MEXICO
INTERNATIONAL
CHAMBER OF COMMERCE

The world business organization

PAUTA 97

INNOVACIÓN PARA TODOS

AGOSTO • 2021

PAUTA 97

AGOSTO 2021

ICC México PAUTA 97
Boletín Informativo del Capítulo Mexicano de la Cámara Internacional de Comercio, A.C.

Consejo Editorial
Presidente
Claus von Wobeser

Vicepresidentes
Alberto Espinosa Desigaud
Federico Bernaldo de Quirós
Nelly Molina Peralta

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
Belén Esquivel Llaguno
Rosaura Revueltas Martínez

Gerente de Eventos
Abigail Blanco Rojano

Creación en Formato electrónico
Rafael Ríos Kunkel

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, exclusivo para socios del Capítulo Mexicano de la Cámara Internacional de Comercio. Las ideas expuestas por nuestros colaboradores no corresponden necesariamente al pensamiento de ICC México. Su distribución es exclusivamente para socios activos 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: 04-2020-030417361700-203
Especie: Difusión vía red de cómputo. Género: Difusiones periódicas
Domicilio de la publicación y del distribuidor: Maricopa 10 piso 6, Col. Nápoles C.P. 03710, Ciudad de México
Teléfonos: (52) 5687 2203, 5687 2207, 5687 2321 5687 2507, 5687 2601.
Título. ICC MEXICO PAUTA BOLETIN INFORMATIVO DEL CAPITULO MEXICANO DE LA CAMARA INTERNACIONAL DE COMERCIO A.C.

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.

Género: Difusiones Periódicas
Especie: Difusión vía red de computo
web: www.iccmex.mx
e-mail: ygonzalez@iccmex.org.mx; laltamirano@iccmex.org.mx

ÍNDICE

Carta del Presidente 1

México como Velocista Digital: el potencial de su economía digital 3

Economía digital: la oportunidad a partir de la pandemia 10

Domain Name and Trademark Enforcement inMexico and its connection with E-commerce 14

El impuesto a los robots

Inteligencia artificial: el enfoque europeo 36

Mercado Libre y sus herramientas para el combate a la falsificación y piratería 42

Por qué ahora más que nunca es relevante la ciberseguridad 48

Manual de Ciberseguridad de ICC 53

Estimados socios:

Encarar los retos generados por la pandemia COVID-19 requerirá de dos factores clave: acceso a la tecnología y capacidad de innovación, razón por la que fueron elegidos como ejes temáticos de la edición 97 de Pauta, que ICC México pone a su consideración.

El artículo "México como Velocista Digital: El potencial de su economía digital" plantea que el país forma parte de un grupo de 16 economías emergentes con alto potencial de las tecnologías para transformar la economía, detonar la productividad e impulsar un crecimiento económico sostenido e inclusivo. Por todo ello, existe la oportunidad de lograr un impacto económico sin precedentes en los próximos años, siempre que se adopten programas y políticas públicas estratégicas y se establezcan marcos jurídicos y políticas de gobierno que promuevan la innovación y la competitividad y, sobre todo, la formación de capital humano con base en inversiones de los sectores público y privado.

En el análisis "Economía digital: La oportunidad a partir de la pandemia" se explica cómo, en medio de la crisis financiera por COVID-19, las pequeñas y medianas empresas encontraron nuevas formas de atraer nuevos clientes, reactivar sus ventas, diversificar su cartera de consumidores y lograron expandir sus negocios a través de las herramientas digitales como Facebook, Instagram y WhatsApp, que en México al igual que en todo el mundo, han devenido en nuevos escaparates y escenarios para millones de empresas, especialmente las MiPymes.

En el proceso de evolución acelerada del comercio digital, contar con un nombre propio de dominio y el reconocimiento de marca puede hacer la diferencia entre el éxito o el fracaso en el entorno de comercio digital. El lector encontrará el texto *Domain Name and Trademark Enforement in Mexico and its connection with E-commerce* ("Observancia de nombres de dominio y de marcas en México, y su relación con el comercio electrónico"), donde se exponen casos de disputas de nombres de dominio y explican las características del sistema legal marcario en México, regulado por la Ley Federal deProtección de la Propiedad Industrial y se examinan puntos importantes de la modernización del régimen legal de esta actividad, considerando la tendencia global de la digitalización. En este análisis se subraya la importancia para las empresas de definir una estrategia legal para el uso de nombres de dominios, con el fin de salvaguardar el futuro de los negocios en esta área vital para la economía en la etapa post-COVID.

Precisamente, en esta fase caracterizada por la innovación, en el artículo "Impuesto a los Robots" se plantea que algoritmos sofisticados tienen la capacidad de reemplazar a millones de trabajadores que realizan actividades cognitivas, esto es, actividades complejas, en adición a aquellos que realizan actividades mecánicas o repetitivas. En este espacio se ofrece un análisis sobre las pretensiones de gravar a la inteligencia artificial, donde se apunta la necesidad de encontrar un balance entre el cuidado de los empleos tradicionales y la necesidad de promover el desarrollo tecnológico, teniendo presente el riesgo de llegar a extremos que podrían afectar gravemente la competitividad local e internacional de diversos sectores económicos alrededor del mundo.

En esta edición se incluye el artículo “Inteligencia artificial: el enfoque europeo”, que considera que la inteligencia artificial tiene impactos importantes en nuestras vidas y que, como tal, debe tener reglas y límites, con una orientación que privilegie la igualdad, la dignidad y la privacidad de las personas, visión que marca un franco contrapunto de China y Estados Unidos.

El lector encontrará, además, el texto “Mercado Libre y sus herramientas para el combate a la falsificación y piratería”, donde se detalla la iniciativa de la empresa líder en comercio electrónico mediante el Programa de Protección de Marca, que ofrece herramientas en los 18 países donde opera, para realizar denuncias y mecanismos de moderación automática mediante el uso de tecnologías de machine learning con el objetivo de mantener una plataforma libre de productos falsificados y pirateados.

En el artículo “Por qué ahora más que nunca es relevante la ciberseguridad”, se explica que la adopción exponencial de las tecnologías de la información a causa de la pandemia COVID-19 ha atraído a actores maliciosos al ciberespacio, que tratan de aprovecharse de las vulnerabilidades expuestas por la pandemia. Por ello, se propone que las empresas, gobiernos y la sociedad contribuyamos a lograr la implementación de políticas públicas que aseguren la adopción de tecnologías que nos permita tener un mundo digital más seguro.

El lector también encontrará en este espacio la Guía ICC de Ciberseguridad, donde se explica el impacto de la actividad de la ciberdelincuencia, que golpea especialmente a las pequeñas y medianas empresas, por lo que plantea la necesidad de la cooperación internacional, homologación de regulaciones y el fortalecimiento de capacidades indispensables para el desarrollo seguro de la economía digital.

Con este esfuerzo editorial, ICC fortalece una de las campañas prioritarias de nuestro programa de trabajo: Hacer que la tecnología trabaje para todos, la cual se conecta con nuestro hub de conocimiento Innovación para Todos, cuya finalidad es llevar a la práctica acciones y soluciones para conducir un cambio global a gran escala que provea instrumentos que permitan a las empresas beneficiarse de la economía digital y del internet seguro, en un entorno que proteja la propiedad intelectual, combata la piratería y asegure los beneficios del e-commerce.

Un saludo afectuoso.

Claus von Wobeser
Presidente

México como Velocista Digital

El potencial de su economía digital.

Lina Ornelas Núñez

Presidenta de la Comisión de Economía Digital de ICC México y
Head of Government Affairs & Public Policy. Google

Resumen

El artículo muestra la importancia de las tecnologías digitales en los países con mercados emergentes, llamados *velocistas digitales*. Esta figura busca exponer el potencial que tienen las tecnologías para transformar la economía y detonar la productividad y un crecimiento económico sostenido e inclusivo, que contribuya a reducir las brechas de desigualdad existentes. Las naciones emergentes podrán beneficiarse de este nuevo fenómeno siempre que instrumenten políticas públicas que se traduzcan en fuertes inversiones en el capital humano, infraestructura yestablezcan marcos jurídicos y políticas de gobierno que promuevan la innovación y la competitividad.

En 1987 el premio Nobel de Economía, Robert Solow afirmó en un artículo publicado en The New York Times, que “se puede apreciar la influencia de la era de las computadoras en todas partes, menos en las estadísticas de productividad”. Solow hacía referencia a la creciente inversión e incorporación quehicieron las empresas en TICs durante las décadas de 1970 y 1980 en Estados Unidos, inversión que no lograba verse reflejada en su productividad. Este fenómeno sería conocido como la “Paradoja de Solow”.

Hoy, cuarenta años después, con el acceso masivo a internet, esta paradoja parece manifestarse en las tecnologías digitales, pues a pesar de la gran penetración que han tenido en la economía, esto no necesariamente se ha traducido en un aumento de la productividad, que es uno de los pilares del desarrollo económico a largo plazo. Este fenómeno se analiza en *The Digital Sprinters: Driving Growth in Emerging Markets*[1], una investigación preparada por AlphaBeta para Google, sobre dieciséis economías emergentes, que denominan como los “velocistas digitales”. Estas dieciséis economías en estudio son: Argentina, Brasil, Chile, Colombia, Egipto, Israel, Kenia, México, Nigeria, Perú, Arabia Saudita, Sudáfrica, Rusia, Turquía, Emiratos Árabes Unidos y Ucrania.

En los “velocistas digitales” se observa cómo el rápido crecimiento de la penetración de Internet y las tecnologías no correspondió con una mejora en la productividad ni con un ritmo más rápido de crecimiento económico pues, a pesar de que la cantidad de usuarios de Internet creció el 9,2 por ciento, la productividad laboral aumentó sólo un 0,6 por ciento y el PIB per cápita en sólo un 0,1 por ciento. La razón principal de este bajo desempeño, a pesar de la creciente penetración digital, se debe a que no es suficiente centrarse solamente en generar acceso a las tecnologías digitales si lo anterior no se respalda con programas públicos que permitan aprovechar sus beneficios, en todos los sectores de la economía.

El informe asegura que las tecnologías digitales podrían crear una oportunidad potencial anual de hasta 3.4 billones de dólares de impacto económico para 2030 en estas economías emergentes, lo que haría transformar su desarrollo económico de forma positiva. Es un hecho que estos países, incluyendo México, tendrán la necesidad de reconstruir sus economías en el mundo de la post-pandemia, luego del impacto negativo que trajo el COVID-19, por lo que resulta crucial sacar ventaja de ese dividendo digital en potencia.

El desafío estriba entonces en hacer que las tecnologías digitales sean un detonador de la productividad y de un crecimiento económico sostenido e inclusivo, es decir, que contribuya a reducir las brechas de desigualdad que existen en nuestras sociedades. Esto únicamente se podrá lograr si, además del desarrollo de la infraestructura física para la conectividad, se realizan fuertes inversiones en el capital humano y se establecen marcos jurídicos y políticas de gobiernos que promuevan la innovación y la competitividad.

[1]The Digital Sprinters: Driving Growth in Emerging Markets, el estudio puede consultarse en el siguiente enlace: https://blog.google/documents/94/The_Digital_Sprinters_FINAL.pdf/

Los desafíos y oportunidades de México como "Digital Sprinter"

La investigación de AlphaBeta concluyó que, en las economías emergentes analizadas, el crecimiento en la penetración de internet no se ha traducido en un mayor crecimiento económico. En el caso de México, durante el periodo 2013 - 2019 el acceso de la población a Internet ha crecido a un promedio anual del 9,9 por ciento, en tanto que los aumentos anuales en promedio han sido del orden del 2,7 por ciento en el caso del PIB real y de un 1 por ciento en el caso de productividad laboral. La pandemia generada por el virus SARS-CoV2 (COVID-19) y la crisis económica que la ha acompañado, que en nuestro país ha significado una disminución del 8.5 por ciento en el PIB, sólo ha hecho que la disparidad entre acceso a internet y crecimiento económico sea aún más dramática.

Esto es muestra de que el mero desarrollo de la infraestructura, si bien es una condición necesaria, no es suficiente para detonar el crecimiento económico y que se requieren de más acciones de política pública para ir más allá de la penetración del Internet y conseguir que los beneficios del mundo digital impacten en el desarrollo económico y, sobre todo, en el bienestar de las personas.

En ese sentido, la crisis derivada de la pandemia por COVID-19 debe verse como una oportunidad para transformar la realidad de México y transitar a una economía digital, lo que necesariamente implica re-enfocar las políticas públicas en los siguientes ámbitos:

Infraestructura Física. - El nuevo marco regulatorio en materia de Telecomunicaciones,[2] ha impulsado un crecimiento en la conectividad. El Instituto Nacional de Estadística y Geografía (INEGI) en su Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2020, señala que el país cuenta con 84.1 millones de usuarios de internet, que representan 70.1% de la población de seis años o más. Esta cifra revela un aumento de usuarios de 1.9 puntos porcentuales respecto a 2019, 4.3 por ciento respecto de 2018 (65.8%) y de 12.7 puntos porcentuales en relación con 2015.[3] Asimismo, el Instituto Federal de Telecomunicaciones (IFT) señala que México se encuentra dentro de los 10 países con mayor crecimiento en el uso de fibra óptica.[4]

[2] Cabe recordar que se publicaron en el Diario Oficial de la Federación el 11 de junio de 2013 la Reforma Constitucional en materia de Telecomunicaciones y el 14 de julio de 2014 la nueva Ley Federal de Telecomunicaciones y Radiodifusión

[3] Instituto Nacional de Estadística y Geografía (INEGI), 22 de junio de 2021, comunicado de prensa 352/21: Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020 en https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf Consultado el día 3 de julio de 2020.

[4] Instituto Federal de Telecomunicaciones (IFT), 27 de julio de 2020, comunicado de prensa 56/2020: México segundo país con mayor crecimiento en teledensidad de Banda Ancha Móvil: OCDE en http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/mexico-segundo-pais-con-mayor-crecimiento-en-teledensidad-de-banda-ancha-movil-ocde-comunicado Consultado el día 3 de julio de 2020.

Este crecimiento se ha dado principalmente en zonas que son fáciles de conectar, es decir, áreas urbanas con mayor densidad poblacional y de mayores ingresos. El verdadero desafío radica en proveer de conectividad en zonas rurales, de difícil acceso y en las que la población no tiene la capacidad económica para contratar un servicio de Internet. En este caso, se requieren fuertes inversiones del sector público, reutilizar la infraestructura pública existente, una política eficiente de utilización del espectro radioeléctrico e incentivos al sector privado para que inviertan en zonas que les son poco rentables. El objetivo debe ser que las comunidades y personas de pocos recursos puedan tener accesoa Internet y no se continúen perpetuando las desigualdades en este sector, ya que ante la ausencia de acceso a las oportunidades que brinda el internet, las diferencias se exacerban aún más con el resto dela población ya conectada y que comienza a obtener los beneficios de la educación en línea, el comercio electrónico o el teletrabajo.

Construir una infraestructura digital que esté lista para el futuro, pensada para ofrecer interoperabilidad y actualizaciones. - En un escenario tecnológico en rápida evolución, los desafíos surgen cuando se crea una infraestructura digital pensando en una tecnología en particular que podría terminar siendo obsoleta a futuro. De forma similar, si la infraestructura se construye teniendo en cuenta sólo a ciertos proveedores o empresas, se podría generar problemas de interoperabilidad que pueden generar fragmentación, altos costos de transacción y provocar problemas de competencia. El desarrollo de la infraestructura digital tanto pública como privada, debe procurar ser neutral para asegurar que estos

procesos sean competitivos y evitar que se elijan tecnologías ineficientes o costosas en el largo plazo.

Conectividad personal. - El desarrollo de la infraestructura física de telecomunicaciones debe ir acompañado de una política que le garantice a la población el acceso a un dispositivo para que se pueda conectar a Internet. Independientemente de que el Estado pueda proporcionar los dispositivos directamente a las poblaciones menos favorecidas como un apoyo social, es primordial que se establezca una política que garantice la asequibilidad de los mismos, lo que se puede fomentar mediante la flexibilidad de trámites aduaneros y tasas arancelarias, homologando estándares técnicos y facilitando la certificación de los equipos.

Fomentar el Desarrollo de Capital Humano. - Un desarrollo económico incluyente que aproveche los beneficios de la economía digital, no es posible al margen de la alfabetización digital. La transición a una economía digital requiere de una fuerza laboral con habilidades y competencias que le permitan desarrollarse en la economía digital. Esto requiere de inversiones importantes en capital humano, empezando por la transformación de los modelos, planes y programas de educación pública desde los niveles educativos básicos.

Promover la innovación tecnológica y el emprendimiento. - El surgimiento de nuevos modelos de negocios basados en la innovación tecnológica son el vehículo para que la economía digital realmente despegue. Para ello, consideramos que será fundamental:

- **Promover usos innovadores de datos.** No obstante que los datos por sí mismos pudieran no tener un valor intrínseco, el proceso de recopilar información, colocarla en una estructura relevante, interpretarla para formar conocimiento y realizar análisis a partir de la data paragenerar información y conocimiento, sin duda crea valor. Los datos colaborativos han generado un gran entusiasmo en todo el mundo por su potencial para impulsar la innovación a través de la investigación y el desarrollo en los sectores privados y académicos. Un portal único para acceder a la información puede desempeñar un papel fundamental en la difusión de dichos datos, esto se podría fomentar con una Ley de Datos Abiertos en México en un futuro cercano, e incluso promover un Hub de Datos Abiertos al amparo del T-MEC que contiene las disposicionesadecuadas en materia de libre flujo de datos, medidas para su adecuada protección (que garanticen la privacidad de los individuos a los que se refieren), así como la prohibición de localización forzada de datos

- **Establecer plataformas para interactuar e innovar en la colaboración (“crowdsourcing”).** Las innovaciones para mejorar los servicios estatales pueden surgir de cualquier persona y en cualquier lugar, por lo tanto, los gobiernos son responsables de involucrar y empoderar a los ciudadanos para que participen en este proceso. Algunos proyectos en otros países han incluido, por ejemplo, iniciativas para mejorar la información ganadera en tiempo real, una aplicación móvilpara promover buenas prácticas agrícolas y la digitalización de servicios del gobierno.

- **Desarrollar centros de transformación digital (innovación) y fábricas modelo (educación).** Estos son lugares físicos donde los emprendedores, empresarios, investigadores e innovadores pueden acercarse a probar nuevas tecnologías y aplicaciones digitales, en los cuales, además, puede ofrecerse capacitación y desarrollo de aptitudes. La implementación exitosa de tales iniciativas requiere un fuerte compromiso por parte de la industria, para garantizar que se vean los beneficios de la colaboración, implementando un enfoque riguroso para identificar las tecnologías y sectores clave en los que concentrarse (sin descuidar los sectores tradicionales) y asegurando que haya marcos claros que rijan el uso de la propiedad intelectual que se genera.

Cómputo en la Nube. - La computación en la nube ha ampliado el acceso a la infraestructura informática, al permitir que empresas de distintos tamaños puedan acceder a las mismas herramientas, aplicaciones y servicios sin tener que realizar grandes inversiones y con altas medidas de ciberseguridad.Esto promueve la competencia y el desarrollo de nuevos productos y servicios. Asimismo, las tecnologías

de computación en la nube aplicadas al gobierno podrían generar importantes beneficios relativos a la eficiencia y ahorros de costos para los presupuestos de TIC del gobierno.

Digitalización de pagos. - Los gobiernos de todo el mundo permiten, cada día más, métodos de pago online y móviles para abonar servicios y repartos de subsidios o ayudas estatales. Realizar esto puede impulsar la implementación de los productos FinTech en la población, desde arriba hacia abajo, y puede reducir costos y el manejo de dinero en efectivo. También es un canal directo para la inclusión financiera, que por lo general, las personas experimentan con sus primeras cuentas en servicios financieros digitales, como las billeteras móviles. Finalmente, la utilización de pagos digitales permite un mejor seguimiento y una forma de cobrar impuestos más eficientes, que a su vez puede reducir las fugas de dinero y mejorar la recaudación.

Competencia Económica. - Contar con una regulación que promueva la competencia y no se enfoque en tratar de excluir a ciertos agentes económicos es fundamental para el florecimiento de la economía digital. Establecer legislaciones y políticas diseñadas para "*reorganizar*" los mercados suelen estar destinadas al fracaso, ya que no abordan la causa subyacente que pudiera haber impedido la competencia. Por ello, las acciones de las autoridades en materia de competencia deben basarse en casos concretos y con fundamento en pruebas que acrediten de manera fehaciente las conductas anticompetitivas y que no impidan la innovación que acarrea grandes beneficios a los usuarios finales.

Gobierno Digital. - Impulsar la digitalización del Gobierno tiene beneficios sociales intrínsecos, no sólo en términos de eficiencia en las labores internas, sino también de frente a la sociedad. La digitalización de los servicios gubernamentales puede tener efectos secundarios económicos importantes por dos razones clave: puede mejorar la prestación de servicios públicos y transparentar la función gubernamental.

Conclusiones

Para que México salga de la nueva versión de la paradoja de Solow y se enfile por el camino de los velocistas digitales requiere abrir la discusión sobre las políticas centradas en la transformación digital de la economía, la sociedad y el gobierno. Este es objetivo del estudio *The Digital Sprinters: Driving Growth in Emerging Markets,* comprender cómo las economías emergentes pueden aprovechar al máximo las tecnologías digitales para percibir ganancias en el desarrollo económico. Capturar este dividendo digital en potencia, puede ser la respuesta para reconstruir a la economía luego del impacto de la pandemia por COVID-19, atender los problemas derivados de la crisis económica y las demandas sociales por una mayor equidad. Esto requiere de una redefinición de las políticas públicas y de fuertes inversiones nosólo del sector público, sino también del privado. El éxito dependerá de la colaboración entre empresas y gobierno.

El país tiene hoy la posibilidad de beneficiarse de un impacto económico sin precedentes en los próximos años, siempre que se adopten programas y políticas públicas estratégicas en apoyo a la plena utilización de las tecnologías digitales, que no se reducen únicamente a ofrecer acceso a Internet e infraestructura, como parece haberse creído, sino que vayan a los negocios basados en la datificación, en el crowdsourcing, la digitalización de pagos, el uso extensivo de la nube y, sobre todo, en la formación de capital humano. Si no invertimos en las personas, no se podrá alcanzar un crecimiento económico inclusivo que disminuya las desigualdades presentes en nuestra sociedad. En ICC, desde la Comisión de Economía Digital, hemos creado un subgrupo de trabajo multi-actor y multidisciplinario para abordar y discutir las mejores políticas públicas para que nuestro país sea un velocista digital.

Economía digital: La oportunidad a partir de la pandemia

Artículo de Facebook

Resumen del caso: En medio de la crisis financiera por COVID-19, las pequeñas y medianas empresas encontraron nuevas formas de conectar y hacer crecer sus negocios a través de las herramientas digitales. Facebook, Instagram y WhatsApp se volvieron los nuevos escaparates y escenarios para miles de MiPyMEs. Esta realidad también impulsó a que las empresas generaran productos orientados a la reactivación económica.

***

De un día al otro, negocios en todo el país empezaron a cerrar sus puertas, los teatros dejaron de dar funciones, los restaurantes tuvieron que adoptar nuevos protocolos, los hoteles redujeron su capacidad y los salones de eventos tuvieron que replantear su estrategia comercial.

En total, de acuerdo al INEGI, se cerraron más de un millón de negocios entre 2019 y finales de 2020 y se perdieron más de 3.2 millones de empleos formales en consecuencia. Sin embargo, para muchos pequeños y medianos negocios fue una oportunidad para extender su alcance y conectar con los consumidores en nuevos ámbitos. Para casi todos, la adopción digital fue el nombre del juego durante 2020 y continúa siendo la mejor apuesta para la resiliencia y la reinvención económica.

En pocos meses, los teatros migraron a plataformas digitales, los restaurantes ofertaron sus menúes en redes sociales, los hoteles mantuvieron contacto con sus clientes a través de servicios de mensajería y algunos comerciantes encontraron en Internet nuevas oportunidades de negocio para exportar sus productos. Según algunos cálculos, en 2020 se dio un salto de tres años en un par de meses y de acuerdo con el estudio de la Asociación Mexicanas de Ventas Online (AMVO), el comercio electrónico alcanzó los $316 mil millones de pesos durante el año pasado, un crecimiento de 81% en comparación con el año anterior.

Pero ¿cómo se llevó a cabo la adopción digital para las MiPyMEs mexicanas en este periodo acelerado? Según el estudio “Radiografía del Emprendimiento” de la Asociación de Emprendedores de México (ASEM), 36% de estas empresas estableció su presencia digital apenas en 2020, utilizando plataformas digitales como Facebook (88%), Instagram (56%) y WhatsApp (55%) para difundir sus productos.

Adoptar herramientas digitales intuitivas y sin costo permitió a las MiPyMEs atraer clientes nuevos, reactivar sus ventas y diversificar su cartera de clientes. Lo que podría significar una inversión de cientos de miles de pesos y una adopción tecnológica de años para otras empresas, las MiPyMEs lo resolvieron en pocos eses con herramientas como WhatsApp o Facebook Messenger. ¿La fórmula? Conveniencia y alcance sin costos adicionales; encontrar potenciales clientes en los espacios digitales.

El viaje a la transformación digital: El caso de Vagando por México

Vagando por México, una agencia de viajes que se especializa en experiencias accesibles para todo tipo de viajeros, fue fundada por José de Jesús en 2015. Cuando inició, José trató de llenar los cupos para sus primeros dos viajes. Necesitaba alrededor de 12 personas por viaje para que fuera viable, pero tras solo recibir dos registros para cada uno, tuvo que cancelarlos.

En septiembre decide pautar **$200 pesos en Facebook, con los que llenó 100 lugares**, permitiéndole cerrar 2015 con 12 viajes en total. A partir de esto, Vagando por México decide enfocarse en el uso de Marketing Digital para hacer crecer su negocio, incorporando también Instagram y WhatsApp a las aplicaciones a través de las cuales ofrece sus servicios y atiende a sus clientes.

Luego llegó 2020 y, a pesar de que en todo el año **llenaron 70 viajes**, la mayoría de estos ocurrieron de enero a marzo y los siguientes tres meses estuvieron detenidos. Durante este tiempo investigaron nuevas rutas y viajes que se ajustaran a la situación cuando pudieran reanudar actividades. Mantuvieron comunicación con sus clientes en redes sociales para preservar su presencia de mercado. En julio regresaron con capacidad reducida, visitando lugares que permitieran distanciamiento social y espacios abiertos.

Actualmente, la empresa utiliza **Facebook para promover los viajes y su calendario**, y la sección de

opiniones le ha ayudado a que los nuevos clientes se sientan seguros de contratar sus servicios. **Instagram sirve para mostrar imágenes y videos de los destinos y WhastApp es su principal canal de atención a clientes y ventas.**

En 2021, **Vagando por México ha realizado 100 viajes** y está en camino a recuperar su ritmo prepandemia. Hoy la empresa ofrece **70 destinos en todo México**, cuenta con especialidades como planes gastronómicos y próximamente abrirá dos oficinas más en Toluca y Querétaro.

El **80% del tráfico a su sitio viene de las plataformas de Facebook** y sus inversiones en pauta tiene un **retorno de inversión de 100x en promedio**.

Por otra parte, las empresas de tecnología empezaron a lanzar productos específicos que respondían a las necesidades de los pequeños empresarios, tales como una función para que los emprendedores pudieran crear una tienda en línea desde Facebook e Instagram; una opción para que los negocios que dependían de eventos presenciales pudieran monetizar sus contenidos y el lanzamiento de catálogos en WhatsApp Business, para mostrar fotos, precios y descripciones de productos, entre muchos otros.

Como consecuencia de esta sinergia, la recuperación económica empezó a volverse una realidad, incluyendo para sectores más impactados como los negocios liderados por mujeres. El "Reporte global sobre el estado de las pequeñas empresas" que analizó el impacto que la pandemia tuvo en más de 180 mil negocios de más de 50 países y regiones, incluyendo a más de 3,500 empresas mexicanas, descubrió que:

- Las empresas en operación pasaron de 61% en mayo de 2020 a 76% en febrero de 2021.
- Las empresas aumentaron lentamente su número de empleados, pasando de 34% en mayo a 38% en febrero de 2021.
- La caída de ventas de las empresas se redujo en 18%, de mayo de 2020 a febrero de 2021.
- Las empresas lideradas por mujeres activas pasaron de 56% en mayo a 76% en febrero de 2021.

Esta realidad también inspiró programas que atendieron necesidades específicas, tales como "Ella Hace Historia" de Facebook, una serie de capacitaciones orientadas a que las mujeres, dueñas de negocios, tuvieran conocimientos para acceder a financiamiento, fortalecieran su presencia en línea y desarrollaran habilidades en Marketing Digital. De julio a diciembre de 2020, 9,300 mujeres accedieron a los módulos de información financiera de esta iniciativa.

Durante la pandemia también se creó un Centro de Recursos para Empresas desde Facebook, que incluye consejos y capacitaciones para ayudar a negocios a seguir conectados con sus comunidades. Asimismo, contempla recursos sobre el trabajo a distancia y en línea.

Estos se sumaron a los ya disponibles antes de la contingencia como Blueprint que ofrece programas de capacitación y cursos online gratuitos, Facebook para empresas, un sitio que brinda orientación sobre cómo hacer negocios en las plataformas de Facebook y las capacitaciones en Marketing Digital, "Impulsa con Facebook", que desde 2018 han alcanzado a más de 62 mil personas.

En la actualidad, hay más de 200 millones de empresas en el mundo –en su mayoría MiPyMEs– que utilizan las herramientas gratuitas de Facebook para llegar a sus clientes todos los meses. Un crecimiento de más de 40% desde enero de 2020, cuando había 140 millones de negocios en estas plataformas.

Yendo hacia la recuperación económica, la resiliencia y apalancamiento en tecnologías como las aplicaciones de Facebook, que los negocios han desarrollado durante la pandemia, serán las fortalezas que les permitirán prosperar en los próximos meses y años.

Domain Name and Trademark Enforcement in Mexico and its connection with E-commerce

Gloria Niembro

She has a bachelor's degree in law from Instituto Tecnologico Autonomo de Mexico, and a master's degree in law from Benjamin N. Cardozo School of Law, New York. Gloria is Director of the Intellectual Property practice at Chevez Ruiz Zamarripa since 2020.

She has published several articles on national and worldwide distribution magazines. Her legal practice focuses both on consultancy and litigation, with ample expertise in enforcing intellectual property rights.

The author gratefully acknowledges the assistance of Arturo Revilla and Carlos Austria, attorneys at Chevez Ruiz Zamarripa, in the updating and researching of this article.

Abstract

The fast-paced technological developments and the current global crisis have pushed companies to change their on-site stores to digital stores. When launching an e-commerce website, traders should be aware that having a proper domain name, as well as a recognized and appealing trademark can make the difference between commercial success or failure.

IP squatters and infringers are present in the cyberspace and have taken over domain names containing third party trademarks. This article will analyze the courses of action available under the recently enacted Mexican Federal Law for the Protection of Industrial Property and the Local Dispute Resolution Policy for right holders to enforce their .mx domain names, as well as their pros and cons in light of Mexican law particularities.

[5] Gloria Niembro is Director of Intellectual Property at Chevez Ruiz Zamarripa. The author gratefully acknowledges the assistance of Arturo Revilla and Carlos Austria, attorneys at Chevez Ruiz Zamarripa in the updating andresearching of this article.

I. INTRODUCTION

Companies and their clients have been forced to embrace the digital economy in the age of COVID-19. Many brand owners that functioned as e-commerce platforms saw their market value increase considerably as the only way of keep selling and doing transactions was online. On the other hand, the companies who previously did not engage in e-commerce or had a small sales sector, began selling products online and developing their own platforms, to offer consumers a better experience and to stay afloat during the pandemic, experiencing an increase in its market value as well[6].

In August 2020 the growth of electronic commerce grew in the entire Latin American region by 4.8%, attributing it to the quarantine product of the pandemic[7]. In October 2020, based on data from the National Institute of Statistics and Geography (INEGI), online sales in Mexico increased by 37% to that date, emphasizing that the pandemic led many consumers to electronic commerce, eliminating fears of fraud and generational barriers[8].

Last February 2021, the Mexican Association for Online Sales (AMVO) reported an increase in e-commerce of up to 81% in 2020 compared to 2019[9] [10]. Moreover, five out of ten companies in Mexico are doubling their online presence by investing in efficient and solid electronic commerce platforms,and reducing real estate costs on physical stores.

Social Media, Domain names and Branding

Being active on social media and securing appealing domain names has become crucial for trademark owners that desire to target consumers more precisely and widely. In this infinite and borderless space that the Internet offers and that has been growing exponentially, traders and companies must distinguish themselves to identify their products and services from the rest. Such distinctiveness is obtained not only by seeking a trademark registration but also by securing an internet domain and social networks' profiles that mirror such trademark.

Trademarks' presence in domain names and social media is widespread. Social networks are the entry door where consumers first become aware of the existence of certain businesses. A brand owner must be an active domain registrant and social networks' holder in order to create digital brand identity. The method of establishing an online presence is changing rapidly given the unique and viral nature ofthe social media and the domain market.

The main function of a trademark, being a source identifier, is well reflected on the use of it online. Social media provides the users diverse platforms where consumers and owners can interact freely and

[6] https://www.forbes.com.mx/negocios-amazon-mercado-libre-rappi-crecen-america-latina-google/
[7] https://www.kantarworldpanel.com/mx/Noticias-/Ecommerce-el-ganador-de-esta-pandemia
[8] https://www.eleconomista.com.mx/opinion/La-pandemia-cambio-el-comercio-electronico-para-siempre-20201109-0057.html
[9] https://www.elfinanciero.com.mx/bloomberg-businessweek/la-pandemia-dispara-el-comercio-electronico/
[10] https://marketing4ecommerce.mx/crecimiento-del-ecommerce-en-mexico-81-amvo/

in a wider spectrum. Domain names are commonly comprised of at least one trademark and are registered to enable internet users to locate a company's site on the web.

The use of trademarks online is broad and may be seen in domain names, in usernames and Uniform Resource Locators (URLs) of account holders, as logos placed in profiles, in the content of users' posts, in conversations and other relatively dynamic online content, and in targeted advertisements. These uses may constitute business opportunities for trademark owners, but they also pose distinct challenges to the continued legal functioning of a mark if it is used improperly.

Domain names and .mx country code

MX is Mexico´s country code Top Level Domain. The extension ".com.mx" has been available since 1993. After its closure in 1997, on 2009, NIC Mexico (Network Information Center Mexico), the organization in charge of the administration of the .MX ccTLD announced that .MX domains would be available once again.

According to NIC Mexico[11], the number of current .MX domains that are currently active is as follows:

.com.mx	849,703
.gob.mx	10,339
.net.mx	296
.edu.mx	14,708
.org.mx	15,033
.mx	352,274
TOTAL	**1'242,353**

These numbers continue to grow steadily. The growth as we have seen, can be explained by an increasing interest of registrants in the Mexican market or due to commercial strategies focused on creating a closer bond with consumers from Mexico and the need of companies to adapt or continue trading digitally in light of the social and movement restrictions.

In addition, it is likely that trademark owners have an increasing interest in preventing the registration of .MX domain names that are constituted by or that include their trademarks by non-related third parties (cybersquatting). However, piracy and counterfeiting are significant problems in Mexico and infringement and unfair competition activities have extended to the internet.

[11] https://www.nicmexico.mx/estadisticas-dominios/

Just like the trademark implies exclusivity for its holder over certain term to identify certain goods or services under a specific distinctive sign, a domain name gives its holder exclusivity to host and identify a website through a specific URL that can contain the trader's trademark and/or name.

Based on the foregoing, it is recommendable that people engaged in trade, as well as businesses, consider registering .MX domains, even if they do not have immediate plans of entering the Mexican market. It is important to note that having a direct relation with Mexico is not a requirement for registering ".com.mx" and ".MX" domains. Therefore, the registration of these domains can be done without significant requirements.

In addition to this preventive strategy, it is likely that a person or business finds that a .MX domain name that is identical or confusingly similar to their trademark has been already registered by a third party without authorization. In this article, we will focus on the intersection between trademark enforcement activities, internet domain names and e-commerce.

II. CHARACTERISTICS OF MEXICO´S TRADEMARK SYSTEM

A. Obtaining the right to exclusive use

Mexico´s trademark system is mainly regulated by the Federal Law for the Protection of Industrial Property. Mexico is not purely a first to file or a first to use system, it is a so-called mixed system because while only the registration of a mark provides an exclusive right to use a mark, use of a mark, even without registration, can provide certain rights to the user, such as the following:

- A Mexican registration will have no effect against a third party who in good faith used the same trademark, a confusingly similar one, on the same or similar products or services, if it started to use the trademark before the filing date or first use date stated in the application of the mark claiming a better right.

- A trademark registration can be invalidated if it is identical or confusingly similar to another trademark that was used in Mexico or abroad before the filing date of the application, if the person or entity claiming the right of prior use proves said use without interruption in Mexico or abroad before the filing date or, the date of first use stated in the trademark application.

- Notwithstanding the above, despite the mixed nature of the Mexican system, the registration trademarks is strongly encouraged to ensure the right to exclusive use.

B. Provisions concerning domain names in the Federal Law for the Protection of Industrial Property

- The general rule is that domain names are registered through a domain name registrar and can be done by anyone, no matter where the registrant is located and providing basic contact information. Although there are certain extensions for domain names that link them with a specific country (i.e. ".MX", ".DE", et al), once you have secured a domain name, it will be valid worldwide and unless there are some geo-blocking measures in place, people will able to have access to it from anywhere in the world.

- The recently enacted Federal Law for the Protection of Industrial Property in Mexico sanction as administrative infringements certain behaviors related to domain names. This was a huge progress within the Mexican IP legislation to modernize it and adequate it to the digital era we are living on and to the content of international treaties Mexico has adhered to in the past years.

- For instance, section XVIII of article 386 sanctions the use of a registered trademark as part of a domain name, or one that is confusingly similar, without the consent of the owner of such trademark, as well as the use of a registered domain name as part of a trademark, without the consent of the owner, as long as the products/services offered on the website related thereto are covered by the trademark registration.

- Likewise, section XX sanctions using a registered trademark or one confusingly similar to a registered one as a domain name or as part of it, when such domain name is related to a person or legal entity that produces, imports or commercializes goods or services that are identical or similar to the ones covered by the registered trademark, without having the express and written consent of the trademark holder or the person entitled to grant such content.

- To pursue and sanction these infringing behaviors the Mexican Institute of Industrial Property ("IMPI") requires the affected party to file an administrative declaration for infringement complaint request.

- The sanctions established by the Federal Law for the Protection of Industrial Property go from substantial administrative fines to permanent closure of the establishment, depending on the severity of the infringing conduct, the intentionality of the conduct and the economic capacity of the infringing party.

III. ALTERNATIVES AVAILABLE FOR TRADEMARK OWNERS

Besides having the possibility of filing an infringement complaint based on sections XVIII and XX of article 386 of the Federal Law for the Protection of Industrial Property, trademark owners may, also consider the following alternatives when facing the existence of a ".MX" domain that has been registered without authorization by a third party:

- Filing a complaint with the World Intellectual Property Organization (WIPO) arbitration and mediation center pursuant to the Local Domain Name Dispute Resolution Policy (LDRP).
- Filing an infringement action based on unfair competition.

- Filing a complaint with NIC Mexico.

A. LDRP Complaint

According to NIC Mexico, https://www.dominios.mx/politicas-generales-de-nombre-de-dominio-mx/, "[a]ll the people who consider affected its rights (promoter) and that wish to ask for the cancellation of the registration or transfer of the ownership of a ".MX" domain name, agree to submit to the Dispute Resolution Policy on Domain Names ".MX" (LDRP) and the respective regulation, before a serviceprovider of dispute resolution authorized by the Registry .MX, made by an independent and impartial group of experts."

The decisions rendered in connection with .MX domains from 2001 to 2021 may be consulted at https://www.wipo.int/amc/en/domains/search/index.html.

1. Relevant decisions and analysis

LDRP proceedings do not vary substantially from those brought pursuant to the Uniform Domain Name Dispute Resolution Policy. Nevertheless, it is important that those not familiarized with the Mexican legal system and practice are aware of previous decisions, in order for them to decide what steps to take when considering bringing an action based on the LDRP. The following highlights gathered from recent cases may be useful for that purpose:

I. Having a trademark registration that was filed prior to the registration of the domain name is not, by itself, enough to prove bad faith or illegitimate interests of the party who registered the domain name in dispute. Moreover, the existence of a trademark registration may not be sufficient to establish exclusive rights over a trademark, as illustrated by the following decisions:

Descriptive Term. a) Result: Dismissal. *DMX2011-0026*. Disputed domain names: [laboro.com.mx] and [laboro.mx]. In this case, the Panelist considered that the word "laboro" was descriptive, although the trademark registration for the mark LABORO was in full force and effect and had not been declared descriptive by a Mexican authority. Consequently, the descriptiveness of the trademark may be studied and declared by the Panelist without a previous analysis from Mexican authorities, such as IMPI.

b) Result: Dismissal. *DMX2019-0034*. Disputed domain name: [autoplaza.mx]. Even if the complainant is the owner of a trademark that happens to be the same as the domain name, if such trademark is constituted with generic terms, it forms a descriptive term. In this case, despite owning the trademark AUTOPLAZA, the complainant could not do anything against the registrant of the domain.

. **Fan Site**. Result: Dismissal. *DMX2011-0016.* Disputed domain name: [pumasunam.com.mx]. Even if the complainant owned trademark registrations for PUMAS, the Panelist considered that no bad faith was proved, since the domain name was used for a fan site. The fact that the complainant already owned the domain names [pumas.unam.mx] and [clubpumasunam.com.mx] was considered irrelevant. Furthermore, if a domain name is related to a website that serves as a public discussion forum, freedom of speech must be privileged.

. **Last Name**. a) Result: Dismissal. *DMX2011-0014.* Disputed domain name: [martell.com.mx]. The registrant, an individual who was known by the last name Martell, was contacted by Martell & Co. in an attempt to negotiate the purchase of the domain name. The registrant responded stating that the domain was not for sale and that it was "worth much more than the offer (of Martell & Co.)." No specific monetary request was made and the Panelist ruled in favor of the registrant.

b) Result: Transfer. *DMX2017-0030*. Disputed domain name: [bose.com.mx]. The registrant claimed that trademarks referring to or including a last name, should not have any enforceable rights over a domain name given the common use of same. The panel found there is no legal basis for such argument, since distinctive signs are not limited by short characters, regardless of whether they make reference tosomeone's last name. The Panelist decided to transfer the domain name.

II. The existence of redirection to certain sites, as well as parking or inactive domains have been important elements in the finding of bad faith:

. **Redirection**. a) Result: Transfer. *DMX2012-0006*. Disputed domain names: [google.com.mx] and [gmail.com.mx]. The disputed domain names redirected to websites that displayed content that was identical to the one present in the domain names google.com and gmail.com. Through pay-per-click links, the websites offered misdirected users' prices in exchange for completing a survey. The Panelistconcluded that the respondent was acting in bad faith.

b) Result: Transfer. *DMX2020-0002*. Disputed Domain Name [billpocket.mx]. After registering a .com domain name, the complainant discovered an identical domain name under the country code TLD .mx that redirected to the website of its main competition. The respondent offered to sell the domain in exchange for money. This was deemed as bad faith by the Panelist and the .mx domain name was transferred to the complainant.

. **Parking**. a) Result: Transfer. *DMX2011-0010*. Disputed domain names: [skype.com.mx] and [skype.mx]. The Panelist recognized that the use of a domain name to post parking and landing pages does not *by itself* confer rights or legitimate interests arising from "legitimate noncommercial or fair use" of the domain name, especially where resulting in a connection to goods or services competitive with those of the trademark rights holder.

b) Result: Transfer. *DMX2019-0022*. Disputed name [thehomedepot.com.mx]. Int this case, the panel reinforced that parking does not grant any kind of right or legal interest for the benefit of the domain name's registrant.

. **Inactive**. Result: Transfer. *DMX2009-0008*. Disputed Domain Name [wendys.com.mx]. If the respondent is not currently using the domain name, but has the intention to use it for different commercial reasons than those of interest for the complainant, it is necessary to demonstrate said situation a) by submitting reliable evidence and b) by referring - in the webpage´s content- to the reason why the domain name isnot in use but that it will be in the near future (i.e. in maintenance). Otherwise, the respondent will not be able to prove legitimate interests, as it happened in this particular case.

. **Undue Advantage.** Result: Transfer. *DMX2020-0011*. Disputed Domain Name [arlafoodsingredients.com.mx]. Complainant claimed that the domain name's registrant used to work for the company. Since the registrant did not respond to this point, it was presumed that she acted on bad faith by taking advantage of her prior position and knowledge. The domain name was transferred.

III. Factors to determine similarity to the extent of confusion

. **Additional Terms**. Result: Transfers: a) *DMX2011-0034*. Disputed Domain Names: [ikeamexico.com.mx] and [ikeamexico.mx] and b) *DMX2020-0006*. Disputed Domain Name: [electroluxcdmx.mx]. The addition of generic words such as "*mexico*" and abbreviations such as "cdmx" does not provide distinctiveness to the disputed domain names vis-a-vis the rights of the complainant.

. **Punctuation Marks**. a) Result: Transfer. *DMX2009-0008*. Disputed Domain Name [wendys.com.mx]. A domain name cannot be comprised of apostrophes or punctuation marks; therefore, the respondent´s argument that similarity was absent because the registered mark had an apostrophe and the domain name did not was disregarded.

b) Result: Transfer. *DMX2018-0032*. Disputed Domain Names: [papajohns.com.mx] y [papajohns.mx]. The fact that punctuation marks are present in a trademark but not in the domain name is irrelevant when assessing whether a domain name is confusingly similar to a trademark.

IV. Panelists have ample leeway to decide.

. **UDRP Parallel Criterion**. a) Result: Transfer. *DMX2011-0034*. Disputed Domain Names: [ikeamexico.com.mx] and [ikeamexico.mx]. The Panelist decided to consider, among others factors, the decision issued by a different Panel during an UDRP proceeding in connection with the domain name [ikeamexico.com], where the matter was resolved in favor of the Complainant.

b) Result: Transfer. *DMX2017-0033*. Disputed Domain Name: [teradata.com.mx] On a similar basis, the panel considered previous disputes the owner was part of, as a way of signaling a repetitive conduct of registering domain names using well-known trademarks.

. **Implied consent** a) Result: Transfer. *DMX2011-0013*. Disputed Domain Name: [wella.com.mx]. The parties exchanged communications and the respondent expressed his agreement to transfer the domain name. However, the parties did not reach an agreement; and the proceeding continued. The Panelist was empowered to order the transfer of the domain name, since the respondent had already agreed to transfer it in the exchanges of communications inter-parties.

b) Result: Transfer. *DMX2019-0021*. Disputed Domain Name [venequip.com.mx]. Implied consent shall be taken into account when the owner does not answer. The complainant's statements of facts must be deemed truthful when the registrant does not reply to the arbitration request.

. **Registration of domain name occurring before trademark registration**. Result: Transfer. *DMX2011-0013*. Disputed Domain Name: [wella.com.mx]. The domain name was acquired by the respondent before the trademark WELLA was granted to the complainant. Said situation was not considered by the Panelist given the previous communications between the parties, which lead to the transfer of the domain name to the complainant.

. **Former licensee.** Result: Dismissal. *DMX2011-0034.* Disputed Domain Name [philipcrosby.com.mx]. The registrant was a licensee of Philip Crosby Associates and this license was revoked by the complainant, which resulted in the registrant being impeded from using the mark. The panel requested Philip Crosby Associates to submit proof of existence of trademark registrations, but the latter did not, causing the dismissal of the complaint.

. **Prior Copyright.** a) Result: Dismissal. *DMX2011-0026.* Disputed domain names: [laboro.com.mx] and [laboro.mx]. The owner of the domain name had copyrights with respect to a graphic design shown in the content of the website at issue. This situation was taken into account by the Panelist in order to allege that the respondent had legitimate rights to the domain name.

b) Result: Transfer. *DMX2018-0011*. Disputed domain name: [lancet.mx]. In this case, the panel took into consideration the copyrights granted by the Mexican Copyright Office to the complainant and decided to order the transfer of the domain name.

. **Settlement**. Result. Transfer. *DMX2019-0019*. Disputed domain name: [clarolife.mx]. Complainant claimed that the domain name was similar to the trademark in question. The registrant pointed out that the domain name was for a small business with services and products unrelated to the trademark of the

complainant. Parties came to an agreement of transferring the domain to the complaint, which the panel ratified.

B. Infringement Actions, provisional measures, and remedies

Apart from the specific provisions (i.e. sections XVIII and XX) related to domain names contained in article 386 of the Federal Law for the Protection of Industrial Property Law, the same article sets forth a catalogue of conducts that constitute administrative infringements too and that can be used as basis to bring legal actions against an infringing domain name. These infringements include, for example, the commission, in the exercise of an industrial or mercantile activity, of any act deceiving the public or causing it or inducing it to erroneously believe or assume:

- The existence of a relationship or association between an establishment and that of a third party;
- That a product is manufactured under specification, license or authorization of a third party;
- That services are rendered or products are sold under authorization, license or specification of a third party.

These provisions are especially relevant regarding domain names. In this regard, when a domain name which is identical or confusingly similar to a Mexican trademark registration is used in connection with a website with content that could cause error or confusion among the consumer public, it would be possible to bring an infringement action under sections II, XVII, XXI, XXIV of article 386 of the FederalLaw for the Protection of Industrial Property, in addition to the specific provisions pertaining to domain names.

While Mexican legislation does not expressly forbid the registration in bad faith of domain names, it does prohibit the registration of distinctive signs in bad faith pursuant to section XXII of article 173. To that extent, the second paragraph of this legal provision provides a general definition of what is considered bad faith: “Bad faith will be understood, among other cases, to have applied for the registration of a sign with the purpose of obtaining an undue benefit or advantage to the detriment of its legitimate owner”.

Although this definition of bad faith is not entirely clear and definite, it gives enough discretion for both IMPI and judicial authorities to construe it according to the actual circumstances and the particulars of each case, as the concept of bad faith keeps evolving and expanding throughout time.

In that regard, the fact that a domain name and a trademark registration were registered in Mexico by a bad faith unrelated party can be used by the legitimate owner as evidence to invalidate the registration and cancel or transfer the domain name.

Another important addition the Federal Law for the Protection of Industrial Property includes, is the possibility of requesting the imposition of provisional measures in the digital environment. To this extent, section VII of article 344 envisages that IMPI can order to any alleged infringer or to a third party the suspension, blocking, remotion and cessation of acts that constitute a violation to said industrial property rights through any virtual, digital or electronic platform or medium.

Now, in order to have solid bases to bring an infringement action based on the other sections of article 386 of the Federal Law for the Protection of Industrial Property different from sections XVIII or XX, it is necessary that the infringer uses the violated trademark, not only in the domain name, but in the content of the website.

This is an important difference between the LDRP proceeding and the infringement action not based on sections XVIII or XX, since the former do not require that the owner of the domain name necessarily uses the trademark throughout the website, since it is sufficient if the domain name is confusingly similar or identical to the registered trademark, and the complainant proves bad faith and illegitimate rights of the domain name´s owner. Also, in the LDRP proceeding there are several bases to prove bad faith and illegitimate rights, for example redirection, parking, inactivity, that are activities that do not imply to use of the mark in question.

The possibilities of bringing a successful infringement claim will significantly depend on the evidence that is submitted. It is advisable to certify the existence of the illegal use of the trademark in the website through a notary public, since the content of a webpage may be changed and it is important to have evidence that proves the infringement. It is important to note that certifications made by notary publics are vested with full faith and credit. In this manner, the owner of a trademark registration will be protected and able to prove infringement in case the infringer changes the content of its webpage, once summon is duly served or a cease and desist letter is delivered.

Further, the affected party can also claim damages from the infringer through a special procedure held before IMPI or a lawsuit before a civil federal or local Court. The law states that the amount of damages to be awarded will ascend at least to 40% of the sale price of each infringing good/service and will also consider the lost profits suffered by the affected party, the profits made by the infringer and the price the infringer would have paid for obtaining a license.

Finally, trademark owners in Mexico should take into account that a registration that is not used during three consecutive years by the owner or by the licensee of record will be vulnerable to a non-use cancellation action. Therefore, when evaluating the possibility of bringing an infringement action against athird party, it is important to verify that the mark has been used in accordance with legal requirements.

C. Complaint with an approved Registrar by NIC Mexico

As it was mentioned previously, the Registry responsible for administering the territorial domain name .MX (ccTLD) is NIC Mexico. Its main functions include providing information services and registration for .MX domain names and maintaining the respective database.

1. <u>NIC Mexico´s policy regarding false information</u>

According to NIC Mexico's policy, a third party that has a better right than the current holder over the ownership of a domain name may file a report in order to attempt the cancellation of the domain name. The report should state that the information provided by the owner of the domain name is false.

Once the report is filed, NIC Mexico grants a term to submit, by courier, physical evidence and/or documents available that demonstrate the falsehood of the information provided by the Registrant. The owner will have another term in order to provide correct information or evidence that proves that the information was accurate. If the documentation or evidence filed by the Registrant is not sufficient, NIC Mexico may proceed to remove the domain name, and at that time, the third party with a better right will be able to request and obtain the domain name.

2. Other bases for suspension or deletion

There are other bases for suspending or deleting a domain name by the Mexican Registry, namely:

a. The domain name was not paid by the registrar.
b. Upon the request of an authority.
c. If the Registry .MX needs to establish communication with the registrar in relation to a domain name and the latter does not respond within the required period of time. In such case, the domain name may be suspended or deleted.
d. If the registrant information and/or the contact information and/or the domain name information is not updated.
e. If the registrant and/or the contacts designated for the domain name fail to comply with the Base Policies of the Registry.

IV. CEASE AND DESIST LETTERS

Cease and Desist letters are a recommendable option when the transfer or cancellation of a .MX domain name is sought. The obvious advantage of these documents is that they may help to avoid incurring in the expenses of a LDRP or infringement proceeding; however, there are other advantages under Mexican practice.

A. Particularities

The format of a letter of consent for use in Mexico will not differ, in general, from the format of a letter used in other jurisdictions. Normally, the letter will include information regarding the person or entity on behalf of whom the letter is being sent, as well as the prior right it holds. Furthermore, it will describe the situation that led to its remission (e.g. the registration of a domain name that is identical or confusingly similar to a trademark of the sender), it will identify the remedies the sender has rights to and may seek. Finally, it will include the remedy the sender is seeking, this being usually the transfer of the domain name in its favor. A deadline for responding may be included in order to speed up the transfer or to determine the moment in which other actions should be considered.

However, under Mexican practice, the following particularities should be taken into account:

1. Previous cases have demonstrated that the correspondence between the parties can be decisive

In the wella.com.mx case, the Panelist decided that because the Registrant had agreed in a communication to the Complainant to transfer the domain name, said transfer should take place, even a final agreement had not been fully completed. The language of cease and desist letters should becarefully chosen to avoid acquiring undesired obligations.

2. Hiring a notary public is advisable if an infringement action is being considered

As mentioned previously, notary public´s certifications are vested with full faith and credit. The delivery of a cease and desist letter certified by a notary public will be presumed as a fact. Furthermore, itwill help in establishing that the infringing conduct was being knowingly committed. The Federal Law for the Protection of Industrial Property provides additional sanctions for infringers who acted knowingly.

V. PRACTICAL ADVICE AND PROPOSED STRATEGIES

Some points to consider when defining a legal strategy in a domain name related case are as follows:

1. Secure trademark rights in Mexico and secure relevant domain names

If interested in a .MX domain, consider registering trademarks in Mexico also. While Panels have not stated that having a Mexican trademark registration will be necessary for the defense or transfer of a .MX domain name, the existence of such a registration will be a very favorable factor.

Although a famous or well-known trademark does not have to b registered in Mexico, it is advisable to have a trademark registration that supports the notoriety of the mark and its exclusive right, since the Panelists in LDRP proceedings might consider that the character of famous must be declared by the Mexican Trademark Office and not by them.

When talking about e-commerce, it is of utmost importance. The online commerce keeps growing, and as such, the offer on the market for different products grows too and the importance of having a distinction on our products with it.

However, there is also another fact to consider. The territoriality principle establishes that the effects and rights granted by a trademark registration are valid only in the territory on which it was granted. However, in terms of international e-commerce, all sort of products are offered and digital IP rights infringements are committed in a larger scale, from abroad, without any barriers or territorial boundaries, which calls for right holders to be more aware of their IP assets and to take all the available actions to prevent infringers from profiting and free-riding on both their trademarks and efforts.

Under this scenario, two identical or confusingly similar trademark registrations might be perfectly valid in their respective territories as they were granted by the competent authorities, however if these two trademark owners carry out operations on each other’s countries then they might be infringing their respective trademark registrations.

The situation itself can be harmful for their trademarks in each other's country as advertising and offering similar products online with highly similar trademarks can compromise or cause confusion in the consumers regarding the quality and origin of the goods and services and might mislead the potential buyers to acquire one product when they were originally looking for another one.

On the other hand, the existence of confusingly similar domain names or identical ones that only change with regards to their extension can also be misleading and might cause confusion in the consumers, which in the end will also affect online merchants. In order to mitigate such risks many companies opt for registering several domain names containing their trademarks or company name with the most commons internet domain extensions (i.e. .com, .com.mx, .mx, .net, etc. depending on their target market) and by doing so they monopolize such domains (even though they are unactive) and prevent third parties from registering it and to engage into cybersquatting activities.

When the legitimate owner of the trademark or a company name arrives too late to the cyberspace and the domain names containing such words are already registered by a third party whether unintentionally or as a consequence of cybersquatting behaviors, the legitimate owner has to startproceedings to get those domains assigned or cancelled.

Fortunately, WIPO has been very aware of these risks and the proceedings to recover a domain name from an illegitimate owner are expedite and simpler than national Court proceedings (at least speaking from a Mexican perspective).

It is important to create awareness and improve existing domestic legal remedies and proceedings to be up to date with technological developments that allow right holders to defend their IP rights in a fast paced world with tendency to a full automatization and digitization. As a matter of fact, in marketplace companies, such as Amazon, sellers are not allowed to advertise or list their products unless they prove to have a trademark registration in the country where they are based. Another action taken by these companies to tackle infringers is the creation of brand registries for the people listing their goods or services within their websites.

2. Check for prior trademark rights

Trademark rights will serve as a basis to bring a LRDP. However, the disputed .MX domain registrant may also have trademark rights. Conducting a trademark search prior to taking action will help to add certainty to a possible claim and to avoid unexpected twists when start taking legal actions.

3. Evaluate trademark distinctiveness and use

As it is evident from the laboro.com.mx and laboro.mx case, Experts and Panels have plenty of leeway when assessing the merits of a claim, including determining if a registered trademark lacks distinctiveness. Assessing the distinctiveness of a trademark that will be used as base of a complaint or infringement action is recommendable.

When pursuing an infringement action, it should not be overlooked that the alleged infringer has the possibility of filing a counterclaim and challenge the validity of the trademark or to seek their cancellation on non-use grounds, which might lead and cause the plaintiff not only to lose the infringement action, but also to lose its registration if certain circumstances are met.

4. Consider other IP rights

In Mexico, the Copyright law provides the possibility of registering reservations of rights. These provide an exclusive right to use the titles or names of periodic publications, transmissions, symbolic or fictitious characters or people of groups engaged in artistic activities. There has been an ongoing debate in Mexico as to the relation of reservations of rights with trademarks and how they may become adversaryrights. The .MX LDRP includes the possibility of using other Intellectual Property rights, such as reservations of rights to bring a complaint.

5. Pay attention to differences between the UDRP and the .MX LDRP

As pointed out by WIPO in http://www.wipo.int/amc/en/domains/cctld/mx/index.html, the LDRP provides wider protection than the UDRP by including not only trademarks, but also slogans, reservations of rights and geographical indications in which the complainant has rights.

Furthermore, WIPO has noted that "whereas the UDRP requires the complainant to prove both that the domain name was registered and used in bad faith, under the LDRP it is sufficient to prove that either the registration or subsequent use of the domain name by the registrant occurred in bad faith."

6. Learn about local formalities

In Mexico, notary publics are important participants in the obtaining of solid evidence. The certifications made by notary publics are vested with full faith and credit. It is therefore advisable to consider hiring the services of a notary public to obtain certifications about the use of a domain name or about the content of a webpage associate with it. For instance, a notary public may certify the existenceof "domain for sale" banners in a webpage, which can be helpful in a finding of bad faith. Furthermore, a notary public may certify the existence of content in websites, which could be useful in case of an infringement action based on unauthorized use of trademarks or on unfair competition.

7. Obtain a price

When trying to obtain the transfer of a .mx domain, if there are signs that the registrant has the intention to sell it for more than out of pocket expenses, try getting an exact number in writing. This will facilitate proving bad faith.

VI. CONCLUSION

E-commerce has been growing fast since it was implemented and specially in the light of the current worldwide health crisis, which has caused traders to adapt their retail model to the current circumstances and to invest into digitization and in protecting their IP assets more than ever.

In that regard, it is important to have a unique and distinctive presence online which is accomplished by securing a domain name that matches and mirrors the registrant's trademark or corporate name and that will help to start building solid online positioning and brand equity.

The digital world and specifically e-commerce has been proven very effective and profitable, despite its own particularities and legal challenges. Legislations such as the Mexican Federal Law for the Protection of Industrial Property have acknowledged such situation and introduced sanctions and provisional measures in the digital world for those engaging into cybersquatting behaviors or infringements committed in the digital space.

Trademark owners, as well as other intellectual property right holders, have the possibility of bringing actions against third party who have registered .MX domains that may enter in conflict with their rights.

In most cases, the options will include the filing of a complaint with WIPO pursuant to the LDRP, the filing of an infringement or an unfair competition action, and/or filing a complaint with NIC Mexico. The viability and convenience of each alternative will, of course, depend on factors such as the manner in which the domain was registered and the use the registrant has made of same and moreover, the objectives sought by the affected party.

Cease and desist letters should be considered as useful tool before engaging any of these proceedings, because they can both help to avoid the expenses of complaints and litigation and they can serve as evidence in said proceedings.

The particularities of the Mexican practice and legal system should be analyzed and considered when evaluating a strategy aimed to obtain the cancellation, suspension or transfer of a domain name or to the bringing of an infringement action.

The enactment of the Federal Law for the Protection of the Industrial Property was a modernization of the Mexican IP regime and it will be both a challenge and an opportunity for Mexican Courts to construe and decide the cases based on these new provisions, considering the changes we have experienced due to the full digitalization global tendency.

Finally, the research behind this article has shown us that domain names are important intangible assets that are as valuable as trademarks that companies should be aware of to take advantage and make use of all the legal tools available to enforce their rights against online free-riders and infringers.

El impuesto a los robots

Valentín Ibarra Melero

Licenciado en Derecho por la Universidad Panamericana, con Especialidad en Derecho Fiscal y Maestría en Derecho Fiscal por dicha Universidad. Actualmente es socio en Chevez, Ruiz, Zamarripa y Cía con especialización en litigio fiscal y administrativo, incluyendo el derecho de la tecnología financiera (“Fintech”), materia que imparte en la Universidad Iberoamericana. Ha publicado artículos en revistas nacionales e internacionales especializadas, incluyendo diversos libros.

Ernesto Silva González

Ernesto Silva cursó la carrera de Derecho en la Universidad Panamericana y desde 2015, ha desempeñado su práctica profesional en Chevez, Ruiz, Zamarripa y Cía, donde actualmente es abogado senior con especialización en litigio fiscal y administrativo en diversos sectores. Ha publicado diversos artículos en revistas nacionales e internacionales especializadas.

Resumen

Actualmente la tecnología ha sustituido al ser humano en muchas funciones laborales que son desarrolladas por robots de manera más eficiente y económica, con lo cual, ha nacido la idea de crear impuestos a su uso, con la finalidad recuperar la recaudación que se ha perdido y, además, impulsar el trabajo humano en el futuro cercano.

La inteligencia artificial como catalizador para una nueva economía automatizada

A principios del siglo XIX ocurrió una gran conmoción en Inglaterra. Miles de artesanos ingleses denominados “luditas” comenzaron a destruir máquinas textiles instaladas por empresarios bajo el temor de que el uso de esta nueva tecnología tendría como consecuencia la extinción de sus puestos de trabajo.

La “rebelión de los luditas” no sería la última vez en la que existiría preocupación por la capacidad de máquinas de reemplazar a los seres humanos en sus funciones laborales, y las consecuencias macroeconómicas que esto podría tener.

Sin embargo, si analizamos la historia económica de nuestra especie considerando los efectos que han tenido los avances tecnológicos en los puestos de trabajo, podremos advertir que, a pesar de la implementación de todo tipo de máquinas que realizan actividades que el ser humano previamente realizaba, no ha existido una elevación radical ni sostenida en los índices de desempleo, ni mucho menos, esta implementación se ha reflejado en la extinción del trabajo humano.

Como lo señala el economista Henry Hazlitt, si bien la implementación de máquinas ha derivado en la disminución de ciertos puestos de trabajo (como podrían ser artesanos, agricultores y otros trabajadores de cuello azul), lo cierto es que dichos avances tecnológicos han dado lugar al auge de nuevas profesiones (ingenieros, programadores, analistas, entre otros).

En este sentido, ¿Cómo podría justificarse que, en algún punto, lleguemos a un estado en donde exista una automatización a gran escala? y, por lo tanto, ¿De qué forma podría justificarse la implementación de un impuesto a los robots?

Gordon Moore, co-fundador de Intel, advirtió en su obra “*Progress In Digital Integrated Electronics*” que la complejidad en los circuitos integrados se duplica cada dos años. Al crecimiento exponencial en materia informática hoy se le conoce como “La Ley de Moore” e implica que la tecnología no solamente aumenta su capacidad de procesamiento con el paso del tiempo, sino que también se vuelva más barata.

Los cambios exponenciales en la tecnología han dado lugar a la creación de la inteligencia artificial, la cual teóricamente tiene un potencial ilimitado para reemplazar al ser humano en la gran mayoría de las ocupaciones existentes actualmente, incluyendo aquellas de carácter complejo.

La inteligencia computacional, mejor conocida como “*inteligencia artificial*” ha sido definida por David Poole, profesor de la Universidad de British Columbia, como el “*estudio del diseño de agentes inteligentes*”. Un agente inteligente es “*un sistema que actúa inteligentemente. Lo que hace es adaptarse para sus circunstancias y su meta, es flexible en un cambio de entorno y de metas, aprende de la experiencia y elige opciones apropiadas tomando en consideración sus limitaciones perceptuales ycomputación finita.”*

Como lo señala la organización Deep AI, la inteligencia artificial se desarrolla a partir de técnicas de “*machine learning*” o “aprendizaje automático”, concepto definido como aquel “*campo de las ciencias*

computacionales que tiene por objetivo el enseñar a computadoras cómo aprender y actuar sin ser expresamente programadas para llevar a cabo acciones específicas. El aprendizaje automático es uno que utiliza el análisis de datos para construir y adaptar modelos, lo que permite a programas "aprender" a través de la experiencia".

Actualmente, se han desarrollado máquinas que funcionan con base en inteligencia artificial que, aprendiendo por sí mismas, son capaces de realizar actividades que previamente solo podían realizar los seres humanos. Existen numerosos casos en una gran variedad de materias y profesiones: desde recepcionistas y meseros robot en restaurantes de Japón, cajeros de chequeo automático en tiendas, el auge del comercio electrónico que rápidamente está ocasionando una pérdida de relevancia de tiendas físicas, la continua automatización en fábricas, hasta incluso, robots que componen música creados por plataformas digitales y que crean obras de arte como aquella pintura creada por Obvious que se vendió por £330,000.

El peligro de la automatización no se encuentra limitado a puestos de trabajo que funcionan a base de actividades "manuales y repetitivas" fáciles de programar, sino que se ha extendido incluso a profesiones "cognitivas". La inteligencia artificial ha ocasionado que actualmente existan softwares que de forma autónoma escriban artículos periodísticos, analizan y traducen documentos, efectúan análisis de datos e incluso, en el ámbito legal, redactan documentos.

Según un estudio publicado por el McKinsey Global Institute, en Estados Unidos el 55% de las actividades que requieren estudios menores a un diploma de educación secundaria pueden ser automatizables, mientras que dicho porcentaje es 22% para actividades cuyo ejercicio requiere undiploma universitario.

Asimismo, dicho instituto estima que algoritmos sofisticados tienen la capacidad de reemplazar aproximadamente a 140 millones de trabajadores que realizan actividades cognitivas, esto es, actividades complejas (en adición a aquellos que realizan actividades mecánicas o repetitivas).

Las conclusiones publicadas por McKinsey consideraron el nivel de desarrollo tecnológico actual, por lo que, en un futuro, es posible que los porcentajes de automatización aumenten considerablemente a medida en que la tecnología avanza cada vez más. Nick Bostrom, un investigador de la Universidad de Oxford, condujo un estudio con otros especialistas de la materia, quienes estimaron, en promedio, que existe un 50% de posibilidad de que para el año 2050 existan máquinas que posean un nivel de inteligencia igual al de los seres humanos.

En este sentido, surge la interrogante de si será conveniente que, en un futuro no muy lejano, se implemente una especie de gravamen o impuesto a este tipo de tecnologías a efecto de desacelerar de cierta forma el reemplazo de las personas por parte de las máquinas en sus puestos de trabajo, al mismo tiempo que se incentive el trabajo humano.

Ello, considerando que una automatización en gran escala podría ocasionar cuestiones preocupantes como pérdida de empleos, la necesidad de aumentar el gasto público para sufragar gastos de seguridad social cada vez mayores e, incluso, pérdidas potenciales en ingresos públicos derivado de una

disminución en la recaudación del impuesto sobre la renta e impuesto al valor agregado de los desempleados.

Propuestas tributarias actuales

En años recientes se ha discutido la posibilidad de implementar un impuesto a aquellos robots que reemplacen a los seres humanos en sus puestos laborales, lo cual, parte de la premisa de que el trabajo que realicen los robots debería ser gravado de la misma manera que el trabajo que desempeñan los seres humanos. Si, por ejemplo, alguien trabaja en un taller o una fábrica ganando unos 50 mil dólares al año, los ingresos que recibe la persona son gravados por el gobierno a una determinada tasa o tarifa. Si un robot realizara el mismo trabajo que esa persona, no existiría dicha tributación.

Es importante entender que esta teoría se ha generado en una época de rápido desarrollo tecnológico, en donde los avances en materia de inteligencia artificial podrían derivar, en un futuro no muy lejano, en un incremento en las tasas de desempleo, con la reducción correspondiente de los recursos tributarios relacionados con estas funciones.

Establecer medidas que graven el uso de este tipo de tecnología podría ser la clave para, por una parte, incentivar el uso de trabajo humano y, por otra, desacelerar el proceso de automatización laboral que ya ha comenzado desde hace varios años.

El impuesto al reemplazo del ser humano

Dentro de las múltiples propuestas tributarias que existen actualmente en relación con el uso de tecnología e inteligencia artificial, encontramos algunas que buscan implementar mecanismos que gravenel reemplazo de las personas en sus funciones de trabajo. El impuesto gravaría directamente a los negocios que adopten estas herramientas y, según los defensores de esta teoría, se justificaría en la medida en que el uso de tecnología automatizada además de generar desempleo, potencialmentederivaría en una mayor eficiencia, disminución de costos, aumento de productividad y, por ende, en mayores utilidades para los negocios que los adquieran.

Al tratarse de un tributo que grava el uso de máquinas en lugar de generar trabajos para seres humanos, nos encontraríamos ante una contribución con reglas y principios jurídicos propios, independiente de otros impuestos como el impuesto sobre la renta, el impuesto al valor agregado, entre otros.

Bill De Blasio, candidato a la nominación democrática a la presidencia de Estados Unidos y exalcalde de Nueva York, publicó en el periódico Wired una propuesta de impuesto a los robots que implicaba la creación de una agencia federal denominada *"Federal Automation and Worker Protection Agency"* que regularía cualquier empresa que incremente procesos automatizados y, por tal motivo, reemplazara a sus trabajadores, en cuyo caso, ésta se encontraría obligada a conseguir nuevos empleos a sus extrabajadores con la misma paga, o bien, pagarles una cuota de separación.

Asimismo, aquellas compañías que eliminaran puestos de trabajo y omitieran asegurar plazas de trabajo nuevas, pagarían un equivalente al impuesto sobre nóminas (*payroll tax)* de cinco años por cada empleo eliminado, con el fin de que dichos recursos sean utilizados para la creación de empleos.

Este tipo de impuesto se asemeja a lo que hoy se conoce como un tributo con una finalidad extrafiscal, pues en realidad no pretende gravar de manera directa las utilidades de la empresa, sino incrementar la tributación en aquellas empresas que, por la implementación de tecnología, pudieran generar una pérdida de empleos tradicionales.

El impuesto al uso de tecnología

Existen otro tipo de iniciativas que se encuentran enfocadas de manera directa al uso de robots como parte del proceso productivo, que buscan gravarlos como una entidad que, por si misma, puede ser sujeta a obligaciones tributarias.

Maddy Delvaux, integrante del Parlamento Europeo, ha propuesto una iniciativa que busca crear una especie de "personalidad jurídica" a cierto tipo de "robots inteligentes", obligando a las empresas a efectuar el pago de cuotas de seguridad social por su uso.

En el reporte presentado ante el Parlamento Europeo, se propuso clasificar como robots inteligentes a aquellos que tengan ciertas características específicas como la capacidad de adquirir autonomía a través de sensores y/o intercambiar datos con su entorno (interconectividad), analizar dichos datos, aprender a través de la experiencia e interacción, adaptar su conducta y acciones a su entorno, entre otras.

Maddy Delvaux propuso que los robots inteligentes sean registrados ante una agencia de la Unión Europea y que las empresas que los utilicen presenten un reporte revelando el número de robots inteligentes utilizados, los ahorros obtenidos por su uso y la proporción de aquellos ingresos obtenidos que se derive del uso de esta tecnología.

El impuesto consistiría en un pago de cuotas similares a las de seguridad social por cada robot utilizado.

Implementar un impuesto de este tipo a los robots conlleva diversos retos que tendrían que ser enfrentados por los legisladores al momento de establecer la mecánica del tributo, como definir con precisión qué debe considerarse un robot o qué tipo de tecnología sería objeto del gravamen, si es un impuesto aplicable a todo tipo de industrias y sectores sin distinguir las particularidades de cada uno de ellos, entre muchos otros.

El impuesto en contra del uso de tecnología

Existen otras posturas más radicales que tienen como finalidad primordial gravar el uso de tecnología e inteligencia artificial mediante el establecimiento de medidas que desincentiven su uso, promoviendo así el trabajo humano.

Estas propuestas buscan eliminar o limitar la deducción o los beneficios fiscales relacionados con la implementación de tecnología.
Actualmente, se busca incentivar la inversión en tecnología, ya que en términos generales su uso ha provocado un incremento en los niveles de productividad y la obtención de mayores utilidades que se reflejan en una mayor recaudación.

Sin embargo, existen ahora propuestas que sugieren eliminar cualquier tipo de estímulo fiscal a las empresas que utilicen ciertos tipos de tecnología, e incluso, llegan al extremo de recomendar la eliminación o cuando menos, limitar la deducción de las erogaciones relacionadas con su implementación, a fin de desincentivar de manera drástica la automatización de puestos de trabajo.

Corea del Sur fue el primer país en implementar una medida de este tipo al modificar el Decreto de Restricción de Tributación Especial, para reducir en dos puntos porcentuales ciertos incentivos fiscales que permiten acreditar contra el impuesto sobre la renta, algunos gastos relacionados con la adquisición de maquinaria y equipo informático que incrementen las capacidades de producción, llevándolos de un 3% o 7% dependiendo el tamaño de la empresa, a un 1% o 5%.

Dos años después, como consecuencia de indicadores económicos negativos relacionados con esta modificación, el gobierno de Corea del Sur parcialmente reversó parcialmente la acción tomada en 2017, incrementando en un punto porcentual el acreditamiento en cuestión.

Como se puede advertir, hoy en día existen múltiples teorías sobre la forma en que debe gravarse la implementación de tecnología, con características muy distintas entre ellas y, por ende, con ventajas y desventajas que pudieran ser favorables desde cierta perspectiva, pero trágicas desde otra, por lo cual, es importante continuar analizando la problemática y seguir buscando soluciones que encuentren un justo balance que permita regular, en una medida razonable, esta materia que, sin lugar a dudas, ya es parte de nuestra vida diaria.

Conclusiones

Es incuestionable que la tecnología y sus múltiples aplicaciones incrementan radicalmente la eficiencia y productividad de cualquier sector o empresa, lo cual, en términos generales debería generar un incremento recaudatorio en beneficio del Estado.

No obstante, también es una realidad que la implementación de tecnología necesariamente conlleva cierta tasa de reemplazo de la fuerza laboral tradicional, lo cual podría generar un incremento en el desempleo que será de distinto impacto dependiendo del tipo de sector y tipo de trabajo específico.

Esta realidad multifacética representa complejidades y retos que deben ser abordados desde distintas perspectivas, tanto laborales como tributarias y de seguridad social, pero siempre cuidando el respeto de derechos fundamentales, tanto de las empresas y patrones, como de los trabajadores.

Derivado de lo anterior, en el análisis de cualquier proyecto que pretenda gravar esta materia, es necesario encontrar un balance entre el cuidado de los empleos tradicionales y la necesidad de promoverel desarrollo tecnológico, pues de lo contrario, se corre el riesgo de llegar a extremos que podrían afectar gravemente la competitividad local e internacional de diversos sectores económicos alrededor del mundo.

Bibliografía

De Blasio B. "*Why American Workers Need to Be Protected from Automation*" Wired, 2019, recuperado el 31/10/20 de https://www.wired.com/story/why-american-workers-need-to-be-protected-from-automation/

Delvaux M. "*DRAFT REPORT with recommendations to the Commission on Civil Law Rules on Robotics*", Parlamento Europeo, 2016

Hazlitt H. "Economics in One Lesson" Currency, Estados Unidos,1988

Jung Min-kyung "*Korea to raise tax credit rate for corporate facility investments, R&D*", 2019, The Korea Herald, 2019, recuperado el 14/12/2020 de http://www.koreaherald.com/view.php?ud=20190725000653

Khatchadourian, Raffi "*The doomsday invention*" The New Yorker, 2015, recuperado el 10 de agosto de 2020 de https://www.newyorker.com/magazine/2015/11/23/doomsday-invention-artificial-intelligence-nick-bostrom

"*Machine learning*" Deep AI, recuperado el 10 de julio de 2020 de https://deepai.org/machine-learning-glossary-and-terms/machine-learning.

Manyika J. *et al*. "Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation", McKinsey & Company, Estados Unidos, 2017

Moore, Gordon E. "Progress in Digital Integrated Electronics" Intel, Estados Unidos,1975

Poole, David. "Computational Intelligence: A Logical Aproach": Oxford University Press, 1998

Swire M. "*Korea Enacts 2019 Tax Revision Bill*", Wolters Kluwer, 2019, recuperado el 12/12/20 de https://www.tax-news.com/news/Korea_Enacts_2019_Tax_Revision_Bill____97495.html

"*The robot that takes your job should pay taxes, says Bill Gates*" Quartz Media, 2019, recuperado el 31/10/20 de https://qz.com/911968/bill-gates-the-robot-that-takes-your-job-should-pay-taxes/

Inteligencia artificial: el enfoque europeo

Erick Clavel

Erick es abogado por el Tec de Monterrey, maestro por la Universidad de Chicago y candidato a doctor por la Universidad Panamericana con una investigación sobre medios digitales de solución de controversias.

Erick divide su actividad profesional en tres: dirige el despacho Clavel Abogados enfocado enlitigio civil, mercantil, arbitraje y competencia económica donde representa y asesora clientes nacionales y extranjeros. También dirige la empresa LawKit –una empresa de tecnología legal para abogados en donde mezcla el derecho con la tecnología para mejorar la práctica jurídica desarrollando aplicaciones de inteligencia artificial y análisis de datos. Finalmente, Erick es profesor de cátedra en el Tec de Monterrey Campus Santa Fe en la materia Títulos y Operacionesde Crédito en donde ha sido reconocido dentro del 1% de los mejores profesores de la institucióna nivel nacional.

Erick ha sido acreedor a becas para estudios de posgrado y ha recibido invitaciones para dar conferencias y publicar artículos en México, Estados Unidos y Europa.

***

La inteligencia artificial parece estar por todos lados. Virtualmente cada nuevo producto o servicio se mercadea como “asistido” o “impulsado” por inteligencia artificial o alguna variante similar. Desde un cepillo de dientes hasta un coche, pasando por servicios financieros o de comercio electrónico o incluso software de espionaje, *hackeos* y armas de guerra, nada parece escapar el alcance de esta tecnología.La inteligencia artificial ha permeado y cambiado muchos distintos ámbitos de nuestras vidas e indudablemente lo seguirá haciendo en el futuro con mayor profundidad y fuerza.

Pese a su ubicuidad en el mercado, el marco regulatorio de la inteligencia artificial es casi nulo. No hay reglas específicas para su desarrollo, pruebas, comercialización o responsabilidad sobre la misma. Cualquiera puede desarrollarla, usarla o comercializarla sin límite alguno independientemente de si su uso es benigno o maligno. La política pública de las naciones líderes en inteligencia artificial (China y Estados Unidos, principalmente) ha sido no intervenir con su desarrollo. Esto pudiera estar a punto de cambiar.

El 21 de abril de 2021, la Comisión Europea publicó la “*Propuesta de reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión*”. Esta propuesta es el reconocimiento de la Comisión que la inteligencia artificial tiene impactos importantes en nuestras vidas y que, como tal, debe tener reglas y límites. Esta propuesta es la Unión Europea en franco contrapunto de China y Estados Unidos.

Este artículo es un breve comentario a aspectos relevantes de lo que propone este reglamento, qué –en mi opinión– le faltó y a dónde nos llevará. Aunque esta apenas sea una propuesta, cualquier señal de la Comisión es poderosa y vale la pena analizarla.

I. Amplitud y aproximación de riesgo para la inteligencia artificial

La propuesta de reglamento parte de dos premisas esenciales: una definición amplia de "sistemas de inteligencia artificial" y una distinción de riesgo en su uso.

El reglamento define sistemas de inteligencia artificial como "*el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en* [un anexo del reglamento] *y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa*".

Esta definición es llamativa por su amplitud. El concepto legal bajo el reglamento no incluye sólo aquellos sistemas ultra avanzados que hemos visto en películas de Spielberg o leído en los libros de Asimov. Bajo el reglamento, un software sencillo que produzca recomendaciones o decisiones también es considerado inteligencia artificial. Es decir, tanto los robots más avanzados que utilizan esta tecnología para interactuar con su entorno como los sistemas más sencillos de software que automáticamente decide categorizar un correo electrónico como no deseado y mandarlo a dicha bandeja son inteligencia artificial. Reconociendo que hoy día está en todos lados, la Comisión comienza el reglamento aterrizando el concepto de inteligencia artificial para incluir a muchos más objetos, aplicaciones y, desde luego sujetos.

La segunda premisa es que no todos los sistemas de inteligencia artificial representan el mismo riesgo. Un coche autónomo no es igual al sistema personalizado de recomendación de películas. Dependiendo el uso y las implicaciones, hay distintos riesgos y, por ende, distintos niveles de regulación. Bajo el reglamento hay usos cuyo riesgo es inaceptable, usos de alto riesgo y usos de bajo riesgo. La propuesta se enfoca en mayor medida a los dos primeros.

A. Inteligencia artificial prohibida

La Unión Europea considera usos de riesgo inaceptable principalmente dos: primero, aquellos que pueden generar o incitar un daño físico o psicológico a una persona. Segundo, aquellos que pudieran tener como efecto discriminación social. En concreto, un ejemplo de la primera prohibición podría ser un chatbot que interactúe con personas y que, en dichas interacciones, los convenza de lastimarse olastimar a alguien más. El chatbot impulsado por inteligencia artificial no es el problema. El problema esel potencial uso que se le da.

Casos del segundo supuesto vienen específicamente en el reglamento. El primer caso son sistemas de clasificación social. Estos son sistemas automatizados que asignan una calificación a las personas sobre su comportamiento social –una persona con alta calificación tiene acceso a mejores servicios, créditos, productos, etc. Una calificación baja excluye el acceso a los mismos. Es decir, un especie de buró de

crédito pero para toda la actividad social. China, por ejemplo, está desarrollando un sistema del tipo que la Unión Europea Repudiaría.[12]

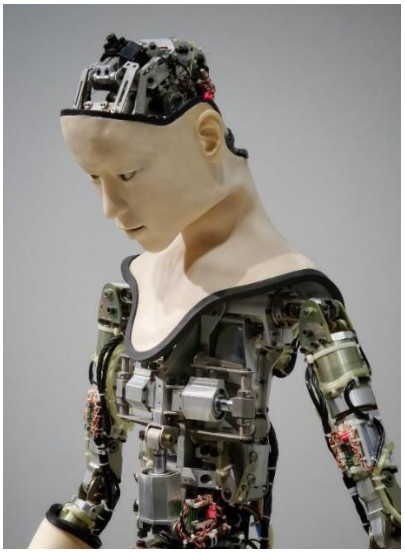
El segundo caso explícitamente mencionado es el uso de la tecnología en "identificación biométrica remota" en tiempo real. El mejor ejemplo de estos sistemas son los softwares de reconocimiento facial. Agencias de seguridad y justicia alrededor del mundo utilizan estos sistemas para encontrar a personas buscadas. Su funcionamiento es conceptualmente sencillo pero técnicamente complejo. Cámaras posicionadas en lugares públicos enfocan nuestras caras mientras pasamos frente a ellas. Estas cámaras transmiten nuestra imagen a un sistema que compara nuestras facciones con aquellas de las personas que están siendo buscadas. La comparación se hace a través de un sistema de inteligencia artificial que ha aprendido como distinguir una cara de otra a partir de analizar millones de caras, analizar y comparar sus factores distintivos: la distancia entre los ojos, los pómulos, la nariz y la boca, entre otros.[13]

La justificación del reglamento establece específicamente por qué este uso está prohibido. La tecnología de reconocimiento facial ha sido sumamente criticada por dos razones principales: primero, porque es una invasión severa a la privacidad. Estas imágenes habitualmente se capturan, transmiten y usan sin el conocimiento –y, menos, el consentimiento– de las personas.[14] Esto es una recolección indiscriminada de datos biométricos impermisible. Segundo, porque estos sistemas arrojan más falsos positivos para las personas de tez oscura que para las personas de tez clara provocando, claramente, un sesgo racial.[15] Cualquiera de estos dos motivos en lo individual es lo suficientemente pernicioso para justificar una prohibición de este uso de inteligencia artificial. Sorprendentemente, ésta no es una opinión global. Cuerpos de seguridad federales alrededor del mundo la permiten y usan sin reparo en estas consideraciones.

La Comisión Europea marca distancia de la postura de otras potencias en inteligencia artificial. Incurrir en una de estas conductas que en otro lado sería completamente legal, aquí sería multado con la pena que resulte mayor entre 30 millones de euros o el 6% de sus *ingresos corporativos globales* durante el ejercicio fiscal anterior a aquel en que incurrió la infracción. Así de claro el mensaje de la Comisión. Con este reglamento toma la obvia y correcta decisión de privilegiar la igualdad, la dignidad y la privacidad de las personas.

B. Inteligencia artificial de alto riesgo

[12] Kobie, Nicole. "The Complicated Truth about China's Social Credit System." WIRED UK, 6 Julio 2019, www.wired.co.uk/article/china-social-credit-system-explained. Consultado el 3 de julio de 2021.
[13] "The Facts on Facial Recognition with Artificial Intelligence." Amazon, aws.amazon.com/rekognition/the-facts-on-facial-recognition-with-artificial-intelligence/. Consultado el 3 de julio de 2021.
[14] Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." The New York Times, 20 Jan. 2020, 0-search-proquest-com.biblioteca-ils.tec.mx/newspapers/secretive-company-that-might-end-privacy-as-we/docview/2342910565/se-2?accountid=11643. Consultado el 3 de julio de 2021.
[15] Propuesta de Reglamento página 30, párrafo 33 de la Exposición de Motivos.



El segundo punto focal del reglamento es el uso de inteligencia artificial en actividades de alto riesgo. Específicamente, el reglamento indica que usos de alto riesgo se dan, entre otros, cuando la tecnología se utiliza como mecanismo de seguridad en productos previamente regulados como maquinaria o equipos médicos. Un ejemplo concreto son los sistemas anticolisión en los coches: esos sistemas que detectan cuando una persona o un objeto está en el camino de un coche mientras éste avanza y hace que se detenga antes del impacto. Claramente, la opinión de la Comisión es que estos sistemas deben estar regulados porque su uso compromete directamente la integridad de las personas.

El reglamento establece distintos requisitos para regular los usos de alto riesgo de la inteligencia artificial. Aquí algunos de los más relevantes:

Primero, el reglamento requiere que los desarrolladores de estos sistemas documenten perfectamente todos los aspectos del sistema: qué datos usan, cómo los usan, cómo se prueba y valida el sistema, su precisión, entre otros.[16]

Segundo, el sistema debe poder ser vigilado por un humano. En dicha vigilancia, el humano debe poder corregir cualquier sesgo en el producto del sistema e, incluso, poder detener el sistema o interrumpir su funcionamiento con una especie de "botón rojo".[17]

Tercero, se establece un deber de informar al usuario sobre sus interacciones con el sistema. Este deber de informar se extiende a indicarle también al usuario que el sistema podría deducir su raza, género, preferencia sexual o emociones o que el sistema puede manipular o producir material artificialmente –por ejemplo cuando se está frente a un video manipulado por un sistema que se hace pasar por un video de una situación real (llamados "*deep fakes*").

Cuarto, los desarrolladores o comercializadores de este sistema deben auditar el sistema continuamente para verificar el cumplimiento de los demás requisitos. Esta auditoria es interna y se debe realizar antes y después de lanzarlo al mercado pues estos sistemas, por su naturaleza "inteligente" pueden evolucionar con el tiempo y no obstante deben seguir cumpliendo con los requisitos.

Estos cuatro requisitos no son los únicos en el reglamento. Hay muchos más con matices y bemoles interesantes que se ajustan más a una tesis que a un artículo. Sin embargo, estos cuatro son suficientes para ilustrar que la Comisión Europea no permitirá más desgobierno en el desarrollo de la inteligencia artificial cuando el uso de la tecnología pueda tener altos costos sociales. La Comisión siempre tendrá un ojo vigilante sobre ella.

[16] Propuesta de Reglamento, artículos 10.2 y 11.1.
[17] Propuesta de Reglamento, artículo 14.

II. Qué hizo falta

El reglamento es exhaustivo sin duda. Sin embargo, hubiera deseado que cubriera algunos rubros que están ausentes y, particularmente, uno de fundamental importancia: la discriminación algorítmica.

La discriminación o sesgo algorítmico se da cuando los procesos que constituyen el sistema de inteligencia artificial perjudican a usuarios o un grupo de éstos con base en ciertas características como pueden ser condición social, raza, género, nacionalidad, preferencia sexual o cualquier otra. Dado que estos sistemas aprenden y evolucionan conforme se les alimenta de datos, puede ser que ese proceso evolutivo comience a generar exclusiones injustificadas hacia un cierto grupo de manera automática. La discriminación que desafortunadamente existe en nuestras sociedades análogas, también se puede dar en el mundo de los unos y los ceros.

El reglamento aborda los efectos de la discriminación algorítmica de forma indirecta. Un ejemplo está en la prohibición de la tecnología de identificación biométrica remota, como el reconocimiento facial en tiempo real. La discriminación de estos sistemas hacia personas con tez oscura está comprobada y por ende la Comisión lo proscribe terminantemente.[18]

Otra forma indirecta es cuando impone el requisito de supervisión humana. El humano puede detener el sistema cuando note que existe un factor de discriminación. Sin embargo, este requisito sólo existe para los sistemas de alto riesgo y la discriminación algorítmica puede existir incluso en sistemas que no son de alto riesgo. Por ejemplo, en los algoritmos que deciden qué información mostrar a uno u a otro usuario.[19] Ese también pudiera llegar a ser una instancia de discriminación con efectos graves. No obstante, estos sistemas no están calificados como de alto riesgo y, por lo tanto, no están sujetos a las exigencias explicadas en este artículo.

El problema está justamente en que el reglamento aborda tangencialmente la discriminación algorítmica. La propuesta le pone un alto sólo cuando se utiliza en un sistema de alto riesgo y no en sí mismo. Es decir, en términos del reglamento, la discriminación es mala como un accesorio, no como un principal. Esto no puede ser correcto. Un algoritmo que discrimina por género, preferencias sexuales, estatus socioeconómico o cualquier otra razón, es un problema en sí mismo. No obstante que la exposición de motivos así lo reconoce y anticipa la necesidad de abordarlo frontalmente, el reglamento –el que finalmente será la fuente legal– no lo replica. Una declaración expresa en el articulado hubiera dado mucho más fuerza al reglamento y hubiera sido en una clara invitación para que todos los desarrolladores, comercializadores y usuarios de esta tecnología inviertan esfuerzos en eliminarla.

[18] Najibi, Alex. “Racial Discrimination in Face Recognition Technology.” Harvard University The Graduate School of Arts and Sciences, 24 Oct. 2020, sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/. Consultado el 3 de julio de 2021.
[19] Dados los tiempos en los que vivimos, espero esto no sea sorpresa para nadie: no todos vemos la misma información en internet. La decisión sobre lo que vemos en una gran porción de las veces la toma un algoritmo con base en muchos factores. Estos factores pueden ir desde nuestro comportamiento en línea hasta nuestro comportamiento en el mundo físico. El punto es personalizar la información en la mayor medida posible para incrementar tráfico o uso de un determinado sitio, plataforma o aplicación.

III. Hacia dónde nos lleva

La propuesta todavía tiene un largo camino que recorrer. Los procesos legislativos en Europa son complejos e intricados. No obstante, el primer paso está aquí y ya ha comenzado a generar olas. En un mundo donde abundan los productos que usan inteligencia artificial desde hace años y donde las mayores potencias han optado por una política pública de absoluto *laissez faire*, la Comisión Europea flexiona su gran músculo regulatorio y propone una política distinta: detener el avance desbocado de la inteligencia artificial y procurar un avance controlado.

Este reglamento es una decisión de política pública difícil, controversial y con el sabor añejo que tienen todos los esfuerzos regulatorios sobre tecnología: ¿regular para mitigar riesgos aún y cuándo esto signifique ralentizar el desarrollo tecnológico y económico? La respuesta es dificilísima. Peor aún, ya que se tomó la decisión, cubrir un aspecto de la problemática muchas veces significa dejar otro lado descubierto. La escala de grises del problema es casi infinita. La Comisión Europea acaba de dar un valiente paso hacia el frente para invitar a la discusión y que valdrá la pena seguir de cerca en sus siguientes etapas. Lo que suceda en Europa abrirá un nuevo frente geopolítico sobre una tecnología que poco a poco se vuelve esencial para los mercados y, en general, la vida en sociedad.

Mercado Libre y sus herramientas para el combate a la falsificación y piratería

Juan Cichero

Desde Octubre 2019, Juan es el Head del Brand Protection Program de Mercado Libre. Antes de sumarse a Mercado Libre, trabajó casi 4 años en Philip Morris International (PMI) como Illicit Trade Prevention Manager para Latam y Canadá. Anteriormente, trabajó por más de 10 años en Nike como Brand Protection Manager liderando los esfuerzos de lucha contra la falsificación de las marcas de NIKE en Argentina, Bolivia, Chile, Paraguay, Perú y Uruguay. Juan es abogado recibido en la Universidad Católica de Argentina.

Guadalupe García Crespo

Desde el 1 de julio Guadalupe es Brand Protection Supervisor de Mercado Libre. Previamente estuvo a cargo de los asuntos de Propiedad Intelectual en el Departamento de Legales de Mercado Libre. Previo a sumarse a la compañía, fue asociada en el estudio Marval, O'Farrel y Mairal en Buenos Aires. Es abogada egresada de la Universidad de Buenos Aires y Agente de la Propiedad Industrial. Cursó la Maestría en Propiedad Intelectual de la Universidad Austral, actualmente elaborando su tesis. Completó el Programa de Derecho de Internet y Tecnología de las Comunicaciones de la Universidad San Andrés, y fue becada en 2019 para realizar el entrenamiento de la Oficina Japonesa de Patentes para profesionales de Propiedad Intelectual.

Resumen ejecutivo

- Mercado Libre es la plataforma tecnológica de comercio electrónico y fintech más grande de latinoamérica
- Actualmente opera en 18 países de la región, ofreciendo soluciones a particulares y empresas tanto para comprar y vender productos y servicios como para realizar pagos
- La prioridad de Mercado Libre es la confianza de sus clientes, por ello es primordial ofrecer productos originales y de calidad
-
- Por esta razón, Mercado Libre creó el **Brand Protection Program (BPP)** un programa para trabajar junto con los titulares de derechos de propiedad intelectual ofreciéndoles una herramienta para realizar denuncias y asimismo, aplicando mecanismos de moderación automática mediante el uso de tecnologías de *machine learning* con el objetivo de mantener una plataforma libre de productos falsificados y pirateados y ofrecer la mejor experiencia de compra a los usuarios.

Introducción

Mercado Libre es la plataforma tecnológica de comercio electrónico y fintech más grande de la región, con operaciones en 18 países de América Latina. Con más de 21 años de experiencia, Mercado Libre ofrece soluciones para que particulares y empresas puedan comprar, vender, ofrecer, enviar y pagar bienes y servicios a través de Internet mediante sus plataformas: Mercado Libre, Mercado Pago y Mercado Envíos.

Siendo el *shopping destination* #1 en la región, la principal prioridad de Mercado Libre es garantizar la mejor experiencia de compra para nuestros usuarios. En la búsqueda de este objetivo, Mercado Libre se esfuerza por generar credibilidad y confianza para cada actor que usa sus servicios y mantiene un fuerte compromiso para eliminar el flagelo de la falsificación y piratería de los sitios de Mercado Libre.

De esta forma, estamos constantemente ideando nuevas soluciones que les permitan a los titulares de derechos proteger su propiedad intelectual y sancionar así a quienes no cumplan con nuestras políticas.

El Brand Protection Program de Mercado Libre

Para Mercado Libre la confianza de los compradores es primordial para el funcionamiento de la plataforma. En este sentido, trabajamos junto a los titulares de derechos en la protección de su propiedad intelectual **para garantizar un espacio transaccional seguro y confiable para todos y asegurar así la mejor experiencia para todos nuestros compradores**.

En por ello que en el año 2000, (tan solo un año después de que Mercado Libre inicie sus operaciones), nace el “Programa de Protección de Propiedad Intelectual”, conocido también como “PPPI”, un programa que brinda a todos los titulares de derechos de propiedad intelectual la posibilidad de monitorear y denunciar publicaciones en supuesta infracción a sus derechos para que las mismas sean removidas del sitio, sean usuarios del marketplace o no.

A partir del año 2018, con el crecimiento de las ventas online en la región, Mercado Libre implementó ciertas medidas proactivas tendientes a remover vendedores maliciosos que operaban en la plataforma y al mismo tiempo introduce algunas mejoras en el proceso de adhesión al programa.

Sin embargo, en mayo de 2019 se produce un hito importante con el lanzamiento de una **herramienta mediante la cual los titulares de derechos pueden denunciar infracciones de una manera mucho más ágil y sencilla**.

Adicionalmente, ese mismo año, hemos comenzado a implementar paulatinamente **diferentes medidas proactivas para mejorar la detección de publicaciones** en presunta infracción marcaria, que incluyen el uso de inteligencia artificial (AI) y modelos de *machine learning* **que nos permite eliminar automáticamente de nuestra plataforma publicaciones que ofrecen productos falsificados o pirateados.**

En diciembre de 2019, renovamos nuestro programa con el objetivo de estar más cerca de las marcas y otros titulares de derechos pasándose a llamar **Brand Protection Program (BPP)**

Junto con la renovación del programa, hemos lanzado una página exclusiva www.brandprotectionprogram.com donde puede obtenerse más información sobre nuestro programa y cómo sumarse. Adicionalmente, los interesados podrán ver cuales son las principales ventajas del programa y de la herramienta de denuncias, tendrán acceso a los términos y condiciones del programa, a una sección de preguntas y respuestas frequentes, la posibilidad de descargar un toolkit sobre "*cómo defender tus derechos de propiedad intelectual en Mercado Libre*", así como también un acceso directo a la herramienta, entre otros.

La herramienta de denuncias

Las principales características de la herramienta de denuncias son:

- Está disponible en los 18 países en los que Mercado Libre opera.
- Se utiliza **una sola cuenta** para monitorear y denunciar publicaciones en los 18 países.
- Es **gratuita.**
- Permite que los miembros se registren y protejan todo su portafolio de derechos de propiedad intelectual, incluidas las marcas, derechos de autor, patentes y modelos de utilidad y los modelos y diseños industriales.
- Cuenta con un **procedimiento de notificación y remoción**, con la posibilidad de descargo por parte del vendedor.
- Permite realizar **búsquedas en tiempo real** en todos nuestros sitios, con la posibilidad de realizar denuncias individualmente o en forma masiva con tan solo unos clics.
- Permite **aplicar filtros especiales** y brinda la posibilidad de buscar con varios criterios que facilitan y hacen más eficiente la experiencia de denuncia.
- Cuenta con una **auditoría de vendedores**, para diferenciar los vendedores confiables de los sospechosos.
- Permite **crear y compartir informes** personalizados.

- Cuenta con una **herramienta de administración de casos** (proceso de notificación de respuesta) para realizar un seguimiento de las respuestas de los vendedores denunciados en el mismo lugar.
- Permite tener **varios perfiles** en una misma cuenta para trabajar en equipo.
- Está disponible en **inglés, español y portugués.**

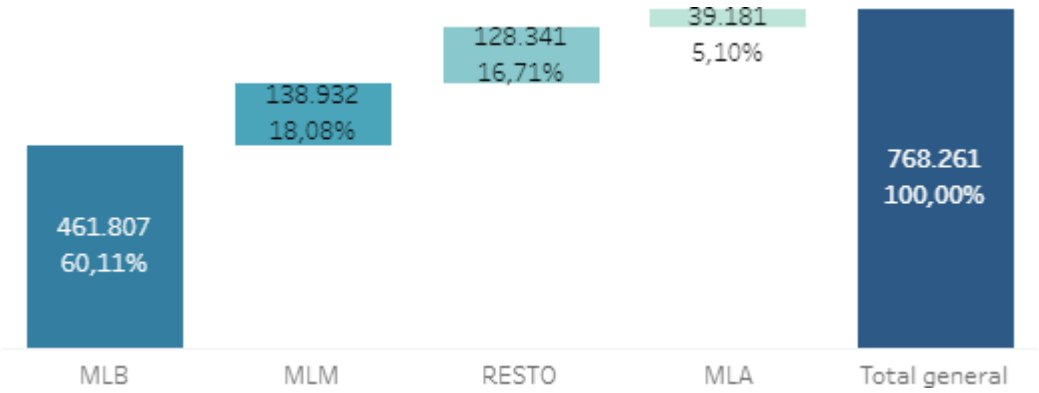
Acuerdos de colaboración

Desde Mercado Libre entendemos que aunar esfuerzos con asociaciones, cámaras y organismos del sector público, nos permite generar sinergias y ser más efectivos en la lucha contra la falsificación y la piratería.

En este sentido, Mercado Libre ha celebrado acuerdos de colaboración con distintas asociaciones, cámaras y organismos de gobierno en distintos países de la región, como ser, laCámara Argentina del Libro (CAL), Cámara Colombiana del Libro, Cámara Argentina de Productores de Fonogramas y Videogramas (CAPIF), la Agencia Nacional do Cinema (ANCINE-Brasil) y la Asociación Nacional de Broadcasters (ANDEBU-Uruguay) y, más recientemente, con el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) de Perú. Actualmente, también existen otros acuerdos en negociación en distintos países de la región.

BPP en números

- En la actualidad, el BPP tiene más de **5.400 miembros adheridos** y **más de 110.000 derechos de propiedad intelectua**l.
- Aproximadamente un **0,08% de las publicaciones son mensualmente denunciadas por los miembros del programa** por infringir sus derechos de propiedad intelectual. Esto es mínimo en relación a los millones de listados y operaciones que se realizan diariamente. Aun así, conscientes de que es una problemática que afecta a todas las industrias, nuestro objetivo es queen nuestra plataforma no se comercialice ningún producto en infracción.
- Durante el primer semestre de 2021, los miembros del programa denunciaron más de **768 mil** publicaciones mientras que Mercado Libre removió proactivamente más de **5 millones** de publicaciones en infracción.
- El mayor volumen de denuncias confirmadas se concentra en Brasil, que es el principal mercado de la región. **En el primer semestre de 2021, el 60,11% de las denuncias se concentraron en Brasil, seguido por México con el 18,08%** tal como puede apreciarse en el siguiente gráfico:



- Los principales motivos de denuncia fueron falsificación (42,6%), derecho de autor (15,16%), uso ilegítimo de marca (13,78% y software pirata (12,27%):

- Finalmente, **más de 14 mil cuentas** fueron inhabilitadas de manera permanente.

Conclusión

Para Mercado Libre, velar por la protección de la Propiedad Intelectual es un pilar fundamental. Trabajamos constantemente para que los usuarios sigan eligiendo y confiando en nuestra plataforma.

Toda infracción a la propiedad Intelectual afecta la reputación de las marcas afectadas, pero también a la nuestra, generando pérdidas para nuestra compañía además de afectar a otros actores, como ser el Estado que deja de recaudar impuestos y los consumidores que adquieren productos de menor calidad.

Y justamente, la implementación del programa nos ha permitido tener una mayor colaboración con titulares de derechos para combatir infracciones a su propiedad intelectual y redunda en beneficios para nuestros usuarios que pueden adquirir productos originales y seguros.

Por qué ahora más que nunca es relevante la ciberseguridad

Jimena Mora Corredor –
Directora de Seguridad Digital para Latinoamérica de Microsoft

Rebeca Servin Lewis –
Directora de Asuntos Jurídicos, Corporativos y de Filantropía de Microsoft México

Durante el 2020 vivimos de primera mano lo que desde hace algunos años intuíamos: cada vez somos más digitales. En cuestión de semanas vimos cómo muchas de nuestras actividades implicaron un incremento en el uso de tecnologías de la información; nuestro trabajo, estudio, compras, controles médicos e inclusos fiestas y reuniones tuvieron un jugador invisible que fue la tecnología. Lo que pensamos que sería una circunstancia de meses, se volvió la "nueva normalidad" y entendimos, como humanidad, que la transformación digital llegó para quedarse.

La situación en la que nos encontramos no tiene precedentes, la pandemia fue la "chispa" que impulsó la adopción exponencial de las tecnologías de la información. En México vimos cómo los empresarios y entidades educativas concretaron en meses la transformación digital que tenían prevista para implementar en años, y el tráfico de banda ancha que se presentó en tres semanas produjo el crecimiento que se esperaría que sucediera en un año completo. Sin duda, la pandemia apuntaló a la tecnología digital como una piedra angular de la sociedad moderna.

Pero, en muchos sentidos, las conversaciones sobre transformación digital que tenemos actualmente son similares a las que teníamos hace más de un año: el uso de la tecnología y su poder transformador no es nuevo; y los desafíos que implica tampoco lo son. Al final nos encontramos con la necesidad de cumplir con el reto de asegurar y proteger la tecnología que utilizamos. Entonces, ¿por qué ahora más que nunca es relevante la ciberseguridad?

Precisamente por el uso exponencial de las tecnologías de la información. A medida que más y más personas usan Internet, aumentando el número de dispositivos conectados, a medida en que cada vez más nuestra vida "física" se transforma en una vida digital, el ciberespacio se ve atraído por un mayor número de actores maliciosos que buscan hacer daño basado en todo tipo de motivaciones, además de que las amenazas de estos actores se han vuelto especialmente sofisticadas en los últimos meses, ya que tratan de aprovecharse de la confusión y las vulnerabilidades expuestas por la pandemia:

- El aprovechamiento e implementación de la tecnología, no suele ser tan simple como apretar un interruptor, y los nuevos usuarios acceden a las tecnologías sin entrenamiento y son expuestos a un enorme abanico de tecnologías.

- Listos o no, millones de personas se vieron empujadas a trabajar desde casa, lo que significa que ahora más personas están accediendo a datos corporativos sensibles a través de las redes domésticas y con dispositivos que no están preparados para enfrentar amenazas sofisticadas en ciberseguridad.

- Todos los países del mundo han visto al menos un ciberataque temático de COVID-19. Los atacantes incluyen datos para hacerse pasar por entidades de confianza como la Organización Mundial de la Salud (OMS) y otros grupos relacionados con la atención sanitaria con el fin de aprovechar su credibilidad para atraer a personas desprevenidas y lograr un "click" en enlaces maliciosos o que revelen información personal. Este vector de ataque es conocido como "phishing" y es el causante del 90% de las intrusiones informáticas que se presentan a nivel mundial.

- Y quizás las amenazas más siniestras -cuyo crecimiento es alarmante- que se han observado durante la pandemia son aquellas dirigidas contra jóvenes y niños. Los riesgos en menores son principalmente el cyberbulling (acoso cibernético), interacciones con contenido sexual y grooming (un adulto se pone en contacto con un menor de edad con el fin de ganarse su confianza para luego hacerlo participar en alguna actividad sexual online o en persona).

- Finalmente, el incremento en los ataques que se denominan ataques Estado-Nación que se producen por gobiernos contra civiles en aparentes tiempos de paz[20].

Estas situaciones nos hacen advertir cómo los temas de privacidad, seguridad y corresponsabilidad están estrechamente relacionados, teniendo como principales actores a las empresas de tecnología, gobiernos y ciudadanía.

Por una parte, las empresas de tecnología crean nuevas herramientas y soluciones para abordar los desafíos en seguridad, centrándose particularmente en un enfoque de "cero confianza" en el desarrollo de sus tecnologías; esto quiere decir que las empresas consideran a la seguridad como punto de partiday la integran en cada una de las etapas de desarrollo. De igual manera, la inteligencia artificial[21], *machine learning* y el análisis de datos permiten que las empresas de tecnología puedan identificar parámetros, algoritmos o conductas maliciosas y así prevenir, detectar y responder ante la ocurrencia de estos ataques. Este esfuerzo implica inversiones importantes por parte de las empresas de tecnología[22] para el desarrollo de sus productos o servicios, así como asociaciones con el resto de la industria para compartir inteligencia frente a los vectores de ataque y orientación frente a las posibles acciones de remediación. Asimismo, en realidad, son las empresas de tecnología las primeras en responder cuando un ciberataque ocurre, colaborando con sus clientes en la atención de los incidentes y en muchos casos en la

[20] Algunos ejemplos de este tipo son los ocurridos con Sony Pictures en el 2014 y las elecciones presidenciales de Estados Unidos en el 2016.
[21] Microsoft analiza más de 8 trillones de señales de seguridad diarias.
[22] Por ejemplo, Microsoft invierte $1 billón de dólares anuales en desarrollo de características de seguridad de sus productos.

coordinación de las actividades de remediación. Un punto importante para mencionar es que las actualizaciones de software suelen incluir “parches” y mejoras continuas de seguridad.

Los gobiernos son otro actor activo, cuya razón de ser es la protección de la integridad y patrimonio de las personas. En la experiencia internacional, países que han logrado una capacidad robusta en temas de seguridad, lo han conseguido al implementar programas, estrategias o planes nacionales de ciberseguridad, que involucran la colaboración de todos los actores (gobiernos, empresas y sociedad civil) y que no sólo establecen principios generales, sino que crean agencias especializadas en ciberseguridad que articulan e invierten en procesos de fortalecimiento de capacidades tanto personales como tecnológicas, con objetivos medibles y concretos a corto plazo. En México hay importantes casosde éxito basados en la colaboración conjunta de diversos sectores; por ejemplo, en su oportunidad el CERT, ISPS y Microsoft lograron hacer la disrupción de dos redes criminales informáticas, denominadas Neccurs y Trickbot cuyos objetivos eran robar datos personales de usuarios con propósitos ilícitos, y. promover noticias falsas.

Vale la pena mencionar la iniciativa del gobierno francés, de crear principios básicos para ser adoptados por los diferentes gobiernos, empresas y sociedad civil para promover un ambiente digital seguro, conocida como *“El llamado de Paris para la confianza y seguridad en el ciberespacio”*[23]. Se trata de la primera iniciativa diplomática que no sólo incluye a gobiernos sino a sociedad civil y empresas. El llamado de Paris cuenta con más de 600 miembros, en donde alrededor de 80 gobiernos (incluido México) se han adherido.

Por último y quizás el punto más importante son los usuarios. La pandemia nos ha hecho notar que todos necesitamos invertir en nuestra capacitación en el uso seguro de tecnologías de la información:

- Capacitación en el uso de herramientas tecnológicas: Todos debemos conocer las diferentes herramientas y funcionalidades de los productos y servicios para ser más eficientes en el mundo digital.
- Desarrollo de habilidades para la empleabilidad: Se estima que en Latinoamérica en los próximos cinco años, se crearán 149 millones nuevos empleos en campos como el desarrollo de software, la ciberseguridad y el aprendizaje automático.
- Civilidad Digital: Tenemos que complementar con programas de convivencia digital para que nuestros niños y jóvenes eviten situaciones de riesgo, tomen decisiones informadas y entiendan mejor cómo proteger su privacidad y así se conviertan en buenos ciudadanos digitales, desarrollando un sentido de propiedad y responsabilidad personal que les ayudará a tomar decisiones éticas en el mundo en línea[24].

Asimismo, los usuarios tienen que adoptar prácticas para evitar ataques y fraudes que comprometan su seguridad, como podrían ser:

[23] Paris Call for Trust and Security in Cyberspace — Paris Call
[24] Por ejemplo, el pasado mes de diciembre, Microsoft y CONALEP presentaron el e-book denominado “ESENCIALES EN SEGURIDAD DIGITAL” cuyo objetivo es crear una cultura de civilidad digital y concientizar e impactar a los niños y jóvenes respecto de las conductas, situaciones de riesgos y buenas prácticas en el entorno digital.

- Actualización de los sistemas de información. Más de la mitad de las actualizaciones en los sistemas operativos y de ofimática son para ofrecer mejores capacidades en seguridad.
- Uso de contraseña segura.
- Implementación de sistemas de doble autenticación.
- Educación sobre los riesgos asociados al uso de Internet: En muchas ocasiones somos nosotros mismos lo que nos ponemos en riesgo sin ni siquiera notarlo, ponemos nuestra información más sensible disponible en redes sociales, tenemos claves de fácil acceso y en muchas ocasiones hacemos click en archivos adjuntos sin ni siquiera considerar alertas mínimas como verificar el remitente.

Por otra parte, los gobiernos y las empresas de tecnología pueden tener las prácticas y los servicios más sofisticados, pero sin la adopción y concientización por parte de los usuarios, estos esfuerzos son insuficientes.

En conclusión, debemos hacer un frente común entre empresas, gobiernos y usuarios en donde cada uno participe en la adopción de tecnologías, implementación de políticas públicas, capacitación, etc. que nos permita tener un mundo digital más seguro.

ICC Policy Primer on Cybersecurity

INTRODUCTION

The private sector has and continues to assume significant roles and responsibilities in the development of information communication technologies (ICTs). As the representative of 45 million companies of all sizes and sectors in over 100 countries, the International Chamber of Commerce (ICC) is committed to ensuring that digital technologies work for everyone, every day, everywhere, in order to fully realise the potential of the digital economy and to safeguard proper functioning of critical infrastructures. While this was always an important goal, in the context of the current COVID-19 pandemic it is fundamental, as safe, secure and resilient digital networks are vital to maintain the proper functioning of our economies and societies and protect lives and livelihoods across the globe.

ICC works with governments and businesses worldwide to build a common understanding of what constitutes a robust cybersecurity policy given the proliferation/ever increasing tide of attacks and best practices in order to foster a more secure Internet for businesses and users.

With a hundred-year history of developing globally recognised applicable rules by convening experts and practitioners, ICC considers it essential that businesses and governments have

a shared understanding of how to conceptualise cybersecurity risks, targets, impacts, and responses, including national and international laws and norms. While governments and business have different roles in addressing cybersecurity, they are mutually reinforcing.

This policy primer highlights some of the main issues and challenges that businesses and society are facing. Part 1 of the paper presents a non-exhaustive list as a starting point to identifying key issues, so that all stakeholders can work together towards effective solutions. Part 2 of the paper outlines key areas where ICC and its members will develop further issue papers to provide further considerations, practical tools and policy recommendations for both private and public sector actors.

CONTEXT: The impact of cyber threats on business

With damage related to cybercrime projected to hit $6 trillion annually by 2021[25], businesses, policymakers and users struggle to keep up with rapidly evolving online threats. Today, cybercrime impacts all businesses regardless of size or industry or geographical location, with around 50% of all cyber attacks being committed against small and medium-sized enterprises (SMEs).[26]

The digital economy, the Internet, and the cross-border data flows that support it have already accounted for considerable GDP growth in many countries.[27] Arguably, the greatest economic impact of the digital economy comes from the digitalisation of traditional industry processes, as companies across all sectors seek to use technology to improve their business operations and models.[28] However, cybercrime threatens to thwart the potential economic impact of ICT and digital, as

[26] Cybersecurity Ventures (2017) Cybercrime Report
[27] McKinsey (2011) The great transformer: The impact of the Internet on economic growth and prosperity
[28] UNCTAD (2017) World Investment Report 2017: Investment and the Digital Economy

consumer and business express concern over cybersecurity.[29]

As the COVID-19 pandemic spread across the globe, many organisations started moving substantial parts of their operations online in order to ensure business continuity, protect workers and continue to serve customers. In the wake of the crisis, there has been an upsurge in the use of online and digital tools that created and continues to create new opportunities for malicious actors to take advantage of the disruptive effects of the crisis and target businesses, especially SMEs for cyber-attacks.

Even before the current crisis, the impact of cyber attacks was increasingly worrying. In 2019, the average cost of a data breach was USD$ 3.92 million.[30] A recent report suggests that small businesses are the target of over 40% of cyber-attacks with an average loss per attack of more than US$ 188,000.[31] Yet, the cost of cyber breach for business extends beyond just purely monetary damage, as the loss of trade secrets, privileged and proprietary information, or reputational damage could threaten to destroy a business altogether.[32] In the United States, 60% of SMEs are out of business within six months of a cyber attack.[33] As businesses across all parts of the traditional economy, from manufacturing to energy, seek to digitalise their operations as a way to increase competitiveness, this provides new opportunities for cybercrime to further expand, especially as state and non-state actors increasingly seek to target and disrupt critical infrastructure and systems.[34]

The borderless nature of the Internet, the digital economy, increased cyber-physical interdependency through IoT, and cybercrime paints a complex legal and operational picture for cybersecurity. Almost all sectors utilise ICT and rely on the Internet for everything from the simplest to the most strategic tasks. Global supply chains are increasingly interconnected, and the ICT systems along those supply chains have both internal and external devices meant to facilitate business operations. However, these interconnected systems create a complex landscape where combating cybercrime can prove particularly challenging, as malicious actors can easily exploit vulnerabilities in business processes and target individual employees across all parts of the supply chain. In addition to operational and behavioural risks, the technical manifestations of cyber attacks—from Malware to Ransomware to supply chain cyber attacks—are constantly evolving.

Furthermore, increased government investment in advanced cyber capabilities has in no small part driven the escalation of sophisticated attacks.[35] Reports suggest that more than 60 nations are now developing such capabilities[36] as the business community continues to be exposed to serious and growing cyber threats from state actors.[37] State-sponsored espionage has been

on the rise, with 20% of global businesses ranking it as the most serious risk to their business.[38] Many of today's most sophisticated cyberattacks have been attributed either directly to States or to

[29] Mckinsey (2015) Digitizing the value chain
[30] Ponemon (2019) Cost of a Data Breach Report
[31] Verizon (2019) Data Breach Investigation Report
[32] Eubanks (2017) The True Cost Of Cybercrime For Businesses. Council Post; Ponemon (2016) Cost of Cyber Crime Study & the Risk of Business Innovation
[33] Miller (2016) 60% of small companies that suffer a cyber attack are out of business within six months. Denver Post.
[34] McKinsey (2019) Unlocking the value of digital operations in electric power generation; UNCTAD (2017) World Investment Report 2017: Investment and the Digital Economy
[35] Hi-Tech Crime Trends 2018. Group-IB. Oct. 2018. https://www.group-ib.com/media/hi-tech-crime-trends-2018/
[36] Valantino-DeVries, Jenniter, Lam Thuy Vo, Danny Yadron. Cataloging the World's Cyberforces. Wall Street Journal. http://graphics.wsj.com/world-catalogue-cyberwar-tools/
[37] Council on Foreign Relations (n.d.) State-sponsored cyber operations tracker
[38] Businesswire (2017) Cyber Espionage Tops the List as Most Serious Threat Concern to Global Businesses in 2017

the actions of their proxies. Even attacks conducted by independent malicious actors are often a downstream consequence of government activity, as cyber capabilities proliferate quickly when they are stolen, sold, or otherwise repurposed to criminal ends. Increasingly, we are seeing advanced cyber powers sitting atop a toxic pyramid of malicious actors, with their tools and tactics proliferating downward and into a dangerous ecosystem of affiliated and unaffiliated threat actors with both political and criminal objectives.

At the same time, when it comes to cyber-attacks there are significant asymmetries between offenders and defenders in skills, tools and cost. Out of 10,000 attacks, the defender needs to be right10,000 times, while the offender only once, to be successful. Offenders oftentimes have a larger, better equipped toolbox compared to the defence capacities of businesses (especially MSMEs) and users. Cybercrime has a high pay-out ratio, with relatively small cost from the attacker, while defensive cyber-expenditures are considerably higher. Thus, businesses, consumers and users of technology are fighting a losing battle, without the support of governments both in the domestic and international realm.

Neither businesses nor governments can combat these borderless threats on their own.Cybersecurity is a resource intensive activity, tapping into both private and public sector reserves. As businesses and regulators both seek to find meaningful ways to mitigate cybersecurity concerns, collaboration is required in order to build awareness of vulnerabilities and incidents and to increase resilience against these complex, borderless cyber threats.

The private sector relies on a secure, stable and trustworthy policy and regulatory environment to foster opportunity, spur innovation, and create value for communities. Actions that undermine this enabling environment pose a threat not only to security, but also to economic development and livelihoods. It is therefore imperative that industry take part in international policy discussions on cybersecurity, for two main reasons.

First, a common interpretation of international law and norms is necessary to ensure legal certainty and the predictability of state behaviour, which in turn has a very significant impact on investment decisions and on the risks that companies can quantify in their multinational operations.

Second, due to the borderless and interconnected nature of both the digital economy and cyberthreats, national approaches to cybersecurity require international agreements and cooperation in order to work properly.

Tangible outcomes and concrete indicators that objectively reflect responsible state behaviour in cyber-space are needed. While the important issues regarding the process and norms that aim to provide conduits and mechanisms to achieve outcomes continue to be essential, there is an urgent need for measurable improvements on the ground. Defining shared outcomes, indicators and follow up procedures in the short and long term are critical. The private sector is best placed to inform policymakers of the uses and desired effects of such measures as well as to point out potential barriers that might impact their implementation.

PART 1: CURRENT CHALLENGES IN CYBERSECURITY

Lack of common understanding of cybersecurity threats and concepts

The impact of a cyber attack varies significantly due to the nature of the actor, the motive, the target and the threat category, as well as the frequency, the degree of success of an incident and the severity of the consequence. One of the challenges of fostering comprehensive approaches tocybersecurity is the lack of definition and common understanding of the types of threats.

This complexity and consistently changing environment makes conceptualising threats difficult, fragmenting approaches to cybersecurity and thus contributing to an environment where cybercrime can flourish.

A lack of common and effective interpretation of norms and laws

Collaboratively addressing cybercrime is important for creating effective global cyber resilience. While there have been a number of international and bilateral policy statements to restrain cyber attacks targeting enterprises and critical infrastructure, progress in developing and adopting international norms governing and binding states to responsible behaviour in cyberspace has been slow.[39]

At the international level

While many agree that laws offline should also apply online, currently there are major differences among States on the interpretation, applicability and implementation of international law. Without common understanding on how international law, in its entirety, is applied in cyberspace, there

is little hope for defining and enforcing accountability for responsible State behaviour in cyber space, and as a consequence, improving the trust landscape for all stakeholders is impaired.

Cross-border cooperation for cybercrime also faces its own challenges without common effective cross-border criminal investigation and prosecution that is consistent with the rule of law and international treaties, arrangements and international cooperation mechanisms. Arrangements and international cooperation mechanisms between enforcement agencies can often be an effective way to deal with cybercrime that crosses borders. Currently, the Convention on Cybercrime of the Council of Europe (Budapest Convention) is the only binding international instrument on cybercrime aimed at facilitating this level of cooperation. Mutual Legal Assistance Treaties (MLATs) whether bilateral or regional provide another mechanism to enable law enforcement to access data in other jurisdictions with greater efficiency. In this respect, the Convention on Transboundary Organised Crime also has an important part to play.

At the national level

Businesses rely on the support of government to ensure that the necessary laws are in place so that cybercrime activity is illegal. Governments should ensure similar criminalisation of specific cybercrimes and crimes committed in cyberspace to avoid the creation of ‘cybercrime havens’

Lack of cooperation or awareness of similar efforts across jurisdictions and regions poses further

[39] The Group of Governmental Experts is a UN-mandated working group on Advancing responsible State behaviour in cyberspace in the context of international security that has been working since 2004.See, UNGA Resolution 73/266.

challenges to the alignment of policies and regulations, that could help reduce uncertainty and foster trust in the digital ecosystem.

Deficiencies in capacity and confidence-building measures

First-time users and certain demographics (e.g. children, women) are most often affected by the impact of cybercrime, cyberbullying and other cyber risks. These groups and all other Internet users need to be able to identify risks and manage threats effectively to take advantage of the opportunities that the Internet offers.

From a business perspective, it is vital that a company—large or small, click-and-mortar or high- tech—be able to identify their cyber security risk and effectively manage threats to their information systems. At the same time, all business managers spanning from directors of small family business toexecutives of large multinational companies must recognise that absolute security is an elusive goal. Unlike many business challenges, cyber security risk management remains a problem with no easyfix available.

A critical dimension to consider is that many developing countries want and need technical assistance to create the legal, regulatory, and related infrastructure to support the development of a secure, trusted, rules-based digital environment. The need remains great: too many countries still do not have a CERT, data protection at law, cybersecurity legislation in force or national cyber strategies—and the related technical and practical infrastructure that is essential to support them.

The chilling effect of disproportionate regulatory responses

ICT supply chains are global. Integration and interdependence are key aspects of the digital environment that relies on compatible rules between national jurisdictions and global data flows to work seamlessly.

Further cooperation and efforts are needed to develop practices aimed at ensuring cybersecurity measures not only provides necessary protection, but also enable data driven innovations. Global cross border data flows enable both economic growth and societal benefits. Implementing cyber measures that disproportionately restrict cross-border data flows or reduce market access might negatively impact trade, investment, or innovation.

Security is an essential element of trust in new and emerging technologies and a factor that can impact any organisation connected to the Internet, but it is not a one-size-fits-all solution and thus not suited to narrow top-down prescription. As new technologies continue to develop and emerge,cybersecurity implications need to be considered on a case-by-case basis.

PART 2: RESPONDING TO CYBERSECURITY CHALLENGES

In order to address the above-mentioned challenges, ICC recommends that all stakeholders:

- work together to develop a common understanding among both private and public sector actors (at national and international levels) of cybersecurity threats, actors and approaches;
- recognise that international law applies in its entirety in cyberspace; based on this premise, governments, in consultation with all stakeholders, should adhere to agreed international norms as well as develop mechanisms to effectively implement those norms and consider, where appropriate, the development of new international norms and/or national legislation.
- work towards the introduction and application of national criminal policy aimed at the protection of businesses and society from cybercrimes.
- recognise the importance of greater cooperation between national governments in combating cybercrimes with well-functioning and tailored cooperation in criminal matters.
- work together to further expand capacity- and confidence-building measures; and
- consider cybersecurity measures and standards, as they relate to specific existing and emerging technologies, on a case-by-case basis in accordance with international norms and laws, through a risk-based approach.

Conceptualising cyber threats, actors and responses

In securing their own assets and operations and taking steps to protect users and clients, businesses increasingly understand the importance of implementing holistic cybersecurity risk management processes. Businesses constantly develop and deploy measures designed to ensure the security of networks, protect users, protect devices and protect the content residing on these networks from attack. Such measures include activities to not only identify and mitigate cybersecurity risks but alsoto detect, respond to, and recover from cybersecurity incidents or events.

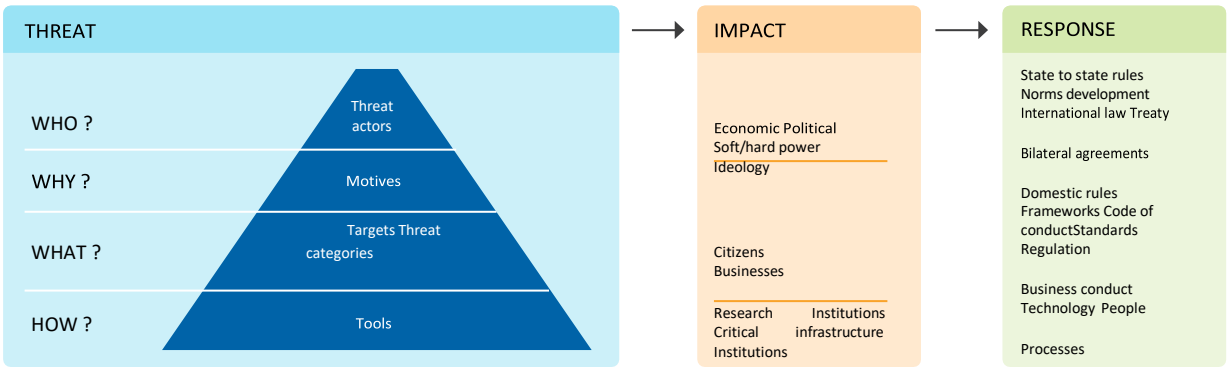
Given the constant threat and responses to cyber attacks, business approaches to cybersecurity, however, can only go so far and effective public-private cooperation is essential to strengthen Internet security and respond to the large and growing range of cybersecurity threats to the global Internet. It is essential that businesses and governments have a shared understanding of how to conceptualise cybersecurity threats, impacts, and responses.

Approaches to cybersecurity must be holistic and consistent across sectors and recognise critical interdependencies in both national and international contexts. As governments seek to promote and ensure sufficient use of effective approaches to cyber risk management, they should be cognisant of similar efforts across jurisdictions and regions and seek to align policies and regulations to the greatest extent practicable.

Globally aligned approaches to cyber risk management can facilitate interoperability and improve visibility and understanding among entities that have cross-border operations. Therefore, it is important that businesses and governments have a shared understanding of how to conceptualise cybersecurity threats, impacts, and responses. Figure 1 helps navigate a common approach to

cybersecurity.

Figure 1. *A common approach to cybersecurity*



Developing and implementing shared norms

While business must be proactive in securing their own assets and operations and taking steps to protect users and clients, they should also be able to count on the support of governments to ensure that the necessary laws are in place and implemented to guarantee that certain cybersecurity events are illegal.

With this in mind, ICC urges governments to implement and adhere to norms that have previously been agreed in UN discussions, as well as to develop mechanisms to effectively implement those norms.

As a first step, governments should start by complying with established international norms and/ or, as needed to increase clarity, develop recognised global norms and practices in collaboration with relevant stakeholders. For example, governments can:

- Develop recognised international norms that promote a stable ecosystem, in collaboration with industry.
- Improve understanding of and consensus regarding the ways in which existing international law govern state behaviour online.
- Leverage previous agreements on norms to provide a roadmap for future discussions and establishment of more specific standards that protects cross-border data flows and free expression. This should also include the commitment for states to consistently prevent any form of cybercrime emanating from its territory and prohibit offensive use of cyber by State actors in peace time, including cyber-enabled, state-sponsored theft of business confidential information and disruptions of critical infrastructure[40].

Business supports the norms agreed by the UN Governmental Group of Experts in 2015 and looks forward to contributing to their implementation and to further strengthening these norms.

In addition, the private sector has already supported, collaborated on, and launched initiatives to

[40] World Economic Forum: Global Risks Report 2018 http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

promote ambitious norms for responsible uses of technology, such as the Global Forum on Cyber Expertise, the Cybersecurity Tech Accord, The Paris Call for Trust and Security in Cyberspace or the Internet Society MANRS initiative, to name a few. We will continue to support such work going forward and will support information sharing and cooperation among such initiatives.

When it comes to fighting cybercrime, governments can implement mechanisms to coordinate international law enforcement efforts and facilitate investigation and extradition processes. The Budapest Convention is the only binding international instrument specifically on cybercrime, and States could consider becoming a signatory to the Budapest Convention or using it as a guideline for developing comprehensive national legislation. States should also take advantage of the Convention on Transboundary Organised Crime to improve mutual legal assistance with respect to cybercrime. Governments can also consider establishing bilateral or regional Mutual Legal Assistance Treaties (MLATs), which enable and facilitate cross-border law enforcement cooperation, while maintaining sufficient protections for privacy and security.

As governments seek to promote or ensure sufficient use of effective approaches to cyber risk management, they should be cognisant of similar efforts across jurisdictions and regions and seek to align policies and regulations to the greatest extent possible. Such approaches also ensure that all local organisations can access best-in-class technologies, services, and security offerings and expand their operations, either by directly growing across markets or by integrating into offerings of cross-region suppliers.

Enhancing capacity building

Increased awareness about cybersecurity and knowledge about how to protect networks can strengthen not only individuals, businesses and communities but also the ability of a whole country to protect critical digital infrastructure and combat cyber threats. This has never been more clear than during the Covid-19 crisis. The maturity of cybersecurity capacity in a country encourages confidence in the online environment and fosters meaningful access by all groups in society, thus helping address digital divides.

ICC has a proud, hundred-year history of providing companies with tools and self-regulatory guidance to promote good business practice. ICC's Commission on the Digital Economy developed a simple, clear guide in 2015 to help business play their part in addressing the increasingly serious challenge of cyber security. The ICC Cyber security guide for business is informed by global cyber security guidelines and national strategies and presents five principles that help enterprises identify cyber security risks and, drawing on various sources and best practices, goes on to pinpoint six key actions that companies should implement.

ICC also recently partnered with the Cyber Readiness Institute (CRI), a non-profit initiative that convenes senior business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium- sized enterprises. Through this partnership, ICC will work to make available the CRI Cyber Readiness Program to all our 45 million members of all sizes and sectors worldwide looking to protect themselves from digital threats.

That said, many countries do not have the fundamentals in their legal codex: data protection

frameworks are missing in dozens of countries; many do not have a CERT/CSIRT, and cybercrime and other cyber legislation is outdated, or entirely missing, in others.[41]

There is a need for much greater capacity building to ensure basic legal and infrastructure to build cyber trust and enable participation in global cybersecurity efforts.

Cybersecurity applications and standards

Trust and confidence in the availability, reliability, and resiliency of information systems and networks, including the Internet, must continue to be strengthened in order to fully realise ICT- enabled economic growth and ensure the seamless operation of global business. All stakeholders must work together to promote effective cyber security practices and the open, secure, stable, resilient, and globally interoperable Internet.

Efforts should be made to both highlight the importance of the issue and encourage continued research, innovation and deployment of context appropriate security solutions. As security solutions are implemented, due regard should also be paid to assure that security measures are consistent and proportionate with the related risks and desired results and consider interoperability across various technology implementations.

In a situation that requires a regulatory response at a national level, proportionality can be achieved by first, assuring good estimates of the impact of cyber attacks on businesses and societies. Second, when considering appropriate (regulatory targeting) and effective (net benefit) regulatory interventions, proportionality can be achieved by balancing the impact of cyber attacks with theprivate and public resources required to strengthen resilience throughout the entire value chain as costs can become prohibitively expensive for smaller organisations.

When considering cyber legislation, states must try to balance the benefits of trade, investment and innovation against genuine national security concerns. In the rare case that national security requirements need to be considered, States should seek to implement measures that are transparent, predictable, proportionate, and not a disguised restriction on trade.

Cyber security standards can often be best achieved through self-commitments of market participants, and various initiatives and cooperation groups already have been set up. Security testingshould be permitted in a manner that facilitates the adoption of Common Criteria (see, e.g. https://www.commoncriteriaportal.org/) and is consistent with existing applicable law. The common standardisation approach enables dynamic adaptation, in order to adjust and take into account technology changes, diverse threats and risk scenarios.

[41] For more details see the Global Cyberlaw Tracker kept by the UN Conference on Trade and Development, at https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commercelegislation-worldwide

CONCLUSION

To achieve positive results, governments should collaborate with other stakeholders to promote a culture of security, with appropriate legislation in place to combat cybercrime. Similarly, appropriate policies and legal frameworks related to data protection and privacy are also essential to ensure that consumers and citizens can continue to trust ICTs and use online services.

Multistakeholder collaboration promotes shared understanding of the multifaceted impact of cyber attacks and helps build consensus on the ways in which existing international law governs nation- state behaviour on the Internet. These exchanges will reflect ongoing learnings on the evolving threat environment and help promote a holistic approach to cybersecurity risk

management. Expert forums such as European Cybersecurity Industry Leaders, 3GPP SECAM, the OECD's Working Party on Security and Privacy in the Digital Economy and the Forum of Incident Response and Security Teams are commendable efforts providing detailed guidance on ways to conceptualise and understand threat actors, tools and technical manifestations. Additionally, national and regional Computer Incident Response Teams (CIRTS) can act as a convener for stakeholders and enable education and best practices on cybersecurity issues.

Effective public-private cooperation is essential to strengthen Internet security and respond to the large and growing range of cybersecurity threats to the global Internet.

ABOUT THE INTERNATIONAL CHAMBER OF COMMERCE (ICC)

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 100 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

International Chamber of Commerce (ICC)

- La ICC, con sede en París, se fundó en 1919, y hoy comprende una red global de más de 45 millones empresas, cámaras de comercio y asociaciones empresariales en más de 130 países, generando más de 1,000 millones de empleos. Nuestra visión es lograr un mundo donde la paz, el crecimiento económico sostenible y la prosperidad compartida, se sustenten en comercio justo, basado en reglas, así como inversión sostenible y respetuosa de los derechos humanos

- 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. Tenemos una estrecha relación con el G20, la OMC, y la OCDE, entre otros organismos.

- 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

❖ International Chamber of Commerce México (ICC México)

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.

Página web www.iccmex.mx