ECIJA
Torre Mural. Av. Insurgentes Sur 1605 piso 10
Col. San José Insurgentes, C.P. 03900,
Ciudad de México, México
Tel: (+52) 5556626840
www.ecija.com

¿Por qué el FBI está investigando a ZOOM? anotaciones sobre privacidad y ciberseguridad en el contexto de las plataformas digitales de videoconferencia en México.

Este documento consta de cuatro partes. La primera provee una introducción y síntesis sobre los hechos analizados, la segunda aborda consideraciones sobre el marco regulatorio en materia de privacidad y ciberseguridad, la tercera analiza las obligaciones contractuales y regulatorias que derivan de este modelo de negocio, finalizando con un cuarto apartado de conclusiones.

I. Introducción

La pandemia del coronavirus ha generado que se suspendan la mayoría de las labores, escuelas y prácticamente todas las reuniones presenciales de grandes y medianos grupos de personas, provocando un incremento masivo en el uso de las plataformas de comunicación a distancia, tales como lo son: Zoom, Google Meet, Microsoft Teams, Skype, entre otras.

El incremento desmesurado en las plataformas digitales colocó a varias de estas en la mira de diversas instituciones internacionales, como lo es el FBI (*Federal Bureau of Investigation*) por problemas relacionados con protección de datos personales, privacidad y ciberseguridad.

El Departamento de Seguridad Nacional de los Estados Unidos (*U.S. Department of Homeland Security*), emitió un comunicado relativo a las amenazas que se presentan ante la ciberseguridad en las plataformas de comunicación a distancia, haciendo referencia en particular a las aplicaciones de Zoom y Microsoft Teams, respectivamente.

Tras las investigaciones anteriormente mencionadas, la plataforma de Zoom comenzó a tomar medidas para la corrección de los problemas que se habían suscitado [1], tales como el "zoombombing", que se refiere al ingreso de terceros extraños a las conferencias en la plataforma, ya sea en reuniones, clases virtuales, o en el ámbito laboral; la actualización de las políticas de privacidad, con el fin de mostrarse más claros respecto a los datos que recolecta la aplicación; así como evitar la recolección de información innecesaria de la cuenta de Facebook de los usuarios.

II. Consideraciones Normativas sobre Privacidad y Ciberseguridad

A consecuencia de la contingencia sanitaria, el memorandum que *Homeland Security* publicó con motivo del uso de plataformas digitales para el teletrabajo[2], advirtió los severos riesgos de seguridad que el uso de éstas contrae, identificando principlamente cuatro prácticas maliciosas: *(i)* phishing, *(ii)* distribución de malwares, *(iii)* cibertaques a las comunicaciones, y *(iv)* registro de dominios de internet con palabras relacionadas al como COVID19 y coronavirus, de uso cuestionable.

[1] Zoom (2020); "*A Message to Our Users*", 1 de Abril de 2020, del Blog Oficial de Zoom; Sitio web: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/
[2] Para conocer el documento completo, acceder a la siguiente liga oficial: https://www.us-cert.gov/ncas/alerts/aa20-099a

Desde un análisis a luz del derecho mexicano, cabe mencionar que toda empresa que ofrezca servicios presenciales o en línea, puede operar en México a través de personas morales constituidas en México, o bien, mediante sociedades extranjeras autorizadas para operar en nuestro país[3], en términos de la Ley de Inversión Extranjera.

Asimismo, primeramente deberán contar con los sistemas de seguridad suficientes y políticas de privacidad que aseguren al usuario de las plataformas que su información se encuentra debidamente resguardada ya que, de lo contrario, serían responsables directamente por cualquier mal uso de ésta.

El primer mecanismo de prevención de riesgos legales, es la clara comunicación de los términos y condiciones de uso de las plataformas. El caso Zoom es aleccionador, ya que todo derivó de un mal manejo de esta información, tal y como lo reconoció la misma plataforma[4].

Considerando que dichas plataformas manejan un cúmulo de información considerable y que por su contenido puede considerarse sensible y personalísima, en México estas empresas están sujetas a un régimen de obligaciones específicas, contenidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Dicha norma, entre diversas obligaciones que impone a quienes tratan datos personales, regula el denominado **aviso de privacidad**, que constituye el documento mediante el cual al usuario se le da a conocer el uso y tratamiento de su información. Dicho aviso, presume la existencia de una expectativa razonable de privacidad.

En consecuencia, si los términos y condiciones del aviso de privacidad de cualquier plataforma, falsea u omite información relativa al encriptamiento y resguardo de la información vertida en las videoconferencias sostenidas a través de la plataforma, se estaría entonces frente a una **falta en materia de privacidad y tratamiento de datos personales**, al omitir información en el aviso de privacidad y el vulnerar la seguridad de bases de datos, locales, programas o equipos.

Asimismo, las disposiciones a seguir en materia de ciberseguridad por parte de estas plataformas, es prioritario. Sin embargo, en México, la escasez de especialistas y regulaciónhace compleja esta labor, toda vez que el marco legal aplicable sería el establecido por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En este sentido, cabe destacar que dicho marco regulatorio al ser insuficiente en materia de ciberseguridad, exige acudir a la regulación internacional para su debida comprensión y dimensión, como lo es el caso del Convenio sobre Ciberdelicuencia o Convenio de Budapest[5], y el Convenio Iberoamericano de Cooperación sobre Investigación y Aseguramiento de Prueba en Materia de Ciberdelincuencia de los Estados miembros de la Conferencia de Ministros de Justicia de los Países Iberoamericanos[6]. Sin embargo, desafortunadamente, a la fecha ninguno de los dos instrumentos internacionales han sido a la fecha ratificados por el Estado Mexicano.

---

[3] En términos del artículo 15º del Código de Comercio, aquellas" *sociedades legalmente constituidas en el extranjero que se establezcan en la República, o tengan en ella alguna agencia ó sucursal, podrán ejercer el comercio, sujetándose a las prescripciones especiales de este Código en todo cuanto concierna a la creación de sus establecimientos dentro del territorio nacional, a sus operaciones mercantiles y a la jurisdicción de los tribunales de la Nación*".

[4] Zoom (2020); "*The Facts Around Zoom and Encryption for Meetings/Webinars*", 1º de Abril de 2020, del Blog Oficial de Zoom; Sitio web: https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/

[5] Es el único tratado internacional vinculante en la materia y constituye una especie de acuerdo marco para que los Estados Parte implementen dentro de su ordenamiento jurídico la legislación pertinente para investigar y perseguir penalmente aquellos delitos cometidos en contra de sistemas o medios informáticos, o mediante el uso de los mismos, y faciliten la cooperación internacional.

[6] Instrumento internacional cuyo objetivo es la cooperación para adoptar medidas de aseguramiento y obtención de pruebas en la lucha contra la ciberdelincuencia.

Una de las medidas que se desprenden de los instrumentos internacionales referidos en líneas anteriores son la tipificación de ciertos delitos, a saber: *(i)* delitos cometidos contra la confidencialidad, integridad y disponibilidad de sistemas y datos informáticos, *(ii)* delitos cometidos mediante el uso de las tecnologías de la información y las telecomunicaciones (fraude y falsificación informáticos), *(iii)* delitos por su contenido (pornografía infantil) y *(iv)* delitos en materia de derecho de autor.

Con respecto a los **delitos cometidos contra la confidencialidad, integridad y disponibilidad de sistemas y datos informáticos**, en México encontramos que éstos, si bien no están tipificados de la misma manera, acciones delictivas similares son sancionadas en el Código Penal Federal, bajo el rubro de revelación de secretos y **acceso ilícito a sistemas y equipos de informática.** El ordenamiento penal prevé como delito el que una persona sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sean propiedad del Estado o del sistema financiero nacional, o bien, que teniendo autorización para ello modifiquen o destruyan dicha información injustificadamente.

III. Implicaciones Contractuales y Corporativas del Modelo de Negocio

Derivado de lo anterior, la operación de un modelo de negocio como el de Zoom, Microsoft Teams, o cualquier plataforma similar, ya sea a través de sociedades legalmente constituidas en México o bien mediante sociedades extranjeras autorizadas para operar en nuestro país, necesariamente implica rigurosos controles contractuales y corporativos para evitar contingencias legales, que pudieran llegar a ser cuantiosas.

Primeramente, el aviso de privacidad de estas plataformas exige una redacción cuidada y detallada; así como el implemenar las medidas de seguridad respectivas para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, cuando éstas plataformas sean utilizadas por entes públicos, en términos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Asimismo, considerando las implicaciones que las faltas en estas materias pueden ocasionar a las empresas que desarrollen u operen dichas plataformas, éstas pueden ser causa de responsabilidad penal, debiendo en consecuencia contar con una **política de integridad corporativa y un órgano de control permanente**, encargado de verificar el cumplimiento de de dichas políticas encaminadas a acciones de prevención delictiva, a efecto de tener derecho a los beneficios que la misma ley establece.

Consecuentemente, contar con un oficial de cumplimiento especializado en el marco normativo ya descrito, resulta esencial (como el modelo que actualmente se está ya desarrollando para instituciones de tecnología financiera), sobre todo si consideramos el desarrollo exponencial de las tecnologías de la información y la frecuencia del aumento en el uso de éstas.

Asimismo, implementar **códigos de ética** dentro de estas empresas (similares a los exigidos en materia de telecomunicaciones) es una medida adicional útil y efectiva, sobre todo si mediante éste se brinda un tratamiento innovador a los servicios de comunicación digital desde la óptica de los **derechos digitales**[7], entendidos éstos como la prolongación de los derechos de la ciudadanía (derechos humanos), pero llevados al mundo digital, pudiendo servir en consecuencia como mecanismos de debida diligencia corporativa para contener y prevenir posibles reclamaciones judiciales por potenciales violaciones a derechos humanos.

IV. Conclusiones

Toda plataforma de servicios digitales puede operar en México, mediante una persona moral legalmente constiuida en términos de las leyes mexicanas, o bien, a través de una sociedad extranjera en términos de la Ley de Inversión Extranjera.

La falta de conciencia y cultura de prevención por parte de las Empresas, es la mayor vulnerabilidad que existe en materia de ciberseguridad, privacidad y protección de datos personales.

En consecuencia, el desarrollo de políticas de contratación claras, integrales y actuales en la prestación de servicios de interconexión digital por videollamada, resultan imprescindibles para evitar contingencias legales por violaciones a la privacidad de los usuarios, tratamiento negligente de datos personales, en su caso, y participación en la comisión de ciberdelitos.

Asimismo, el desarrollo de programas de integridad, control y cumplimiento en estas materias (privacidad y ciberseguridad), resultan herramientas indispensables para la prevención efectiva de riesgos legales asociados con el modelo de negocio de las plataformas.

Finalmente, implementar un tratamiento desde la perspectiva de derechos humanos de la privacidad y la protección de los datos personales de los usuarios o clientes de la empresa, según sea el caso, resulta indispensable para eficientar los resultados de los programas de compliance en la materia de la empresa, toda vez que las faltas en la materia, no sólo traen aparejadas responsabilidades penales, administrativas y civiles, sino también pueden ser equiparables a violaciones de derechos humanos.

ECIJA México, S.C.

Joaquín Rodríguez
(jrodriguezz@ecija.com)

Ricardo Chacón
(rchacon@ecija.com)

Adalberto Mendez
(amendez@ecija.com)

Berenice Sagaón
(bsagaon@ecija.com)

[7] A saber: *(i)* acceso universal e igualitario a internet, sin discriminación de ningún tipo, *(ii)* libertad de expresión, información y comunicación, *(iii)* privacidad y protección de datos, *(iv)* libertad de acceso a cualquier web o plataforma social, *(v)* derecho al olvido, *(vi)* protección de niños, niñas y adolescentes, *(vii)* propiedad intelectual, y *(viii)* derecho a la desconexión digital laboral, principalmente.