La voz
del INADI Núm. 5

INADI
Instituto para el Desarrollo Industrial y la Transformación Digital A.C.

El *nearshoring* y una política industrial digital. La necesidad de una estrategia pública

Claudia Schatan | consejera del INADI | enero, 2024

Leer

Índice

I. Introducción

El objetivo de este capítulo es explorar qué políticas industriales digitales serían necesarias para que México se beneficie de las oportunidades que se le abren con la relocalización de las industrias a nivel global, especialmente el *nearshoring*, considerando que este fenómeno ocurre en un período de grandes cambios tecnológicos.

El proceso de *nearshoring* está trayendo actualmente a muchas empresas que se habían deslocalizado desde centros industriales hacia terceros países –*offshoring*– a partir de los años ochenta, ahora a localidades más cercanas a sus mercados finales, o a otras empresas que participan en la cadena de valor. Este fenómeno busca un acortamiento de dichas cadenas globales de valor (CGV), léxico nada nuevo en los temas de la economía internacional (Gereffi, Humphrey y Sturgeon, 2006; Gereffi, 2013; Humphrey, 2019). Así, después de haberse dispersado por todo el mundo, los procesos productivos tienden a reconcentrarse reduciendo geográficamente la distancia entre sus distintos eslabones.

Las ventajas de bajos costos, especialmente de la mano de obra, en los países en desarrollo ya han dejado de ser tan grandes para las empresas globales como lo fueron hace casi medio siglo, mientras que el salto tecnológico que han dado los procesos de fabricación requieren unas capacidades mucho más sofisticadas que antes para producir, la cual no está disponible en todos los países receptores de esa industria deslocalizada. Ello, aunado a las complicaciones del transporte de las mercancías, el alza en aranceles y aumento en los obstáculos al comercio por motivos geopolíticos, además de la disrupción de las cadenas de valor a raíz de la pandemia, ha llevado al mundo a una reconfiguración de la estrategia productiva a nivel internacional, es decir *re-shoring* (cuando la cadena completa vuelve al país de origen), o *nearshoring* (cuando se instalan más cerca del origen).

El *nearshoring*, que nos ocupa en este capítulo, está ocurriendo en el marco de la Cuarta Revolución Industrial (o industria 4.0) que, además, se sustenta en una revolución digital, que involucra una tecnología tan avanzada como la inteligencia artificial (IA), la robótica, el internet de las cosas (IoT, por sus siglas en inglés), impresión 3D, vehículos autónomos, entre otros. La posibilidad de desarrollar esta industria de frontera depende, a su vez, del avance digital, que aunque se inició en los años 50s, ha cambiado radicalmente. La industria 4.0 necesita de una digitalización y conectividad creciente, lo que involucra la generación y procesamiento de macrodatos (Big Data), una creciente vinculación entre humanos y máquinas (IoT), y para cuya transmisión son necesarias redes celulares cada vez más rápidas y de menor latencia, como las redes 5G. De hecho, el potencial de la actual revolución tecnológica aumenta notoriamente con estas últimas redes en comparación con las 2G, 3G y 4G.

En este trabajo exploraremos las implicaciones que tiene el *nearshoring* en México, considerando que las inversiones que recibe el país en este proceso se centran especialmente en industrias tecnológicamente avanzadas, predominando la Industria 4.0 (automotriz, electrónica, aeroespacial, implementos médicos, etc.) y para que éstas operen eficientemente, la digitalización es esencial. Esta también lo es para el acelerado incremento del flujo de información entre México y sus contrapartes productivas y comerciales que, además, se enfrenta al reto de poder transmitir información a través de fronteras en forma segura (se necesita ciberseguridad). Los diferentes eslabones de la cadena de valor se conectan entre sí cada vez más por en forma virtual y se requiere una política industrial digital que facilite la operación dentro de las propias empresas, entre las empresas reunidas en clusters nacionales y entre las empresas que operan en forma transfronteriza, especialmente entre México y Estados Unidos, y de manera segura.

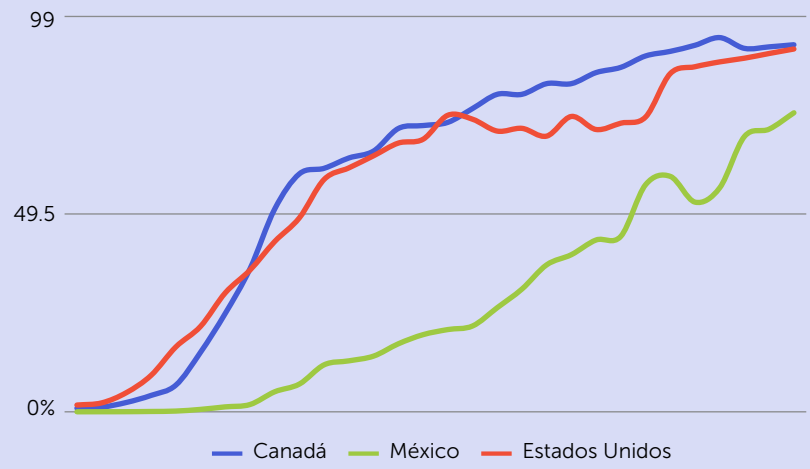
Según un estudio reciente (CEPAL, 2022), en marzo de 2022 la industria digital[1] en el mundo había superado los 25 billones de dólares, es decir, más de la cuarta parte de la economía mundial (27%). Al mismo tiempo, esta industria digital ha experimentado una gran dinámica en su crecimiento: 330% entre 2010 y 2022, tasa cuatro veces mayor que la de las industrias tradicionales, medido en valor de mercado de sus empresas. Este proceso es más lento en América Latina y el Cartibe (ALC), pero de todas formas la penetración de Internet, por ejemplo, avanzaba a un alto ritmo, alcanzando el 66% de la población en 2022, de acuerdo a la misma fuente.

1 Cepal, en el documento citado define a la industria digital como el conjunto de *hardware, software,* Plataformas de Servicios de Internet, Plataformas de comercio electrónico y Telecomunicaciones.

II. El Estado de la digitalización en México

La digitalización ha tenido, sin duda, un avance significativo en México a lo largo de las últimas dos décadas, especialmente si se observa cómo se ha ampliado el acceso de la población a Internet, que alcanzó en 2021 a 75.6% de ella. Este porcentaje, no obstante, seguía siendo bastante menor al logrado por sus contrapartes del T-MEC, Estados Unidos y Canadá, que en aquel año abarcaban algo más del 90% de sus poblaciones con este servicio (Véase Gráfica 1).

GRÁFICA 1. Porcentaje de la población con acceso a Internet, 1992-2021



FUENTE: Banco Mundial, [en línea] https://datos.bancomundial.org/indicador/IT.NET.USER.ZS?end=2021&locations=US-MX-CA&start=1990&view=chart

El acceso promedio de la población en México no revela las grandes diferencias que hay en la disponibilidad de este servicio en el país en la práctica. Ello varía mucho según el ingreso de las personas, de su edad, su ubicación geográfica y su nivel de educación, generando significativas brechas de conectividad al interior del país. En 2021, sólo el 34% de la población de un estrato socioeconómico bajo tenía acceso a Internet, mientras el 92.1% de la población de estrato socioeconómico alto lo tenía (INEGI, 2023). Asimismo, el 81.6% de la población urbana contaba con servicio de Internet en 2022, mientras esa cifra era del 56.5% en las zonas rurales (Evaluare[2]). Las diferencias por grupo etareo también son significativas: en 2021, la mitad de las personas que no usaban Internet superaban los 55 años (Evaluare[3]).

2 Evaluare, https://www.evaluare.mx/2023/01/28/brecha-digital-politicas-publicas-y-acceso-a-internet-en-mexico-como-vamos/ (consultado el 29/05/2023).
3 *Ibidem.*

CUADRO 1. Velocidad Internet Móvil, Internet Fijo y Latencia

ABRIL 2023

	VELOCIDAD INTERNET MÓVIL *			VELOCIDAD INTERNET FIJO*		
	MBPS	LATENCIA	RANKING	MBPS	LATENCIA	RANKING
China	110.1	27	9	215.8	13	4
Canadá	92.63	23	14	146.07	11	16
Estados Unidos	80.38	31	21	202.4	13	7
Brasil	41.04	27	53	106.7	6	32
México	26.13	37	82	50.58	8	87
Perú	18.03	26	113	79,9	10	54

FUENTE: Speedtest, https://www.speedtest.net/global-index (actualizar datos)

MBPS: megabites por Segundo. * Velocidad para bajar información.

Tampoco ayuda a su uso el alto costo de acceso al servicio de internet en México. El país estaba en el lugar 164 en términos de precio por gigabyte (GB) a través de internet móvil entre 233 países en 2022, con 2.89 dólares por GB. Eso lo comparaba desfavorablemente incluso con gran parte de los países de América Latina, ocupando Chile el lugar 32, con un costo de 0.51 dólares por GB, o Brasil que tenía el lugar 54 con un costo de 0.74 dólares por GB, entre otros de la región. No ocurre lo mismo con las contrapartes de México en el T-MEC, pues Canadá y Estados Unidos tienen costos de casi el doble que México por cada GB.[4] [5]

Los altos costos mencionados en México de deben al menos a dos motivos: el elevado precio del expectro radioeléctrico que cobra el gobierno a las empresas de telecomunicaciones así como una gran concentración del mercado de TIC junto con una política de competencia débil para este sector. En 2022, América Móvil tenía el 59.6% de mercado móvil y concentraba el 70% de los ingresos totales del sector.[6] Así, el mercado de telecomunicaciones en México dista mucho de ser un mercado competitivo pues tiene "agentes con poder sustancial de mercado" (potencialmente monopólicos) que requieren de una institución autónoma, como es el Instituto Federal de Telecomunicaciones (IFT), que pueda aplicar regulación asimétrica a los

4 Worldwide mobile data pricing 2022, https://www.cable.co.uk/mobiles/worldwide-data-pricing/

5 En Estados Unidos hay un problema de falta de competencia en los mercados pues tres de cada cinco familias viven en áreas donde cuentan solo con uno o dos proveedores de servicios de Internet (CTN, https://communitytechnetwork.org/blog/why-is-the-internet-more-expensive-in-the-usa-than-in-other-countries/#:~:text=One%20possible%20answer%20is%20the,Americans%20have%20only%20one%20choice), y los altos costos en Canadá tiene similares orígenes (CanNet, https://www.cannettel.com/blog/why-internet-expensive-canada#:~:text=There%20is%20no%20"cheap"%20internet,due%20to%20lack%20of%20competition).

6 Expansión (2023), IFT inicia consulta sobre medidas para reducir preponderancia de América Móvil, https://expansion.mx/empresas/2023/01/04/ift-inicia-consulta-sobre-medidas-para-reducir-preponderancia-de-america-movil, 4 de enero.

distintos actores en dicho sector para que puedan actuar con "piso parejo" entre ellos. Pero no han logrado que el grupo de empresas de América Móvil (que incluye a Telmex, Telcel y Claro Video) dejen de tener prácticas monopólicas y otras empresas como AT&T (más Telefónica, ahora), Megacable, y American Tower no pueden competir en un mercado adecuado porque las primeras no responden a la regulación del IFT (por ejemplo, que el incumbente comparta su infraestructura con las demás empresas más pequeñas, o que las empresas paguen tarifas de conexión diferenciadas, entre otras, de manera que todas puedan hacer nuevas inversiones y crecer).[7] Las medidas aplicadas por IFT deberían ir reduciendo el peso del incumbente en el mercado, pero ello sólo ha ocurrido en forma muy marginal, porque esta institución no tiene la suficiente fortaleza para realizar su labor plenamente.

Más allá de la disponibilidad de conexión a Internet y su costo, está su calidad que, de ser deficiente, impide usar plenamente este servicio. Sin embargo, como se puede observar en el Cuadro 1, México se encontraba lejos de sus contrapartes del Tratado entre México, Estados Unidos y Canadá (T-MEC) en materia de velocidad de internet móvil y fijo, así como de muchos otros países. De hecho, México ocupaba el lugar 81, entre 138 países en 2023, respecto a la velocidad de descarga de internet móvil, que es el más usado en el país. México presenta un gran atraso en este indicador respecto de China, lo que es preocupante si se trata de atraer inversiones que provienen de ese país y que están acostumbrados a contar con una conectividad digital mucho más eficiente que la mexicana.

Es evidente que se necesita fortalecer la infraestructura de TIC en México que, por ahora, presenta diversas limitaciones. Las inversiones que hace México son insuficientes para que se cierre la brecha que tiene con otros países en esta materia: la inversión en telecomunicaciones era de 40 dólares per cápita en 2019, mientras que llegaba a 140 dólares per cápita en ese mismo año, en promedio, en los países de la OCDE. Al mismo tiempo, como se muestra en un libro reciente (Oropeza y Belausarán, 2021) la inversión empresarial en tecnologías de la información en México se destinan en su gran mayoría a los componentes más tradicionales (87%) mientras sólo el 13% de ella va a los segmentos aceleradores de las TI, como son la AI, el IoT, cómputo en la nube, Big Data, entre otros, que impulsan inversiones adicionales en los sectores en las que se incorporan. Ello contrasta con lo que ocurre en países como Corea del Sur, que dedica 58% de esta inversión a los segmentos aceleradores o Estado Unidos que dedica el 37% de su inversión en TI a este sector.

7 Las sanciones impuestas por el IFT son muy pequeñas como para desincentivar una serie de prácticas anticompetitivas contrarias a la Ley Federal de Telecomunicaciones y radiodifusión (CIU, Mecanismos para una Regulación Efectiva (https://www.theciu.com/publicaciones-2/2022/10/5/mecanismos-efectivos-para-una-regulacin-efectiva).

En forma más específica, la evolución del espectro radioeléctrico no se ha desarrollado de acuerdo a lo sugerido por la Unión Internacional de Telecomunicaciones (UIT). Esta entidad aconsejaba que México tuviera 1720 MHz desplegados en 2020, pero en ese momento el país contaba con sólo 700 MHz, es decir, el 40% de lo sugerido por la UIT. Pero, para 2022, en lugar de haberse expandido este expectro, se había contraido (a 660 MHz) debido a la renuncia a concesiones de segmentos de las bandas 850 MHz y PCS justamente por sus altos costos, por parte de Pegaso PCS, S.A. de C.V. (Telefónica Movistar).[8] De acuerdo a los planes del gobierno (y si no hay devoluciones adicionales de espectro), en el mediano-largo plazo se podrían alcanzar 1170 MHz (es decir, 68% de lo recomendado por la UIT para 2020) (IFT, 2022).

Por otra parte, si se consideran los 15,750 MHz de espectro radioeléctrico en bandas milimétricas[9] identificados en la Conferencia Mundial de Radiocomunicaciones Nº 19 de la UIT, que podrían estar disponibles en México en el largo plazo, probablemente se podrían alcanzar los mencionados 1720 MHz (IFT, 2022).

Es de notar, asimismo, que México ha ideado una importante iniciativa de Red Compartida, en una asociación público-privada (APP) con Altan Redes para hacer un mejor uso de la infraestructura de redes que ya existe en el país, ahorrando inversiones nuevas por el lado del sector público, atrayendo inversiones privadas para incrementar el potencial de conexiones y volviendo más competitivo el mercado de telecomunicaciones.[10] La Red Compartida es una red mayorista que tiene el propósito de brindar cobertura nacional de internet con tecnología 4G (incluso 4G LTE, y eventualmente 5G) en México lo que contribuirá a reducir la brecha digital, sobre todo en las comunidades más marginadas del territorio nacional, mejorar la calidad del servicio de conectividad, y reducir costos. Para ello el gobierno dedicó 90 MHz de la banda de frecuencias de 700 MHz del espectro radioeléctrico y en enero de 2017 se firmó un convenio de Red Compartida entre Promotora de Inversiones en Telecomunicaciones (Promtel)[11], Telecomunicaciones de México (TELECOMM) y Altán Redes (empresa privada que ganó la licitación). La Red Compartida mayorista cubriría el 92.2 por ciento de la población en enero de 2028. Es decir, varios años depués del compromiso que se había asumido originalmente (fue revisado el convenio en dos ocasiones, cuando Altan Redes, enfrentando diversas dificultados financieras, solicitó la poster-

8 Renuncias hechas efectivas en diciembre de 2021 y junio de 2022, según IFT, https://www.ift.org.mx/sites/default/files/espectro_imt_en_mexico_2022_0.pdf.
9 Especialmente útil cuando hay una gran concentración de usuarios que quieren acceder de forma simultánea al Internet. También ayuda a empresas en las que es necesario un acceso a Internet estable, con baja latencia.
10 Para una visión más detallada sobre la Red Compartida, sus caractéristicas y funciones, véase Oropeza y Berazaluce (2021).
11 PROMTEL, Organismo (público) Promotor de Inversiones en Telecomunicaciones

gación de los tiempos de cumplimiento). Con todo, Altán Redes en 2021 fue el quinto inversionista del sector de las telecomunicaciones en el país. Una evaluación del desempeño del acuerdo de Redes Compartidas realizado a principios de 2023[12] muestra un avance significativo en varios indicadores.

México carece, por otra parte, de suficientes interconexiones de redes troncales y puntos de intercambio de tráfico de internet (IXP, por sus siglas en inglés). Estos son nodos de interconexión que facilitan el intercambio de tráfico entre distintos proveedores de servicios de internet, lo cual garantiza la eficiencia en las comunicaciones. En México, sin embargo, sólo había dos IXP (Ciudad de México y Mérida) en 2022, en contraste con los 34 con los que contaba Brasil en ese año[13], ésto debido a que los proveedores de servicio de Internet (ISP, por sus siglas en inglés) del primer país prefieren realizar las interconexiones en su vecino país, Estados Unidos, para la transmisión de información por internet, con lo cual aún los intercambios nacionales tienen que pasar por allí para llegar a su destino en el propio país, haciendo este servicio más caro e ineficiente.

La infraestructura necesaria para contar con las redes 5G, por su parte, es esencial para el funcionamiento de la Industria 4.0, pues hace posible una mayor velocidad de red, menor latencia[14] y soporte para más usuarios que las redes previas. Estas redes hacen posible el uso del IoT, el Big Data y la Inteligencia Artificial (IA) dentro de las empresas y a lo largo de las cadenas de valor. Así, las empresas pueden corregir errores, prever y solucionar problemas con anticipación, agilizar la cadena de suministro, optimizar sus inventarios, mejorar la calidad de sus productos y de servicios acorde con la información recabada de los consumidores finales, etc. Esta industria inteligente, que es la que frecuentemente encontramos en las actividades de la industria exportadora en México y la que tenderá a ser más dinámica con el *nearshoring*, necesita redes más potentes que 4G o que el Wi-Fi, estas últimas comparativamente más inestables y con un radio más reducido de operación (Schatan, 2023).

Sin embargo, las redes 5G han avanzado lentamente en México, incluso comparado a otros países latinoamericanos, entre los que ocupaba el octavo lugar en despliegue de ellas a mediados de 2022. Sólo dos empresas –AT&T y Telcel– han puesto a disposición del público redes 5G (desde 2021 y 2022, respectivamente). Para una introducción adecuada de redes 5G, el regulador –Instituto Federal de Telecomunicaciones (IFT)– necesita subastar más espectro 5G, lo que está planeando hacer en 2023, es decir, más de

12 Secretaría de Infraestructura, Comunicaciones, y Transporte y PROMTEL (2023), *Evaluación de la Red Compartida,* https://www.promtel.gob.mx/perfiles/wp-content/uploads/2023/03/Evaluacion-Red-Compartida-2022-vp.pdf
13 Packet Clearing House (2023), Internet Exchange Point Growth by Country. https://www.pch.net/ixp/summary_growth_by_country
14 Latencia es el lapso de tiempo entre la solicitud de información a internet y su respuesta, que puede reducirse a un milisegundo.

330 MHz (IFT, 2023), pero ello seguirá siendo insuficiente. Aún más, incluso el éxito de esta licitación no está asegurado debido al alto precio al que se suele ofrecer el espectro en el mercado (como ocurrió con la licitación IFT-10 en 2021, que no tuvo los resultados esperados). Así, esto lleva a que las redes 5G no funcionen óptimamente porque a falta de expectro adecuado, se usan bandas de 3.4 GHz y 2.5 GHz ya existentes sobre las que se desplegaban redes 4G, pero que no alcanzan el ancho de banda que se necesita para que las redes 5G tengan un desempeño ideal.[15]

El desarrollo tecnológico actual exige un avance en la conectividad y en el desarrollo de la infraestructura en TIC en México mayor a lo que se ha logrado hasta ahora. Aún más, el *nearshoring*, el T-MEC y otros compromisos que insertan a México en la economía regional y global son acuerdos adicionales que necesitan del impulso de la digitalización en el país para aprovechar las oportunidades que tiene por delante.

15 Bnamericas, *Redes 5G en Latinoamérica: su estado actual y lo que viene;* https://www.bnamericas.com/es/reportajes/red

III. *Nearshoring*, acuerdos internacionales regionales, globales y la digitalización

El comercio digital, la producción inteligente, y todas las formas de comunicación virtual avanzan a una gran velocidad y requieren un gran esfuerzo por parte de México para responder a estos retos.

Dentro de las cadenas de valor la digitalización puede conectar a proveedores, con fabricantes, con la esfera del comercio y con los consumidores. Asimismo, se puede mejorar notoriamente la logística, al cobrar la visibilidad y la trazabilidad de toda la cadena de suministro y atender en forma casi inmediata los problemas que surgen en ésta (el IoT puede indicar el tamaño de los inventarios, puede reorientar los envíos, y detectar el mal funcionamiento de equipos). Todo ello lleva a un mucho más eficiente ciclo del producto: diseño, producción y distribución de bienes y servicios. Para que esto ocurra no sólo se necesita contar con la tecnología y la infraestructura apropiada, sino la facilidad de transmisión de información y la seguridad en este proceso.

La necesidad de interoperabilidad entre empresas que se ubican en diferentes países, como es el caso de las empresas que se instalan en México (*nearshoring*) para tener una relación cercana a sus contrapartes productivas o comerciales, especialmente con Estados Unidos, es cada vez mayor. Este acelerado proceso de intercambio transfronterizo de información da lugar a la necesidad de ciberseguridad, incluyendo la protección de datos, para poder efectuar en forma segura todo tipo de transacciones. Muchos países buscan alcanzar el Libre Flujo de Datos con Confianza (*Data Free Flow with Trust, DFFT*) para responder a la necesidad creciente del paso de datos entre ellos. Un estudio del Ministerio de Economía, Comercio e Industria de Japón[16] identificó una serie de actividades productivas que requieren el flujo de información a través de fronteras, entre las cuales están: la comunicación con proveedores y desarrolladores de aplicaciones en línea; intercambio de información con una empresa subcontratada; la colección de información proveniente del exterior en tiempo real gracias al IoT; acceso a plataformas de servicios y al internet como un servicio; servicios de ciberseguridad, entre otros.

Sin embargo, no se ha logrado tener políticas transfronterizas comunes sobre el tema de DFFT internacionalmente. Ha habido esfuerzos unilaterales por parte de algunos países por tener su reglamentación sobre seguridad de datos de manera de dar confianza a terceros países que les canalizan información. También ha habido, e incluso están en marcha, esfuerzos intergubernamentales deliberados para crear ese ambiente de seguridad para el flujo de datos entre distintas naciones, como es el caso, por ejemplo de las

16 Citado por el World Economic Forum (2023)

discusiones llevadas a cabo dentro del grupo G7 (que cuenta ya con un Plan de Acción para promover el DFFT) o en el Grupo G20 (que buscan puntos de convergencia en este tema). También se discute a nivel de organizaciones multilaterales, como la OMC, el Banco Mundial, OCDE y Naciones Unidas, o se buscan arreglos regionales como los de APEC y el T-MEC.

México, por su parte, ya ha asumido compromisos internacionales que le demandan contar con una capacidad en TIC y digitalización, y la transferencia segura de datos con disponibilidad de ciberseguridad incluyendo la protección de datos personales, a los que tiene que responder forzosamente.

En primer lugar, el T-MEC tiene un importante capítulo sobre comercio digital (Capítulo 19[17]) que compromete a los tres socios comerciales de América del Norte a impulsar y proteger el comercio digital, así como a estimular el comercio de productos enteramente digitales: música, juegos, videos, películas, libros electrónicos, entre otros. Esto último se implementa mediante la prohibición de aranceles al comercio de dichos productos. El acuerdo también facilita los negocios transfronterizos entre empresas mediante la autenticación electrónica y las firmas electrónicas, lo que favorece no sólo al comercio virtual, sino también a la operación entre empresas productivas de todo tipo a uno y a otro lado de la frontera.

Asimismo, el Capítulo 19 del T-MEC promueve el mayor flujo de información transfronterizo, por ejemplo, al permitir el libre acceso a la información pública generada por los gobiernos, pero al mismo tiempo requiere la protección de la información personal de los usuarios del comercio digital (para lo que los países deben disponer del marco legal y regulatorio necesario). Con este fin, las Partes del T-MEC deben endosar los "principios y directrices de los organismos internacionales pertinentes, tales como el *Marco de Privacidad de APEC* y la *Recomendación del Consejo de la OCDE relativa a las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales (2013)*." Es decir, deben cumplir con los mejores estándares internacionales de protección de datos, de manera que las transferencias transfronterizas de información se hagan en forma segura.

De hecho, le seguridad es uno de los aspectos centrales de este capítulo 19: "*Las Partes reconocen que las amenazas a la ciberseguridad menoscaban la confianza en el comercio digital. Por consiguiente, las Partes procurarán: I. Desarrollar las capacidades de sus respectivas entidades nacionales responsables de la respuesta a incidentes de ciberseguridad; y II. Fortalecer los mecanismos de colaboración existentes para cooperar en identificar y mitigar las intrusiones maliciosas…*"[18]

17 Capítulo 19, T-MEC, https://www.gob.mx/cms/uploads/attachment/file/465801/19ESPComercioDigital.pdf
18 *Ibidem.*

Nótese que además de los compromisos asumidos por México en Capítulo 19 del T-MEC ya descritos, el país también se adhirió anteriormente al Sistema de Reglas de Privacidad Transfronterizo (CBPR, por sus siglas en inglés) del Foro de Cooperación Económica Asia-Pacífico (APEC) en 2013 (ProtDataMex, 2013). Según este acuerdo, *"sus políticas de privacidad y prácticas serán obligatorias para la entidad participante y serán ejecutables por la autoridad reguladora correspondiente del país en el que se encuentra"* (que en el caso de México es el actual Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI) (ProtDataMex, 2013).

En la medida en que haya diferentes niveles de seguridad entre países para la transmisión de datos y solidez dispar entre sus legislaciones de ciberseguridad, ello dificulta el emprender conjuntamente procesos productivos y comerciales interconectados. Un ejemplo es el caso del "Privacy Shield" (Escudo de Privacidad) suscrito por Estados Unidos con la Unión Europea en 2016 que brindaba la protección necesaria, en principio, para que pudiera transferirse información digital sin obstáculos entre empresas establecidas en estas dos regiones (más de 5,300 empresas hicieron uso de ese acuerdo para operar sin problemas), pero el acuerdo se rompió en 2020, justamente porque la UE consideró que Estados Unidos no contaba con suficientes medidas de protección de datos personales (Véase Recuadro 1).

RECUADRO 1. Acuerdo "Privacy Shield" (Escudo de Privacidad)

La UE y Estados Unidos firmaron en 2016 el Acuerdo "Privacy Shield"* (Escudo de Privacidad) para salvaguardar y facilitar el intenso flujo digital de datos entre sí. En 2020 este acuerdo favorecía a más de 5,300 empresas que habían suscrito este compromiso** pero fue anulado en 2020 por la Corte de Justicia Europea por no resguardar adecuadamente los derechos de privacidad de la información dispuestos por la UE. Esta cancelación ocurrió por el hecho de que Estados Unidos tiene medidas más laxas de protección de datos que las de la UE. La supresión del mencionado compromiso ha obstaculizado la operación de muchas empresas ya que actualmente éstas tienen que conseguir individualmente los permisos para la transmisión de información digital. Hay expectativas de que en 2023 se pueda firmar un "Privacy Shield 2.0" para transferir datos personales de acuerdo a las exigencias de la UE. Fue con este propósito que el Pdte. Joe Biden firmó una Orden Ejecutiva*** para responder a las exigencias de los europeos. En la práctica, esta última disposición impide el acceso de las autoridades de Estados Unidos a los datos personales exportados desde la UE a ese país, que era lo que más objetaba ese grupo de países.

* EUR-LEX (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG
** Congressional Research Service (2022), https://sgp.fas.org/crs/row/IF11613.pdf
*** La Casa Blanca (2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/

Una política industrial que tenga el propósito de promover el *nearshoring* y aprovechar las oportunidades que éste brinda, necesariamente tiene que tomar en consideración no sólo la infraestructura para que las empresas puedan estar conectadas nacional e internacionalmente y cuenten con la mejor tecnología de telecomunicaciones que exige la Industria 4.0, sino, además necesita garantizar que sea factible un gran flujo transfronterizo de información digital de manera segura para personas y empresas. El que México esté cada vez más distante en términos de los estándares de protección de datos personales y ciberseguridad respecto a sus contrapartes, especialmente de Estados Unidos y de Canadá con los que conforma un bloque integrado de comercio y cada vez más de producción (dados el T-MEC y el *nearshoring*, las tensiones geopolíticas entre Estados Unidos y China, v entre otros), puede conducirle a desalentar las inversiones en México (tanto las nacionales como las internacionales). Cuando hablamos de una política industrial para México, como ya hemos visto, necesitamos pensar en un concepto más amplio que el tradicional, es decir, necesitamos considerar una política industrial digital que se aplique a toda la cadena de valor. A la vez, esto tiene que ir acompañado de todas las medidas legales y regulatorias que permitan llevar a cabo esta nueva industrialización en un ambiente digital seguro, de lo contrario, no se darán las condiciones para avanzar hacia un desarrollo productivo moderno, en el que participen los diversos actores interesados.

IV. Ciberseguridad en México[19]

México está entre los países que reciben la mayor cantidad de ataques cibernéticos en el mundo. En 2022 sufrió 187,000 millones de intentos de ciberataques, es decir, un crecimiento de 20% respecto de 2021 y fue el más atacado dentro de América Latina.[20]

El término de ciberseguridad, en realidad, abarca una amplia gama de aspectos relativos a la digitalización: desde la seguridad de red, que la protege de intrusos que quieran extraer sin autorización información o bien quieran atacar de diversas formas a usuarios (*malware*); la seguridad de las aplicaciones, que protege de amenazas al software y dispositivos; la seguridad de la información, que protege la privacidad de los datos tanto en su proceso de transmisión como durante su almacenamiento; la seguridad operativa, cuando se maneja la información, es decir, la forma de acceder a ella (se pueden requerir permisos) y la manera de compartirla.[21]

El desempeño de México en ciberseguridad no ha ido en la dirección deseada ni en la que se ha comprometido. En 2019 este país ocupaba el lugar 66 en el índice de ciberseguridad mundial, mientras a Estados Unidos le correspondía el lugar 35 y a Canadá el 25 entre 166 países. La situación había empeorado para 2023, teniendo México el lugar 90, Estados Unidos el lugar 44 y Canadá el 33, entre 176 países de acuerdo con el Índice de Ciberseguridad Nacional (NCSI, por sus siglas en inglés) (Véase Cuadro 2).[22]

Para asegurar la ciberseguridad en Norteamérica tendría que haber una armonización de normas y leyes relativo a este tema especialmente entre México, Estados Unidos y Canadá.

No existe una ley federal de ciberseguridad en México (aunque hay algunas iniciativas de ley en el Congreso) y los instrumentos legales con que cuenta el país contra los ciberataques están dispersos y son incompletos. Estos están básicamente contenidos en El Código Penal Federal, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y las regulaciones de la Banca e instituciones de crédito.

El Código Penal Federal se encarga de actuar frente a varias transgresiones cibernéticas, como: *piratería*; *phishing* (fraude realizado a través del engaño y manipulación de una persona); *infección de sistemas informáticos con malware* (incluidos ransomware, spyware, gusanos, troyanos y virus), el cual no está tipificado como delito en sí pero puede considerarse una forma

19 Una parte de esta sección se basa en Schatan (2022).
20 IT Master Mag (2023), ¿Cómo está la ciberseguridad en México?, https://www.itmastersmag.com/noticias-analisis/como-esta-la-ciberseguridad-en-mexico/#:~:text=México%20es%20uno%20de%20los,de%2020%25%20frente%20a%202021.
21 Kapersky, ¿Qué es la Ciberseguridad?, https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security
22 National Cybersecurity Index (NCI), https://ncsi.ega.ee/ncsi-index/

de piratería. Lo mismo es cierto de la *posesión o uso de hardware, software u otras herramientas utilizadas para cometer delitos cibernéticos* (que puede ser perseguido como delito de piratería); o bien del *robo de identidad, fraude de identidad* (que se rige por lo establecido por la Ley de Instituciones de Crédito); y *robo electrónico* (similar al anterior) (Schatan, 2023).

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares "exige a los controladores de datos la implementación de medidas de seguridad administrativas, físicas y técnicas para proteger los datos personales contra pérdida, robo o uso no autorizado y deben informar a los interesados de cualquier violación de seguridad"[23], pero la capacidad de aplicar esta ley por parte de la institución encargada de ello, es decir, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), es limitada ya que algunas de sus recomendaciones no son vinculantes, como el dar aviso de un ataque cibernético por parte de quien lo ha sufrido.

En México no se ha concretado una Estrategia Nacional de Ciberseguridad por parte del gobierno.[24] Tampoco existe una entidad encargada exclusivamente de la ciberseguridad, como la tiene Estados Unidos con el U.S. Cybersecurity and Infrastructure Security Agency (CISA). Incluso, los recortes de presupuesto durante la administración del Pdte. López Obrador han detenido los esfuerzos que se habían estado haciendo en digitalización y ciberseguridad. Entre 2018 y 2022 el presupuesto del IFT se redujo de 1,900 millones de pesos a 1,560 millones de pesos, lo que implicó la cancelación o aplazamiento de proyectos (el presupuesto subió marginalmente en 2023[25]). En cambio, existe una Estrategia Institucional para el Ciberespacio (2020-2024) de la Secretaría de Marina (Semar). Un Acuerdo Secretarial del 01/jun/2022 dispuso que la Unidad de Ciberseguridad (UNICIBER) se constituye en la Coordinadora General del Ciberespacio (EMCOGCIBER), dependiendo operativa, orgánica y administrativamente del Estado Mayor General de la Armada (Gobierno de México, 2022).

23 Ciberseguridad, Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas, https://ciberseguridad.com/normativa/latinoamerica/mexico/#Estrategia_Nacional_de_Ciberseguridad

24 Aunque hay una Estrategia de Nacional Digital 2021-2024, ésta no establebe mecanismos que desarrollen la ciberseguridad realmente.

25 Expansión (2022), IFT tendrá un presupuesto de 1,700 mdp para 2023, ligeramente mayor al de 2022 https://expansion.mx/empresas/2022/09/08/el-ift-presupuesto-2023

CUADRO 2 Indice de Ciberseguridad (países escogidos) 2023

RANKING	PAÍS	INDICE DE CIBERSEGURIDAD NACIONAL	NIVEL DE DESARROLLO DE TIC*
1	Bélgica	94.81	74.07
5	Alemania	90.91	80.01
10	España	88.31	72.21
33	Canadá	70.13	75.96
44	Estados Unidos	64.94	81.05
54	Chile	59.74	61.44
71	Brasil	51.95	59.11
72	China	51.95	62.41
90	México	37.66	51.46

FUENTE: NCSI (2023), https://ncsi.ega.ee/ncsi-index/?order=-rank
*** Porcentaje de cumplimiento de Indice de Desarrollo de TIC.**

México es un país altamente expuesto a ataque cibernéticos y no tiene la infraestructura de ciberseguridad necesaria para contar con un sector de TIC sólido. Indicadores de ciber seguridad del NCSI[26], muestran que México carece de análisis e información sobre amenazas cibernéticas (no cuenta con una unidad a nivel nacional especializada en el análisis de ciber amenazas estratégicas, ni hay una publicación anual de la situación de ciber amenazas a nivel nacional, ni hay un sitio de internet para profesionales de TIC y ciberseguridad donde las autoridades puedan dar información sobre este tema). Esta situación puede ser un desincentivo para la inversión extranjera y el *nearshoring* por la vulnerabilidad de las empresas al hackeo. El contar con un sector TIC bien desarrollado y protegido contra los ataques cibernéticos es esencial para el desarrollo de las relaciones productivas y comerciales transfronterizas (Center for Strategic and International Studies (2021).

Es de extrañar que a pesar de la vulnerabilidad ante los ciberataque en México no se haya mejorado el marco legal y regulatorio para asegurar la protección de información digital. En 2022 ocurrieron ciberataques de gran envergadura, afectando al sector comercio, al sector productivo y al militar. Entre otros: Mercado Libre sufrió un acceso no autorizado afectando a 50,000 usuarios de México (de 300,000 en total en América Latina); Foxconn, uno de los principales proveedores de Apple, fue víctima de un ataque

26 National Cybersecurity Index (NCI), https://ncsi.ega.ee/ncsi-index/

de ransomware en su planta de Tijuana, Baja California, luego de que ya había experimentado algo similar en su planta de Ciudad Juárez, Chihuahua. Por su parte, el medio digital *Latinus* hizo públicos documentos hackeados por el grupo delictivo "Guacamaya" a la Secretaría de la Defensa Nacional (extrajeron 10 terabytes de información de diferentes instituciones de países latinoamericanos, y más de la mitad era información resguardada por el ejército mexicano).[27]

En contraste con la inacción en México, en Estados Unidos, como resultado de fuertes ciberataques recientes, se firmaron varias nuevas leyes de ciberseguridad en 2022. La más importante es aquella a nivel federal, *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA), que requiere a las compañías de infraestructura crítica reportar incidentes de ciberseguridad y pago de rescates al Departmento de Seguridad Nacional (DHS, por sus siglas en inglés) en lapsos cortos y definidos de tiempo. Adicionalmente, 24 estados de ese país promulgaron al menos 41 leyes sobre el tema de ciberseguridad en 2022.[28]

27 El Economista, Ciberseguridad México 2022: de Mercado Libre a Guacamaya, https://www.eleconomista.com.mx/tecnologia/Ciberseguridad-Mexico-2022-de-Mercado-Libre-a-Guacamaya-20230108-0003.html, 8 de Enero, 2023.
28 NCSL, Cybersecurity Legislation 2022, https://www.ncsl.org/technology-and-communication/cybersecurity-legislation-2022

V. Una política pública digital consistente con la Industria 4.0 y una postura proactiva frente al *nearshoring*

Con vistas a un proceso intensivo de *nearshoring* en México, una política industrial digital, necesita adoptar una visión mucho más amplia de lo que normalmente se entiende por una política de este tipo, desde múltiples flancos.

Es necesario universalizar el servicio de Internet a toda la población y todas las empresas de manera que las inversiones que vengan a México para aprovechar el *nearshoring* puedan ubicarse no sólo en núcleos que cuenten con este servicio actualmente sino en cualquier parte del país y con las misma calidad de éste. Lo anterior se hace posible en la medida en que el gobierno realice las inversiones requeridas por la infraestructura digital y/o que encuentre soluciones para ello en asociaciones público-privadas, APP, como es el caso de Red Compartida que si bien ha enfrentado problemas avanza con el apoyo mutuo de ambos sectores.

De todas formas se necesita realizar inversiones en infraestructura para las redes 5G pues aún la Red Compartida no puede ofrecer las condiciones óptimas para este tipo de tecnología. Es indispensable subastar más espectro 5G a precios adecuados (ahora el espectro es 60% más caro que el promedio mundial).

Simultáneamente, apremia ampliar la infraestructura para almacenar y transmitir los contenidos (nodos IXPs y centros de datos) en el país, sin los cuales no se puede alcanzar una transmisión eficiente de datos.

Es necesario fortalecer la política de competencia y el IFT de manera que este último organismo pueda evitar el comportamiento monopólico del incumbente en el mercado de telecomunicaciones.

La alfabetización de la población en el manejo de internet también es indispensable para que haya un capital humano que pueda desenvolverse adecuadamente con las nuevas tecnologías digitales.

Una tarea pendiente es contar con el marco legal y regulatorio para asegurar la ciberseguridad incluyendo la protección de datos personales y así dar confianza a los inversionistas nacionales e internacionales para operar desde México. Para este fin habría que promulgar una ley de ciberseguridad y constituir un organismo autónomo que se encargue de su aplicación.

El que se encuentre la Armada Nacional a cargo de perseguir al cibercrimen requiere una evaluación seria dado que no parece estar evitando graves ataques cibernéticos incluso a las propias fuerzas armadas. El o los organismos a cargo de esta delicada labor necesitan tener suficiente expertise e instrumentos para detener los grandes y frecuentes ciberataques en el país.

La tarea de proteger el tráfico y almacenamiento de datos también es esencial para que México pueda cumplir con los compromisos internacionales ya adquiridos en ciberseguridad como el T-MEC y APEC.

Se necesita una cooperación más estrecha entre México y Estados Unidos en materia de ciberseguridad de la cual el primer país puede beneficiarse dada la amplia experiencia del segundo.

México se enriquecería si buscara más relaciones de colaboración con grandes empresas tecnológicas internacionales, las cuales pueden hacer inversiones en el país en I&D, mejorando a la vez, su capacidad en materia de innovación tecnológica. Varias empresas ya realizan este tipo de actividades en México en colaboración con universidades como, por ejemplo, Microsoft y Huawei (Oropeza y Berazaluce, 2021).

VI. Bibliografía

Center for Strategic and International Studies (2021), *The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment*, https://www.csis.org/analysis/development-ict-landscape-mexico-cybersecurity-and-opportunities-investment.

CEPAL y eLac 2024, Unión Europea (2022), *Un camino digital para el desarrollo sostenible de América Latina y el Caribe*, https://repositorio.cepal.org/bitstream/handle/11362/48460/4/S2200899_es.pdf

IFT (2023), *El IFT inicia la consulta pública de integración para recabar información y propuestas para el diseño y elaboración del proyecto de bases de la próxima licitación de espectro para servicios de telefonía y banda ancha móviles*, https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/el-ift-inicia-la-consulta-publica-de-integracion-para-recabar-informacion-y-propuestas-para-el

IFT (2022), *IMT en México; más espectro para aplicaciones de banda ancha inalámbricas*. https://www.ift.org.mx/sites/default/files/imt_en_mexico_2021_febrero2021.pdf

Gereffi, Gary (2014), "Global value chains in a post-Washington Consensus world", Review of International Political Economy, Vol. 21 [en línea] https://www.tandfonline.com/doi/abs/10.1080/09692290.2012.756414

Gereffi, Gary, John Humphrey y Timothy Sturgeon (2005), "The governance of global value chains", Review of International Political Economy, Vol. 12, [en línea] https://www.tandfonline.com/journals/rrip20

Gobierno de México (2022), Coordinadora General del Ciberespacio, https://www.gob.mx/semar/articulos/unidad-de-ciberseguridad-279197#:~:text=Ciberseguridad%20y%20Ciberdefensa.-,En%20Acuerdo%20Secretarial%20Núm.,Mayor%20General%20de%20la%20Armada.

Humphrey, John (2019), Global Value Chains, Edward Elgar Publishing.

INEGI (2023), *Estadísticas a Propósito del Día Mundial del Internet*, https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2023/EAP_Internet23.pdf

Jung, Juan (2021), Mesoamérica digital 2025; Propuesta para una agenda digital mesoamericana, *Serie Desarrollo Productivo*, N° 227, CEPAL.

Oropeza García, Arturo, y Julen Berazaluce Iza (2021), *De la Revolución industrial a la Revolución Digital, Hacia una Agenda Digital para México*, https://www.inadi.mx/_files/ugd/527291_b7ad74a4c9704f628cd945def056943b.pdf

ProtDataMex, *Aceptación de México en el Sistema de Reglas de Privacidad Transfronteriza de APEC*. https://protecciondatos.mx/2013/02/esaceptacin-de-mxico-en-el-sistema-de-reglas-de-privacidad-transfronteriza-de-apecenadmission-mexico-apecs-crossborder-privacy-rules-system/#:~:text=El%20IFAI%20reporta%20que%20México,)%2C%20después%20de%20Estados%20Unidos

Schatan, Claudia (2023), El despliegue de la banda 5G y su potencial para la industria 4.0, *Ciencia*, Vol. 74, Nº 2.

Schatan, Claudia (2022), "Descuido de la Ciberseguridad: un autogol", *Voces México*, Octubre 28. https://vocesmexico.com/opinion/descuido-de-la-ciberseguridad-un-autogol/

World Economic Forum (2023) en "*Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows", Briefing Paper*, enero. https://www3.weforum.org/docs/WEF_Data_Free_Flow_with_Trust_2022.pdf

ProtDataMex (2013), *Aceptación de México en el Sistema de Reglas de Privacidad Transfronteriza de APEC*. https://protecciondatos.mx/2013/02/esaceptacin-de-mxico-en-el-sistema-de-reglas-de-privacidad-transfronteriza-de-apecenadmission-mexico-apecs-crossborder-privacy-rules-system/#:~:text=El%20IFAI%20reporta%20que%20México,)%2C%20después%20de%20Estados%20Unidos

INADI

Mtra. Claudia Schatan

Consejera del Instituto para el Desarrollo Industrial y la Transformación Digital A.C. (INADI)

ENERO 2024