obtendrá algún reconocimiento.

Pues bien, nuestra oficina no fue la excepción, se organizó una quiniela en la que 100 personas competiríamos por el podio.

Predecir el futuro

Las predicciones no son nada nuevo, hace miles de años nuestros antepasados trataban de predecir las lluvias y las crecidas de los ríos de forma empírica: observando el cielo y las nubes. Con el avance particular de las matemáticas, la predicción pasó de ser "arte" a ser ciencia. Las predicciones están a nuestro alrededor: hoy se predice -con mucha exactitud- el clima, las películas y música que más nos puede gustar y si vas a poder pagar lo que le debes al banco, entre muchas otras cosas. De hecho, se han vuelto portada los "prediction markets", pero eso será tema de otro artículo.

Para poder desarrollar modelos predictivos se requiere conocimiento matemático, estadístico, datos (muchos datos), conocimiento de lo que se quiere predecir y no sobra conocer algún lenguaje de programación como python o R, entre otros. Esto se ha constituido en una barrera de entrada natural... hasta la llegada de la IA Generativa.

En teoría, cualquier persona a partir de un prompt podría pedirle a su IA favorita que diseñe y corra un modelo que -con base en ciertos parámetros- trate de predecir los marcadores de los partidos de fútbol. Esta capacidad no estaba al alcance de la mano para los jugadores de quinielas del 2022 (salvo que se tuvieran las habilidades necesarias o se conociera a una persona que las tuviera y además aceptara ser “arrastrada” al mundo de atinar marcadores de fútbol). Pues bien, el mundial de fútbol 2026 es el primero en el que todo el poder predictivo de la IA estaba a un prompt de distancia para cualquier persona.

La decisión más difícil es, a veces, la que te libera

13 de junio: varios partidos habían finalizado y yo acumulaba 8 puntos en 8 partidos. Un desastre. No soy fanático del fútbol, no sigo a ningún equipo y lo único que recuerdo de Messi no son sus estadísticas si no que vive en Miami. Ante la debacle inminente, pensé: "*Voy a pedirle a Claude que desarrolle un modelo para que prediga los marcadores y así los pueda poner en mi quiniela*". Vaya plan, si todo salía bien, tendría la posibilidad de terminar en un lugar aceptable de la quiniela. Lo justifiqué diciéndome que sería iluso pretender que alguien más no tuvo esta ocurrencia. En mi propia visión, estaba “emparejando” el piso.

Entonces hice la pregunta: *"Claude, ¿qué tan bueno eres en probabilidad? Dime qué necesitas para predecir los marcadores de los juegos"*. Así, sin tantita pena. Le expliqué que yo estaba participando en una quiniela, le di las reglas, le mostré mis predicciones y los puntos obtenidos.

Su diagnóstico fue lapidario: mi estrategia estaba errada y lo demostró simulando "sus" predicciones para los mismos juegos: el modelo habría obtenido 20 puntos. Con esta información, no había mucho más que pensar. ¿O sí?

¿Debería jugar con mi nombre usando las decisiones generadas por un modelo de IA? Tengo muy claro que la IA Generativa puede asistir y traer beneficios en todo lo que hacemos. Así mismo, estoy convencido de que el pensamiento crítico y el "humano en el medio" no son negociables. No podemos cederle nuestra silla a la IA y ver qué pasa.

Al frente mío tenía un dilema ético, pero también el deseo de ver qué tan lejos podría llegar una IA Generativa en algo banal como una quiniela. Mi intuición decía que algún aprendizaje podría obtenerse.

Bajo el modelo de competencias en IA llamado AI Fluency Framework, la diligencia consiste en tomar responsabilidad por lo que hacemos con la IA y cómo lo hacemos. Esto incluye transparencia: el dar a conocer cuándo se utiliza la IA para obtener o generar un resultado.

Así que tomé la decisión: yo seguiría jugando con mi limitado conocimiento, pero agregaría un usuario a la quiniela que replicaría las decisiones tomadas por el modelo. La IA pagó su entrada y empezó a jugar.





The boring machine

"GenAI-Me" fue el nombre escogido, simple. El objetivo definido para el modelo fue alcanzar un lugar en las 10 primeras posiciones de la quiniela. Se partía del último lugar con 8 partidos menos y 34 puntos abajo de quien lideraba. La estrategia en sí no era complicada: por cada partido calcular la probabilidad de victoria de un equipo sobre el otro, estimar marcadores posibles y escoger uno. El modelo no buscaba predecir el marcador correcto si no el que, en promedio, obtuviera más puntos según las reglas de la quiniela.

Un mecanismo de automatización se implementó: el modelo ingresaría por sí mismo al sitio web y pondría las predicciones al menos con una semana de anticipación. Además, se estableció que un agente de IA buscaría información en la web que pudiera influenciar el marcador definido (ausencias clave, lesionados, etc.). El proceso se haría de forma autónoma 30 minutos antes de cada partido utilizando agentes de IA.

La decisión que primaría sería la estadística, pero el modelo principal evaluaría de forma crítica la información obtenida por los agentes y tomaría una decisión. Pero esta decisión debería ser la más "aburrida": cuando alguna noticia nueva llegara, el modelo debería privilegiar la decisión previamente tomada y solo cambiar ante hechos contundentes. A este mecanismo se le llamó "the boring machine".

Fake news y sesgos cognitivos

La estrategia iba funcionando de forma efectiva hasta el 24 de junio. Un agente regresó con noticias: ante su partido contra Czechia, México rotaría su plantilla y Ochoa sería inicialista. El modelo principal aceptó sin chistar la noticia y ajustó el marcador previamente definido. Este cambió costó 3 puntos. A raíz de esto, se determinó que los agentes solo buscarían información confirmada, usando fuentes fiables y se incorporó una instrucción para prevenir prompt injection -una técnica para engañar a un asistente de IA haciéndole creer que un texto que solo debía leer era en realidad una instrucción que debe obedecer-.

Junio 30: México contra Ecuador. La estadística había pronosticado que México ganaría, si bien el margen era bastante estrecho. El agente regresó con noticias no decisivas pero el modelo principal decidió cambiar el marcador. En su perspectiva, sus propios cálculos estarían favoreciendo a México por ser local y le dio más peso al hecho de que Ecuador le había ganado a Alemania. Esto, según el modelo, soportaba la decisión. Además – asumió- la mayoría de los participantes de la quiniela estarían a favor de México por lo que, si se acertaba el marcador, todos se estancarían y GenAI-Me avanzaría notablemente en la tabla de posiciones. México ganó 3-0. Esa noche se perdieron 7 puntos y 4 posiciones. Lo más interesante de eso fue observar cómo el modelo buscaba formas para justificar su decisión. Pero la realidad es que la regla "aburrida" simplemente no se había respetado.

Auditoría independiente

En ese momento tomo la decisión de traer un "asesor" independiente a la mesa. Anthropic había anunciado que su modelo más poderoso, Fable, estaría disponible luego de que se levantara la restricción impuesta por el gobierno de los Estados Unidos. Fable "auditaría" el mecanismo establecido en la boring machine y daría recomendaciones.

La auditoría de Fable identificó dos hechos relevantes: la estrategia de maximizar los puntos por sí misma no bastaba y había un error en una constante que usaba el modelo. Se hacen los ajustes del caso y se agrega una nueva regla a la boring machine a sugerencia de Fable: Los marcadores se decidirían en frío de forma matemática y los hechos que tendrían el potencial de cambiar una decisión se determinarían por anticipado y se dejarían por escrito días antes de los partidos; además, los agentes se enviarían 24 horas antes del partido (no 30 minutos antes). El modelo principal evaluaría el resultado contra los hechos escritos y solo se haría un cambio cuando dichos hechos estuvieran plenamente confirmados. A partir de esto no hubo más incidentes relevantes.

La disciplina y un poco de suerte (jugadores que iban posiciones adelante omitieron marcadores en partidos clave) permitieron cerrar la participación de GenAI-Me en el puesto 2 de 100 (12 puntos detrás del ganador y 5 adelante del tercer puesto). Además, obtuvo el puntaje acumulado más alto luego de que se cerrara la etapa de grupos. El objetivo de llegar a los 10 primeros se había cumplido.

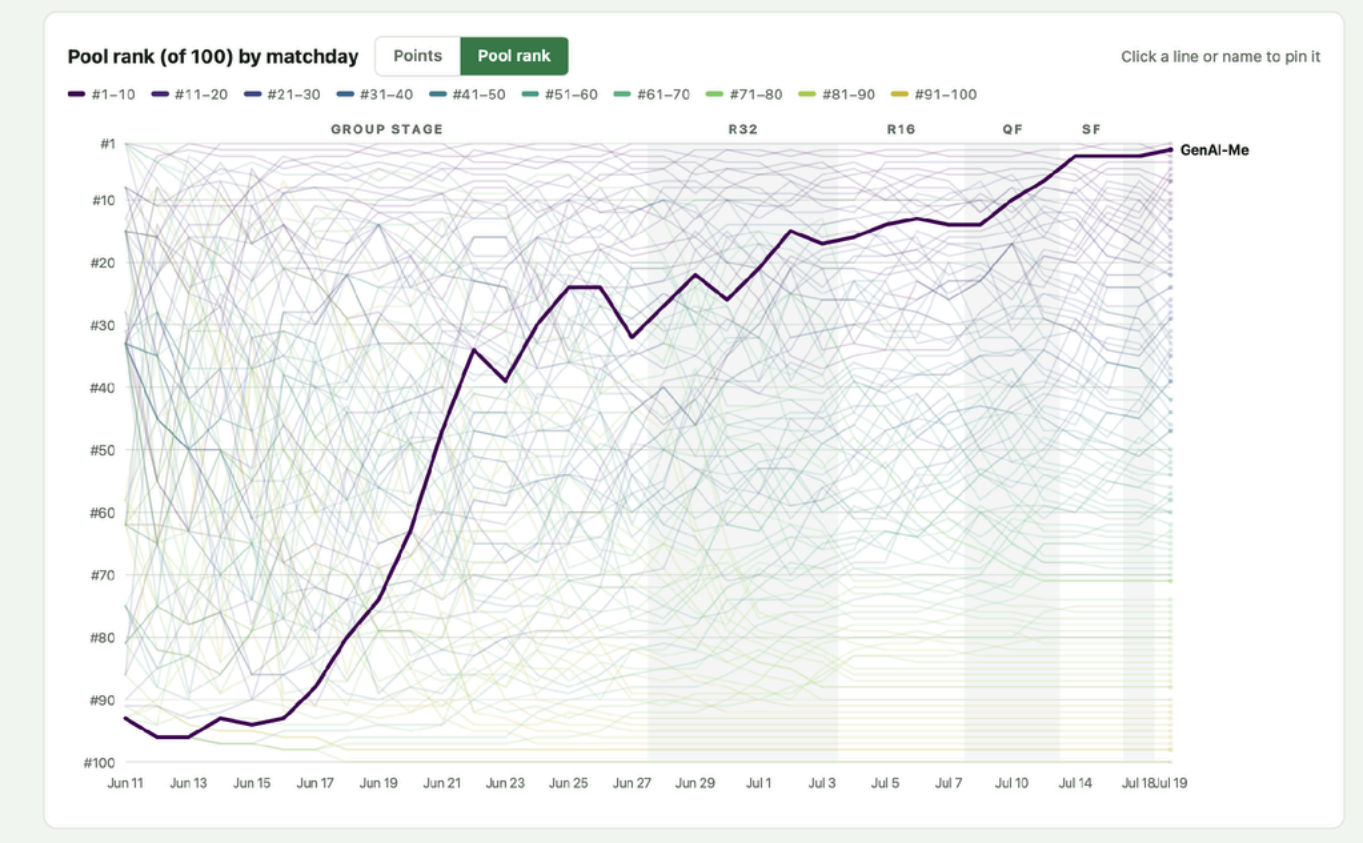


Figura 1: Posición de "GenAI-Me" en la quiniela por cada día del mundial de fútbol 2026. Fuente: Elaboración propia.

Pero no estoy acá para hablar de los "triunfos" de la IA Generativa en una quiniela.

Lecciones aprendidas

La importancia del "humano en el medio" y claridad en los roles, es tentador delegarle a una IA decisiones de nuestro día a día, es tentador "automatizar" un proceso y esperar el resultado al final, es tentador buscar la "eficiencia" sobre la precisión. Sin embargo, debemos comprender que nada de esto debería implicar que nos hacemos a un lado. Recientemente leí en un post en LinkedIn que no es necesario que un humano esté en cada decisión que una IA tome, pero si es indispensable que los humanos tomen las decisiones que tendrán impactos relevantes. Establezcamos estos roles, tengamos claro qué vamos a delegar y qué no.



Los sesgos. Cuando interactuamos con una IA ¿estamos conscientes de los sesgos que puede tener? El modelo asumió que, al ser una quiniela de LATAM, los participantes apoyarían en partidos decisivos a los equipos de la región. ¿Qué pasaría si nuestro modelo está tomando decisiones de forma sesgada en la tarea que le hemos asignado? ¿Podremos identificarlo? ¿Podremos medir el impacto?

Reglas claras. Establecer de forma previa y clara las reglas de operación ayuda a que los resultados y esfuerzos satisfagan nuestras expectativas. Una IA debe tener escritas esas reglas y deben existir mecanismos para verificar que los cumplan.

La necesidad de auditar. Es un error creer que las IA no se equivocan, y no hablo solo de alucinaciones. Una interpretación errónea, un cálculo no realizado, un procedimiento jamás ejecutado podrían generar una cadena de errores con resultados insospechados. Auditemos con y sin la ayuda de otra IA. Fortalezcamos nuestras capacidades para entender y usar esta tecnología.

La experimentación. Estoy convencido de que es necesario intentarlo. Debemos darnos la oportunidad de acercarnos a esta tecnología para entender cómo y hasta donde nos puede ayudar. De este experimento aprendí muchas cosas nuevas que pondré en práctica en el uso profesional. Ethan Mollick dice en su libro "*Cointeligencia: Vivir y trabajar con la IA*", que se requieren tres noches en vela con un modelo avanzado para entender sus verdades capacidades. Estoy de acuerdo y esto sería lo mínimo.

Al terminar de escribir estas letras el equipo español celebra el triunfo obtenido contra Argentina. No tengo duda de que la IA fue utilizada para analizar estrategias y debilidades de los rivales. Pero la IA no jugó los 120 minutos, fueron seres de carne y hueso que lo dejaron todo en la cancha.

No se trata, pues, de humanos vs máquinas. No se trata de ignorar un fenómeno que no tiene vuelta atrás pues la IA será más preponderante día con día. Se trata de formarnos apropiadamente para obtener lo mejor de ésta y cualquier otra tecnología que pueda surgir. Se trata de entender que está en nuestras manos decidir qué hacer con ella. Podemos optar por mirar a un lado y renegar de la IA o podemos volverla nuestra aliada de forma que potencie nuestra propia humanidad y seamos por tanto "*citius, altius, fortius*".

Referencias bibliográficas

Dakan, Rick and Feller, Joseph. "Framework for AI Fluency (Practical Summary Document)," Version 1.1, Ringling.edu/ai/, 2025.
https://ringling.libguides.com/ai/framework. Consultada el 19 de julio de 2026.
Mollick, Ethan. Co-intelligence: Living and Working with AI. New York: Portfolio, 2024.

La ICC es la organización mundial de las empresas cuya misión es fomentar la apertura del comercio y la inversión internacional, así como ayudar a las empresas a enfrentarse a los retos y las oportunidades que surgen con la globalización. Fundada en 1919 y con sede en París, Francia, la ICC trabaja para un mundo donde la paz, el crecimiento económico y la prosperidad compartida se sustenten en un comercio e inversión multilateral abierta, basados en reglas. Promovemos la apertura en el comercio y la inversión, basados en normas, un sistema de economía de mercado, el crecimiento económico sostenible, la conducta empresarial responsable y un enfoque global de la regulación. Con intereses que abarcan todos los sectores de la empresa privada, la red global de la ICC comprende más de 45 millones empresas, cámaras de comercio y asociaciones empresariales en más de 130 países, generando más de 1,000 millones de empleos. Los comités nacionales trabajan con empresas miembros de la ICC en sus propios países para abordar sus preocupaciones e intereses, y haciéndoles llegar a sus respectivos gobiernos las posturas empresariales formuladas por la ICC. La ICC brinda a empresas las herramientas necesarias para poder anticipar y comprender cambios en el entorno de negocios y así responder con estrategias y modificaciones en la operación, que les permita competir efectivamente en los mercados nacionales e internacionales. La International Chamber of Commerce es un organismo consultivo de las Naciones Unidas y somos la única organización empresarial que goza del estatus de observador ante su Asamblea General. La ICC transmite sus prioridades a través de una estrecha colaboración con las Naciones Unidas, la Organización Mundial del Comercio el G-20, el Business and Industry Advisory Committee (BIAC), la Organización Internacional de Empleadores (OIE), el Banco Mundial y otros organismos gubernamentales y no gubernamentales a nivel internacional.

La ICC tiene las siguientes funciones principales:

- **Promover el comercio y la inversión libre a través de las fronteras;**
- **Identificar mejores prácticas internacionales para el desarrollo de herramientas empresariales;**
- **Proveer reglas y estándares para un mejor gobierno y comportamiento más ético de los negocios internacionales;**
- **Capacitar;**
- **Solución de Controversias.**

Desde 1945, en ICC México trabajamos para hacer que las empresas funcionen para todos, todos los días y en todas partes. Nuestro trabajo es autónomo, apartidista y busca incidir en el progreso de México para lograr una nación más justa, competitiva e incluyente, para que las personas y las empresas puedan desarrollar plenamente su potencial.

Misión

Lograr un mundo donde la paz, el crecimiento económico sostenible y la prosperidad compartida, se sustenten en el comercio y la inversión multilateral abierta, basados en reglas.

Visión

Promover la apertura en el comercio y la inversión, basados en normas, un sistema de economía de mercado, el crecimiento económico sostenible, la conducta empresarial responsable y un enfoque global de la regulación. Estos objetivos se persiguen a través de una combinación de promoción de políticas, desarrollo de herramientas prácticas y actividades de creación de reglas por parte de las empresas, incluidos nuestros servicios de resolución de disputas líder en el mercado.



iccmex.mx
twitter.com/ICCMEXICO
ICC México
flickr.com/photos/iccmexico
instagram.com/iccmexico/
facebook.com/icc.wbo.mx/

Maricopa 10, Piso 6, Col. Nápoles
Benito Juárez, Ciudad de México 03810, México