PROPOSICIÓN CON PUNTO DE ACUERDO, POR EL QUE RESPETUOSAMENTE SE EXHORTA AL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES A QUE, EN EL MARCO DE LA EMERGENCIA SANITARIA POR COVID–19, REFUERCE LAS ACCIONES DE COMUNICACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES DE LAS PERSONAS USUARIAS DE PLATAFORMAS DIGITALES, ENTRE ELLAS UNA CAMPAÑA DE ALTO IMPACTO EN EL MAYOR NÚMERO DE MEDIOS DE DIFUSIÓN POSIBLE; Y A LAS UNIDADES ENCARGADAS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN DE LAS DEPENDENCIAS PÚBLICAS, ASÍ COMO DE LA SECRETARÍA DE EDUCACIÓN PÚBLICA A ADOPTAR O BIEN, REFORZAR, LAS MEDIDAS NECESARIAS PARA GARANTIZAR LA INFORMACIÓN Y DATOS PERSONALES DE LAS Y LOS TRABAJADORES Y POBLACIÓN ESTUDIANTIL QUE SE ENCUENTRA UTILIZANDO LAS DIVERSAS PLATAFORMAS DIGITALES PARA REALIZAR SUS ACTIVIDADES LABORALES Y EDUCATIVAS EN EL MARCO DE LA EMERGENCIA SANITARIA POR COVID–19.

La Suscrita Martha Tagle Martínez, diputada federal integrante del Grupo Parlamentario de Movimiento Ciudadano en la LXIV Legislatura del H. Congreso de la Unión, con fundamento en lo señalado en el artículo 78, fracción III de la Constitución Política de los Estados Unidos Mexicanos y los artículos 116 y 122, numeral 1 de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos, así como los artículos 58 y 60 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, someten a la consideración de la Comisión Permanente, la siguiente Proposición con Punto de Acuerdo al tenor de las siguientes:

CONSIDERACIONES

La protección de datos personales es un derecho humano consagrado en diversos instrumentos internacionales y, en la Constitución Política de los Estados Unidos, se encuentra establecido en el artículo 16, párrafo segundo, al indicar que “toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y

cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros" [subrayado propio].

Con esto como referencia, se hace necesario mencionar que "la protección de datos personales existe no solamente un componente de carácter nacional sino también uno estrictamente internacional impuesto por el cambio tecnológico, su velocidad y un alcance que trasciende las fronteras nacionales"[1]. A nivel nacional, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es el órgano encargado de garantizar estos derechos de las y los mexicanos establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. En esta ley se señala que los *datos personales* son "cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información" (artículo tercero, fracción novena).

Por su parte, es necesario destacar que ante la emergencia sanitaria por COVID–19 se ha presentado un aumento generalizado en el uso de las plataformas digitales, entre ellas las redes sociales y las videollamadas a través de sitios como *Zoom*, *Jitsi*, *Hangouts Meet* (*Google*), entre otros. Esto derivado del trabajo en casa, de las

[1] OEA. Protección de Daos Personales. Recuperado el 21 de abril de 2020 de: www.oas.org/es/sla/ddi/proteccion_datos_personales.asp

actividades escolares a distancia en *Moodle*, *Blackboard* u otras –25 millones de estudiantes cuentan con clases en línea–[2], así como de diversas actividades, entre ellas foros virtuales, que se han generado en distintos canales virtuales durante las últimas semanas.

Sin embargo, "si con anterioridad [las personas] poco solemos detenernos a revisar los avisos de privacidad, la necesidad de proximidad social se antepone ahora, a la protección elemental de nuestros datos personales"[3]. Esta afirmación cobra especial relevancia toda vez que plataformas como *Zoom* han sido señaladas por la vulnerabilidad de la información, hackeos y la presunta venta de datos personales de las personas usuarias.

> Debido a la contingencia por el coronavirus Covid–19 millones de personas en el mundo se están quedando en casa y encontrando en la tecnología la mejor opción para mantenerse conectados con su oficina y seres queridos. Precisamente por esa razón que Zoom se volvió tan popular.
>
> La empresa de inteligencia de seguridad cibernética Cyble reveló que ha descubierto que en la dark web, o web oscura, se ofrecen cuentas de Xoom por menos de un centavo. De hecho, la firma de ciberseguridad logró comprar cerca de 530 mil cuentas de la aplicación por mil dólares (…)

[2] Nolasco, Samantha (2020, 31 de marzo). Cuarentena acelerará desarrollo de educación en línea en México. En *El Economista* [en línea], México. Recuperado el 22 de abril de 2020 de: https://www.eleconomista.com.mx/arteseideas/Cuarentena-acelerara-desarrollo-de-educacion-en-linea-en-Mexico-20200331-0152.html

[3] Pimentel, Norma (2020, 2 de abril). Datos Personales, durante la crisis COVID19 y siempre. En *E-consulta* [en línea], México. Recuperado el 21 de abril de 2020 de: https://www.e-consulta.com/opinion/2020-04-02/datos-personales-durante-la-crisis-covid19-y-siempre

> Los datos que pueden encontrarse son listas de direcciones de correo electrónico, contraseñas, URL de reunión personal y chalve de host de cada una de las cuentas robadas de Zoom[4].

Ante situaciones como esta y, a manera de prevención, diversas organizaciones especializadas en el tema –como SocialTIC[5] o R3D Red de Defensa de los Derechos Digitales[6]– han publicado recomendaciones relativas a la privacidad que debe prevalecer al hacer trabajo en casa, o bien al usar plataformas como *Zoom*. Por su parte, el pasado 1º de abril, el INAI emitió la *Nota app para videollamadas ZOOM* en la que, a la par de informar en qué consiste dicha "plataforma de comunicación basada en la nube", alertan sobre los datos que la persona usuaria brinda y aquellos que son recolectados por *Zoom* y para que son usados. Entre estos datos, se encuentra: información de identificación, información técnica sobre los dispositivos, red y conexión a internet, ubicación aproximada, incormación sobre cómo usa la plataforma; configuración y preferencias elegidas por la persona usuaria, metadatos; entre otros[7].

Asimismo, el INAI enlista algunas observaciones derivadas de "la revisión de la política de privacidad", así como los principales riesgos sobre su uso. Entre estos destaca el "acceso no autorizado a las sesiones de videoconferencia" a la par de que Zoom:

---

[4] Cruz, Ariadna (2020, 15 de abril). Millones de cuentas de Zoom se venden en la dark web. En *El Universal* [en línea], México. Recuperado el 22 de abril de 2020 de: https://www.eluniversal.com.mx/techbit/millones-de-cuentas-de-zoom-se-venden-en-la-dark-web

[5] Disponible en: https://socialtic.org/blog/redes-y-tecnologia-digital-para-sobrellevar-la-cuarentena/

[6] R3D (2020). Cómo cuidar mejor tu privacidad al usar Zoom. Recuperado el 24 de abril de 2020 de: https://r3d.mx/2020/04/13/como-cuidar-mejor-tu-privacidad-al-usar-zoom/

[7] INAI (2020). *Nota app para videollamadas ZOOM*, p. 6.

> Recopila, *información del perfil de Facebook* en caso de que el usuario haya dado autorización para iniciar sesión, como nombre, foto de perfil y dirección de correo electrónico. El informe del sitio *Motherboard* publicado el 26 de marzo de 2020 que reveló originalmente el problema de privacidad, la información transferida incluía datos sobre cuándo un usuario abrió la aplicación, la zona horaria del usuario, el sistema operativo del dispositivo, el modelo y el operador del dispositivo, el tamaño de la pantalla, los núcleos del procesador y el espacio en disco. La política de privacidad de Zoom no indicaba claramente que estaba transfiriendo los datos a Facebook, ante esta situación, en una publicación del 27 de marzo de 2020, Zoom dijo que ahora ha eliminado el kit de desarrollo de software (SDK) "Iniciar sesión con Facebook" para iOS, que era la característica vinculada al intercambio de datos (…)[8].

En la misma Nota el INAI emitió una serie de recomendaciones para realizar videollamadas, mismas que a continuación se enlistan: no asociar las cuentas de correo electrónico ni de redes sociales, utilizar contraseñas robustas, actualizar versión de Zoom en los sitios oficiales; no compartir documentos con información personal, revisar los permisos que se proporcionan a la aplicación y analizar si estos son requeridos para el servicio de comunicación que se ofrece; utilizar otro medio para distribuir la información como correos corporativos o instituciones laborales, no utilizarlo para mostrar imágenes inapropiadas y, considerar recomendaciones obre trabajo a distancia emitidas por el INAI, para realizar videollamadas y cualquier tipo de comunicación y envío de información y datos personales de forma segura.

[8] Ídem, p. 10.

De igual forma, el INAI ha emitido diversos boletines de prensa y Guías que incluyen varias recomendaciones para la protección de datos personales en diversas plataformas digitales. Entre ellos:

- INAI 112/2020. Durante emergencia, INAI está pendiente de que sociedad cuente con información oportuna y se protejan datos personales[9].
- INAI 113/2020. INAI emite recomendaciones para proteger datos personales durante trabajo a distancia por COVID–19[10].
- INAI 116/2020. INAI emite recomendaciones para evitar ciberdelitos asociados con pandemia de COVID–19[11].
- Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital[12].
- Herramientas o aplicaciones de Supervisión Parental en Internet[13].
- #QuédateEnCasa. Sugerencias de actividades para realizar durante la contingencia sanitaria[14].
- Trabajo a distancia[15].

Sin embargo, estas acciones no han podido penetrar en la totalidad de las personas usuarias de plataformas digitales, lo cual sigue poniendo en riesgo los datos personales de las y los mexicanos, entre ellos los menores de edad.[16] Lo anterior y, considerando que, por el aislamiento producido por el COVID–19, las personas pasan mayor tiempo en el mundo digital para realizar sus acciones cotidianas y de entretenimiento, se hace necesario un reforzamiento de las acciones para difundir la

[9] Disponible en: http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-112-20.pdf
[10] Disponible en: http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-113-20.pdf
[11] Disponible en: http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-116-20.pdf
[12] Disponible en: http://inicio.ifai.org.mx/Guias/5RecomendacionesPDP_Web.pdf
[13] Disponible en: http://inicio.ifai.org.mx/Guias/GuiaSupervisionParental.pdf
[14] Disponible en: http://inicio.inai.org.mx/nuevo/RecomendacionesINAICOVID19.pdf
[15] Disponible en: https://micrositios.inai.org.mx/covid-19/?page_id=164
[16] OEA. Protección de menores de edad. Recuperado el 24 de abril de 2020 de: http://www.oas.org/es/sla/ddi/proteccion_datos_personales_pg_proteccion_menores.asp

labor del INAI como órgano garante de la protección de datos personales, así como de las recomendaciones que este ha hecho a la ciudadanía.

Asimismo, en el micrositio del INAI dedicado a *Datos personales seguros COVID19* en relación con el trabajo a distancia, enlista una serie de "medidas para proteger la información y datos personales que serán tratados en este esquema temporal de trabajo", dirigidas a organizaciones e instituciones del sector privado y público. Estas medidas son:

Rubro	**Recomendaciones**
Personal	Concientizar al personal sobre la responsabilidad de proteger la integridad, confidencialidad y disponibilidad de la información y datos personales que tratarán para continuar con sus actividades en la modalidad de trabajo a distancia. Cumplir con las medidas de seguridad físicas y técnicas establecidas por la organización, para la protección de la información y datos personales. Cerrar la sesión del equipo de cómputo o sistemas de información cuando no se utilice, tanto en casa como en lugares públicos. Conocer los canales de comunicación en donde se podrá reportar cualquier incidente que comprometa o afecte la seguridad de la información y/o datos personales. Realizar respaldos de la información y/o datos personales de forma regular, para garantizar su disponibilidad.

Acceso a la res y servicios de nube	Utilizar los servicios de nube y las redes de confianza de la organización. Cumplir con las políticas y procedimientos sobre acceso a la red, servicios de nube, usuarios, contraseñas, intercambio y respaldo de información. Usar un canal seguro siempre que se utilice una red pública para conectarse, por ejemplo, una VPN (Red Privada Virtual). En caso de requerir acceso a la red de la organización, para operar sistemas de información, administrar recursos tecnológicos de forma remota o consultar información de la intranet, se sugiere utilizar una VPN. Realizar una revisión física para verificar que los elementos de red funcionen correctamente (modem, cableado, corriente eléctrica, intensidad de la señal).
Correo electrónico	Cumplir con las políticas de la organización relacionadas con el uso de correo electrónico. Usar las cuentas de correo electrónico de trabajo en lugar de cuentas personales para correos electrónicos relacionados con actividades laborales que traten datos personales. Si es estrictamente necesario utilizar cuentas de correo electrónico personales para enviar datos personales o información confidencial adjunta, ésta deberá estar cifrada. Evitar incluir datos personales o información confidencial en el asunto del correo electrónico.

	Antes de enviar un correo electrónico verificar que la dirección del destinatario sea correcta, especialmente en casos donde se envíen datos personales y/o sensibles. Verificar que el entorno donde se utilice el correo electrónico sea seguro, para evitar que personas no autorizadas tengan acceso a datos personales o información.
Dispositivos móviles (equipos de cómputo, tabletas electrónicas y smartphones)	Instalar medidas de seguridad que protejan a los dispositivos móviles de cualquier software malicioso que pueda comprometer la información y datos personales que éstos almacenan. Asegurar que los dispositivos que se utilicen para tratar datos personales o información de la organización cuenten con las últimas actualizaciones instaladas. Verificar que el entorno donde se utilicen los dispositivos móviles sea seguro, para evitar su pérdida o extravío, así como la exposición de datos personales o información a personas no autorizadas. Establecer medidas para bloquear el acceso a los dispositivos en donde se realizará el tratamiento de datos personales o información, a través de un código, patrón o huella. Usar medidas para controlar el acceso a los dispositivos, aplicaciones o servicios, tales como contraseñas robustas, autenticación de múltiples factores y/o cifrado para restringir el acceso al dispositivo y reducir el riesgo de que se comprometa la seguridad de los datos personales o información. Implementar medidas para el borrado remoto de dispositivos en caso de pérdida, robo o extravío.

	Cumplir con las políticas de la organización relacionadas con el uso de dispositivos móviles (tabletas electrónicas, smartphones o laptop).

Fuente: Elaboración propia con información del INAI (2020)[17].

En dicho sentido, las dependencias del sector público deben contar con este tipo de medidas que garanticen la privacidad de la información y datos personales de las personas trabajadoras, así como de la población estudiantil que actualmente desarrolla sus actividades en las múltiples plataformas digitales. Ello, en aras de abonar al ejercicio del derecho que las y los mexicanos tienen sobre sus datos personales. Por lo anterior y, considerando la pertinencia de la adopción de dichas medidas en el marco de la emergencia sanitaria, someto a consideración de esta honorable asamblea la siguiente proposición con los siguientes

PUNTOS DE ACUERDO

PRIMERO. – La Comisión Permanente del H. Congreso de la Unión exhorta respetuosamente al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que, en el marco de la emergencia sanitaria por COVID–19, refuerce las acciones de comunicación en materia de protección de datos personales de las personas usuarias de plataformas digitales, entre ellas una campaña de alto impacto en el mayor número de medios de difusión posible.

[17] INAI (2020). Trabajo a distancia. México. Recuperado el 22 de abril de 2020 de: https://micrositios.inai.org.mx/covid-19/?page_id=164

SEGUNDO. – La Comisión Permanente del H. Congreso de la Unión exhorta a las unidades encargadas de los sistemas de información y comunicación de las dependencias públicas, así como de la Secretaría de Educación Pública a adoptar o bien, reforzar, las medidas necesarias para garantizar la información y datos personales de las y los trabajadores y población estudiantil que se encuentra utilizando las diversas plataformas digitales para realizar sus actividades laborales y educativas en el marco de la emergencia sanitaria por COVID–19.

Dip. Martha Tagle Martínez

Dado en la H. Cámara de Diputados, el día 13 de mayo de 2020.