Ciudad de México, 20 de noviembre de 2020.

Versión estenográfica del Panel 9: Herramientas y medidas de seguridad para resguardar datos personales sensibles, realizado por el Instituto Nacional de Acceso a la Información y Transparencia.

Presentadora: Damos inicio al Panel Herramientas y medidas de seguridad para resguardar datos personales sensibles.

Tenemos el gusto de presentarles a nuestros distinguidos invitados Joel Hernández García, Presidente de la Comisión Interamericana de Derechos Humanos.

Felipe Rotondo, Presidente del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales de Uruguay.

Jorge Luis Pérez Hernández, Director General de Operación Tecnológica de la Agencia Digital de Innovación Pública de la Ciudad de México.

José Antonio Vázquez Acosta, Director de Ciberseguridad de Microsoft México.

Modera este panel la Comisionada Presidenta del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales y Coordinadora de la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia, Reyna Lizbeth Ortega Silva, a quien damos la bienvenida y cedemos el uso de la voz.

Reyna Lizbeth Ortega Silva: Muchísimas gracias.

Muy buenas tardes a todas y a todos los que están siguiendo esta transmisión en vivo.

Estamos hoy en el panel número 9. Cerramos esta Semana Nacional de Transparencia con broche de oro. Vamos a hablar de un tema que ha estado con mucha relevancia con todo este tema de la cuestión sanitaria, la pandemia que se ha desarrollado en todo el mundo.

De forma específica, como ya fue mencionado, Herramientas y medidas de seguridad para resguardar datos personales sensibles. Es un honor, de verdad, estar en esta mesa, poder moderar esta mesa, y estar con tanta personalidad y conocedor de la materia.

Muchísimas gracias por el espacio que nos brindan, y desde luego también al INAI por toda esta semana que ha desarrollado todos estos eventos y, desde luego, a las y los comisionados que desarrollaron este evento, en especial a la Comisionada Blanca Lilia Ibarra Cadena, quien es la Coordinadora de esta Semana Nacional de Transparencia.

Y para dar inicio a este tema tan importante que nos ocupa comentarles que la ronda que llevaremos a cabo, mejor dicho las dos rondas que llevaremos a cabo voy a realizar unas preguntas detonadoras de este tema. Cada uno de nuestros ponentes nos va a dar una explicación de ocho minutos y después vamos a desarrollar otra ronda en la cual cada uno de nuestros ponentes, de acuerdo a las preguntas que nos van haciendo llegar, por medio de las redes sociales, vamos a realizar otras preguntas detonadoras.

En ese sentido le doy la bienvenida y, desde luego, el uso de la voz en unos momentos, después de leer una pequeña reseña curricular, al doctor Joel Hernández García, Presidente de la Comisión Interamericana de Derechos Humanos. De quien me voy a permitir leer nada más un pedacito de su reseña, desde luego amplio currículum y, desde luego, muy conocido por todas y todos; pero nada más para sentar este pequeño precedente.

Presidente de la Rama Mexicana de International Law Association. En el Servicio Exterior de México ascendió al rango de embajador, fungió como representante permanente de México ante la OEA, ha sido profesor invitado en la materia de Derecho Internacional y Organismos Internacionales en diversas instituciones.

En el sentido nada más comentarles que desde luego el objetivo general de este panel, es reflexionar sobre los riesgos que representa la exposición, la información sensible y la necesidad de proporcionar mecanismos para mantener un nivel de seguridad apropiado a todo tipo de datos personales.

Al igual que indagar sobre las medidas de seguridad y las herramientas con las que se cuenta para frenar el flujo inapropiado de información y la sobre-exposición de datos personales sensibles.

Las dos preguntas que les dejo sobre la mesa a nuestros panelistas, son las siguientes:

La número uno: cuáles son las herramientas a nivel internacional que se impulsan para sensibilizar sobre la protección de datos personales, tanto a los titulares de los mismos, como a los responsables de su tratamiento y la segunda, qué se ha hecho para capacitar a los servidores públicos y empresas en materia de protección de datos personales sencillos.

En ese sentido, y como ya lo mencioné, le doy el uso de la voz, hasta por ocho minutos, al doctor Joel Hernández García.

Joel Hernández García: Muchas gracias a la doctora y presidenta comisionada Ortega Silva.

La verdad es que es un gusto estar en este panel, como parte de la Semana Nacional de Transparencia que organiza el Instituto Nacional de Acceso a la Información de México, un órgano constitucional autónomo, que tengo que decir, como mexicano, con mucho orgullo, es un referente en toda la región, el trabajo que ha realizado el INAI y desde luego la Ley de Acceso a la Información y Protección de Datos Personales de México, es un referente.

Y ha habido una gran colaboración, una estrecha colaboración, entre la Comisión Interamericana de Derechos Humanos específicamente su relatoría especial para la libertad de expresión con el INAI, pero también la Organización de Estados Americanos del INAI han avanzado distintos proyectos de coordinación.

Para ir respondiendo las preguntas que nos ha formulado la Presidenta Comisionada, si hablamos de herramientas a nivel internacional, para impulsar la protección de datos personales, aquí me siento obligado de mencionar el trabajo que ha realizado la Comisión Interamericana de Derechos Humanos para la Protección de Dato Personales.

En otras palabras, cuál ha sido la mira en este ámbito.

¿Qué hemos avanzado y sobre todo, qué falta por avanzar? Porque ciertamente es un tema novedoso en la región, pero lo es también, lo digo con toda transparencia, es un tema novedoso en la agenda de la Comisión Interamericana de Derechos Humanos.

Es un tema que ha sido más bien explorado, en las dos vertientes, en la de acceso a la información, y en la protección de datos personales ha sido más bien explorado por la relatoría especial en libertad de expresión, es una oficina técnica que pertenece a la Comisión y que desde ahí la Comisión ha hecho su trabajo de monitoreo y de formulación de recomendaciones a los estados.

Señalo a continuación, cuáles son las obligaciones internacionales que tienen los estados para la protección de datos personales, desde la perspectiva del sistema interamericano de derechos humanos.

Debemos tener presente aquí dos artículos clave en la protección de datos personales contenidos en la Convención Americana de los Derechos Humanos.

Uno es el artículo 11, sobre la protección de la honra y dignidad y el segundo, es el artículo 13 sobre libertad de pensamiento y de expresión.

La interpretación armónica de estos dos instrumentos establecen la obligación que tiene todo Estado, parte de la Convención Americana, como es México, de proteger los datos personales.

¿Por qué digo esto? El artículo 11, fracción II señala que nadie puede ser objeto de injerencias arbitrarias o abusiva en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

Esta disposición, el artículo 11, párrafo dos, es una disposición idéntica a la contenida en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos adoptado en el marco de las Naciones Unidas.

Ambas disposiciones, el artículo 11 de la Convención Americana, el artículo 17 del Pacto Internacional, otorgan a las personas el derecho a la protección de la ley contra esas injerencias o esos ataques.

Por el otro lado, tenemos el artículo 13 que versa sobre la libertad de pensamiento y expresión. Y aquí la parte fundamental del 13.1 señala que toda persona tiene derecho a la libertad de pensamiento y de expresión.

Y esto es una verdad de Perogrullo, nadie pone a discusión este derecho. Pero la parte interesante de este artículo 13 es el desarrollo normativo, cuando señala que el artículo 13, que este derecho comprende la libertad de buscar, recibir y difundir informaciones, ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística o de cualquier otro procedimiento de su elección.

¿Cómo se vincula este artículo 13 que es de libertad de pensamiento y de expresión con la protección de datos personales? Muy sencillo.

Si existe una invasión a los datos personales, se está entonces también coartando este derecho que tienen las personas para buscar recibir y difundir información.

Ninguna persona se va a sentir cómoda de poder buscar información, por ejemplo, a las distintas instituciones mexicanas de acceso a la información, si siente que su privacidad está siendo invadida.

Por eso menciono yo estos dos artículos como dos caras de la moneda. Por una parte, proteger la vida privada, y por la otra en la medida en la que se protege la vida privada, se garantiza también el derecho a buscar recibir y difundir información de toda índole. Este es el ángulo que ha estudiado el tema la Comisión Interamericana.

¿Y por qué resulta tan importante? Porque la emergencia del internet a fines del siglo pasado, modificó de manera radical a la sociedad.

El cambio tecnológico ha producido cambios profundos en el ecosistema de la información y, por ende, ha significado un nuevo escenario para el ejercicio de la libertad de expresión.

Esta emergencia del internet nos presenta oportunidades y desafíos. El internet ha creado oportunidades sin precedentes para la libre expresión, la comunicación, la búsqueda, la posesión e intercambio de información. Con ello se ha facilitado el desarrollo de grandes cantidades de datos acerca de las personas que incluye, entre otros, su ubicación, actividades en línea y con qué personas uno se comunica, toda esta información manejada en archivos accesibles y sistematizables puede ser altamente reveladora de la vida privada.

Entonces, el internet además de estas oportunidades nos ha creado desafíos, que la comisión lo ve en cinco aspectos: primero, la comisión observa en la región una presente violencia contra periodistas en el ecosistema digital; segundo, una vigilancia y violación de la privacidad; tercero, una protección de fuentes de información, es un desafío muy importante cómo proteger las fuentes de información; un cuarto desafío es amenazas a la diversidad y al pluralismo; y un quinto desafío son otras amenazas al discurso público en internet entre las que se incluyen el discurso estigmatizante o descalificante, y el llamado *trolling* por las diversas formas de toxibilidad del debate público.

Para la Comisión Interamericana del Derecho a la Privacidad tiene una relación estrecha con la libertad de expresión; lo han sostenido los dos relatores especiales para libertad de expresión, tanto de la CIDH, como de las Naciones Unidas, las víctimas de la violencia sufren una afectación de sus derechos a la privacidad y a la libertad de expresión; si los esfuerzos por interferir sus comunicaciones son exitosos o no.

La invasión de la privacidad de las personas afecta entonces de manera directa e indirecta el libre desarrollo e intercambio de las ideas, así las restricciones a la privacidad tienen un efecto silenciador que tanto el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, como el artículo 11 de la Convención Americana, que ya citaba buscan proteger.

Buscan proteger la correspondencia privada de invasiones ilegítimas. Y aquí estoy usando correspondencia privada, entre comillas, es el lenguaje de la época de los instrumentos, hoy sabemos bien que esta correspondencia se da básicamente a través de los medios electrónicos, a través de la internet.

Bien. El internet en los últimos años ha revelado de una manera clara esta relación estructural que existe entre el derecho a la libertad de expresión y el derecho a la privacidad. Hoy vemos una multiplicación de los canales de comunicación digitales y la emergencia del internet como una red horizontal que potencia diversas prácticas estatales y privadas que si no son adecuadamente reguladas pueden amenazar la privacidad de los ciudadanos.

Sin un ámbito individual ajeno a la injerencia de actores estatales y no estatales la libertad de expresión puede convertirse en una enunciación hipotética.

Lo dejo hasta ahí para responder a la pregunta. La resumo en pocas palabras: Los estados tienen la obligación de salvaguardar la privacidad o el todo lo que tiene que ver con datos personales en cumplimiento con sus obligaciones internas.

Reyna Lizbeth Ortega Silva: Muchísimas gracias, doctor Joel.

Como bien lo dice la Comisión Interamericana de Derechos Humanos juega un papel fundamental. Hay que recordar los datos personales son un derecho humano, por lo tanto tenemos que tener una protección más amplia.

Cuando hablamos de datos personales sensibles, desde luego que como usted lo mencionó, en los cuales se pone en juego la honra, la dignidad y, desde luego, también estos otros temas en los cuales hay que evitar la discriminación y, desde luego, una agresión grave a las personas, como lo hemos visto que ha sucedido durante esta pandemia, sin duda estamos hablando de una protección muy amplia.

Muchísimas gracias.

Para continuar con el programa me permitiré darle la bienvenida y leer una pequeña, muy pequeña síntesis curricular del maestro Jorge Luis Pérez Hernández, quien es Director General de Operación Tecnológico de la Agencia digital de Innovación Pública de la Ciudad de México.

Tengo que resaltar que en la iniciativa privada ha trabajado en los temas, principalmente de telecomunicaciones, de estructura tecnológica y desarrollo de software.

Maestro Jorge, muchas gracias, y le doy el uso de la voz.

Jorge Pérez: Muchas gracias. Buen día a todos, a todas.

Respecto a lo que preguntabas, yo más que herramientas piensas que si bien ya explicó Joel Hernández, herramientas como política pública, como reglamentarias, yo más pienso que para las empresas y para nosotros los ciudadanos la forma más fácil de saber qué tan importante son los datos personales, son las consecuencias de lo que hemos visto.

¿Qué es lo que hemos visto? Fugas de datos personales de grandes empresas, grandes empresas hablo a nivel Facebook, y de Google, que ha perdido datos personales; Uber, que estuvo expuesta el año pasado; el Linkedin, que seguramente muchos de nosotros tenemos ahí nuestro CV, perdieron datos personales el año pasado.

Las consecuencias de perder datos personales, según una encuesta de IBM en Estados Unidos y Europa representó para cada una de estas empresas, al menos, una pérdida de 3.9 millones de pesos por cada una de las demandas que recibieron. Así de importante es. Si a ti como empresa no te importa, pues puedes perder, al menos, 3.9 millones de pesos por no importante la protección de datos personales.

Y hay casos más drásticos como el de la Asociación Médica en Estados Unidos, la cual se tuvo que ir a la quiebra en julio del año pasado por la cantidad de demandas que tuvo después de exponer los datos de 200 millones de ciudadanos en Estados Unidos. La empresa actualmente en banca rota todavía.

Entonces, de que es importante es importante, y para nosotros como ciudadanos también tener claro que el dar nuestros datos sin leer, sin saber a quién se los estamos dando puede representar un riesgo, incluso, de seguridad para nosotros; seguridad física, ya no hablo de seguridad informática.

Pero bueno, aprovechando esto y la semana de transparencia, esta semana, esto que han presentado ustedes, voy a permitirme compartir pantalla para presentar brevemente qué estamos haciendo desde la Ciudad de México, respecto al tema que hoy nos atañe.

Primero, el tema de transparencia, más que una presentación, quiero mostrarles el sitio, donde se exponen todos los datos no personales, obviamente, de contagios de COVID en la Ciudad de México, hacia dónde va el gasto, qué colonias son las más infectadas, únicamente se hace a nivel colonia, precisamente evitando discriminación, no podemos dar el dato exacto de dónde vive la persona, es a nivel colonia, y viene toda la información de cuánto dinero se está gastando, cuáles son los programas sociales, cuáles son los requisitos, etcétera.

Esto es lo que se hace aquí como gobierno en cuanto a transparentar el gasto, transparencia de información.

Y ahora sí, en cuanto al tema que nos atañe, de herramientas, voy a brincarme algunos slides, cuáles es la estrategia de seguridad informática que estamos tomando.

Voy a brincarme la parte de infraestructura, porque veo que dentro de los panelistas hay expertos como el Microsoft, en ciberseguridad, seguramente (…) del tema de firewall, firewall perimetrales, firewall nivel web, todo esto; entonces, me lo voy a brincar.

Voy a ir prácticamente al desarrollo de software.

¿Qué es lo primero que hacemos nosotros aquí? Primero, analizar, nosotros tenemos una fábrica de software en la ciudad, nosotros hemos hecho todos los desarrollos ahorita que tienen que ver con el tema de COVID y salud, por ejemplo en particular el que se está lanzando ahorita, que para poder entrar a un establecimiento mercantil, no de primera necesidad, es decir, no aplica para sondear mercados, tianguis y este tipo de lugares, se pide que te registres, que anotes tu número telefónico únicamente.

Todos estos desarrollos o el de SMS, tamizaje, videollamadas, seguimiento de rastro de contactos, la información del sistema de rastreo de contactos y del sistema epidemiológico, toda esta

información la recabamos nosotros en diferentes maneras y para todo esto se han llevado estas prácticas.

Se valida primero que los requerimientos no incumplan las medidas de seguridad.

En el tema de la pandemia, no nos ha tocado, pero sí en otros escenarios comúnmente, sobre todo con firma digital, nos piden muchas veces los clientes subir a internet la llave desde que firmas una firma digital. Eso es trascendente.

En esta situación hemos encontrado nada al respecto. Pero se identifica el tipo de información y cómo se va a transmitir, qué informaciones publican, cuál es confidencial, cuál es reservada.

Y a partir de aquí, se hace una arquitectura del software, se separa la base de datos, se separa la aplicación web, se ve si se necesita firewall web, firewall perimetral, si los programadores, los desarrolladores o quienes van a tener acceso a la información para procesarla, se tienen que conectar por BPN, si van a tener un acceso público, un SPTP, todo eso se diseña desde aquí, desde el análisis y el diseño de la arquitectura del software.

Aquí es muy importante si bien los programadores en un inicio tienen que tener acceso a la base de datos, para saber su estructura, para insertar datos o hay usuarios con muchos privilegios, aquí es donde se tiene que detonar quién, cómo y cómo se va a validar qué es lo que están usando, a qué están accediendo, si necesitan ver la información o no, si nada más necesitan insertar información, pues buena la información tiene que ver al encriptarla, no tienen por qué saber qué es lo que están mandando muchas veces.

Únicamente tienen que tener acceso para poder saber si están escribiendo un acceso nivel escritura, lectura, pero una lectura encriptada.

Entonces, al final de cuentas nuestros desarrolladores o la gente que detrás le da mantenimiento y soporte a ese software, al final de cuentas no sabe qué información es la que está ahí, sabe que hay información, se valida, pero va encriptada.

Lo más importante, al final de cuentas se tiene que probar todo esto que estamos diciendo, no nada más tenerlo en papel, sino tenemos aparte un equipo de *CUA* que se encarga también de validar esta parte.

Una parte que olvidé mencionar aquí, se tienen que definir muy bien las versiones de software, librerías de terceros a utilizar. Esto es muy sencillo, tú entras incluso a la página muchas veces de los fabricantes, de los desarrolladores ya sea del sistema operativo o de las librerías, de los *frameworks* que estemos utilizando, y ahí puedes ver directamente muchas veces cuáles son los *boots*, cuáles son los reportes de seguridad que tienen, cuál es la última versión estable, cuáles son los parches que debería de tener dependiendo el frameworks que estés utilizando.

Todo esto se tiene que revisar de manera periódica y estar actualizando todas las librerías y el sistema operativo.

Por último, la estrategia de seguridad en la arquitectura del software. Lo que hacemos, todo nuestro software está autenticado actualmente desde la parte pública con un mecanismo que le llamamos “Llave CDMX”, es una firma digital.

Para obtenerla es muy sencillo. Entras al portal web, das ciertos datos, si quieres una llave no verificada y si quieres una llave verificada para tener acceso a más información o más trámites, si se te piden algunos datos personales, sobre todo enviar tu identificación, enviar ciertos documentos que validen que tú eres la persona que realmente está utilizando esta llave. Eso lo hacemos para la versión pública.

Para la versión interna lo tenemos separado en dos estrategias. Primero, la información para que un programador o una persona de nuestra institución tenga acceso a esta información tiene que tener una VPN.

Una VPN es un cifrado seguro, nosotros la tenemos que instalar en su equipo de cómputo, se firma una responsiva y también desde nuestro manejador de VPN le podemos dar acceso a ciertos servidores, a ciertos recursos y a cierta información.

Todo está va restringido, está muy limitado y muy controlado por nuestra parte de infraestructura.

La integridad de la información simplemente son lo que ya mencionaba, son roles que te permiten tener acceso a pedazos, no hay un rol que tenga un acceso global a toda la información, esto es simplemente por seguridad y además así están divididas nuestras áreas: áreas de bases de datos, áreas de protectores, hay un área de infraestructura; en el área de infraestructura hay quien le da mantenimiento al sistema operativo, hay quien le da mantenimiento a las librerías, los programadores del framework; todo va separado.

Entonces, todo esto va por roles y nadie tiene un acceso global.

Aun así, para mantener la integridad y estar seguros se generan respaldos de manera dinámica, básicamente los hacemos de manera incremental cada seis horas y de manera semanal un full.

Para todo el intercambio de información que llevamos se usan protocolos seguros, insisto, la VPN, HTTPS, STP, restricción a acceso a rutas específicas, eso es muy importante para que no puedan ejecutar comandos.

Que nada más el mismo aplicativo tenga ciertos permisos que ni siquiera el desarrollador, el programador o la gente que ve la información pueda.

No tiene tanta relevancia, pero también mantener alta disponibilidad para que también los ciudadanos siempre tengan acceso a su información. Esa parte simplemente la manejamos como arquitectura, pero es un servicio extra que se da simplemente para manejar un buen servicio de disponibilidad y el ciudadano siempre tenga acceso a lo que requiere.

Ya en cuanto a nuestro hardware físico todo, todo, absolutamente todo lo que hacemos va midiendo el certificado https, todo va con certificado esto es muy importante para uno como ciudadano; comúnmente, seguramente les llega mail apócrifo que los lleva a URLs que se parecen mucho a la de sus bancos, a las páginas de gobierno, nos pasa mucho para licencias y para tarjetas de circulación, pero bueno, es muy fácil

validar si estás en un portal que sí es auténtico, que sí es seguro a partir del certificado https. En unos momentos les muestro o vamos para allá.

Algo que nos pasa mucho a nosotros y seguramente a ustedes también, es el correo es pack, o sea, esto se puede validar a través de los certificados también; aquí, por ejemplo, se supone que ya no tengo cuota en mi correo pero como pueden ver para empezar el dominio, este es el dominio, pues no es el del gobierno, o sea, un dominio de gobierno debería ir .gob.org.mx, aquí es .gob.p y yo no soy del gobierno de Perú evidentemente.

Esto pasa muy comúnmente de este tipo de ataques tenemos diario, diario, miles durante el corte a octubre de ataques de este tipo son 180 millones de ataques, tanto de fishing de mail, como ataques de denegación de servicio que hemos tenido en la Ciudad de México, todos han sido detenidos evidentemente, en el caso del fishing todo se va al spam y para fortalecer un poquito más esto se les ha dado capacitación a los servidores públicos para que no caigan en correos falsos como estos que te llevan a otro link, donde te piden tus datos personales y entonces ellos tienen acceso a toda tu información. Eso me parece bastante importante.

También tenemos mecanismos de control de acceso, control basado en roles como les explicaba. Y, sobre todo, algo que hacemos de manera recurrente es estar buscando todos los parches de seguridad que necesitan tanto nuestro servidores a nivel firmware, sistema operativo, web y todos los words que utilizamos.

Por mi parte, la seguridad de la información es básicamente lo que ya había comentado hace unos minutos, no quiero repetirlo, por lo cual aquí dejaría mi participación.

Reyna Lizbeth Ortega Silva: Muchísimas gracias, maestro Jorge.

Sin duda, como lo menciona tanto en el ámbito público como privado, debemos de tener las medidas de seguridad como nos marca tanto nuestra Ley Federal como nuestra Ley General de Protección de Datos Personales, físicas, técnicas y administrativas.

Ahorita nos acaba de dar una explicación sin duda muy importante de toda la arquitectura que se debe desarrollar con un software bien establecido. Y, desde luego, las medidas que se deben de tomar en cada uno de estos ámbitos.

La tecnología, como ya lo mencionaban nuestros dos ponentes, ahorita vemos la necesidad y desde luego que nos implica estar más protegidos que nunca, todas nuestras actividades por el tema de la pandemia si ya las realizábamos en línea, ahorita la mayoría por no decir que casi todas, son por medio de estos temas y plataformas que debemos de estar más vigilados y protegidos que nunca.

Muchísimas gracias, maestro.

Y si me permiten, continuando con el programa, es un verdadero honor, porque yo soy una gran seguidora de todo su trabajo que hace. La verdad, muchísimo, muchísimo. Soy su fan, así lo voy a decir, presentar al doctor Felipe Rotondo, Presidente del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales de Uruguay.

Quien, si me permiten, no tocar todo su amplio currículum, nada más mencionaré aparte de su cargo actual, que es autor de numerosas publicaciones y expositor en distintos foros, congresos, seminarios. Además de ser un especialista en Derecho Público y Protección de Datos.

Doctor, muchas gracias por atendernos y por tener este espacio para nosotros.

Le doy el uso de la voz, de igual forma con las preguntas que establecí. Muchas gracias.

Felipe Rotondo: Muchas gracias, Comisionada Presidenta Reyna. Es un gusto compartir este panel con ustedes, con tan distinguidos participantes.

El doctor Joel Hernández hizo una presentación excelente, que para mí como profesor de Derecho Administrativo, que fue mi primera actividad y la mantengo, es fundamental el encare jurídico desde el punto de vista

interamericano y con la visión, además, universal de la Declaración de Naciones Unidas.

Mi camino va a seguir mucho más, digamos, un poco lo del doctor Joel Hernández, que lo de Jorge Pérez, porque honestamente no manejó esta visión que él acaba de señalar.

Se ha dicho con razón que los datos personales son el petróleo del siglo XXI, y podemos ver que hoy las empresas tecnológicas son las más grandes del mundo. Ya no la de combustibles o petróleo, etcétera.

Y que esas grandes empresas son las que utilizan en gran escala los datos, y más los datos personales, y que estos hacen a la dignidad de cada ser humano, y más si son sensibles, ya que el contexto de su tratamiento puede entrañar datos importantes respecto a los derechos y libertades fundamentales.

En ese contexto rigen principios básicos en la materia, como la responsabilidad proactiva. Que esta responsabilidad proactiva incluye las medidas organizativas, administrativas, técnicas y está exactamente vinculada o directamente vinculada a la seguridad.

No hay privacidad si no hay protección de datos personales sin seguridad, y más, repito, respecto a los datos sensibles, que exigen un tratamiento mucho más delicado. La regla es, por ejemplo, en el Uruguay que los datos personales requieren consentimiento escrito, que no se admiten bases de datos sensibles, salvo excepciones.

Tenemos ahora el caso, y sería lindísimo hablar, ustedes lo habrán hecho en otros paneles, en la relación de base de datos vinculadas al COVID-19, cómo tienen que permanecer los principios en esta misma materia.

Podrá haber situación de emergencia, el Estado de derecho no puede quedar en pandemia, no puede aislarse. Podremos tener cuarentena nosotros, pero no los principios de derecho, incluido el de seguridad en este tema.

¿Y esto es importante para quién? Para el titular del dato, que somos cada uno de nosotros. Nosotros decimos: somos dueños de los datos,

son nuestros datos. No. Los datos somos nosotros, es un tema de personas, pero además y esto es fundamental, contribuye a la circulación de datos en el comercio internacional.

Por lo tanto, importan las empresas y el flujo internacional de datos tiene una relevancia enorme en ese sentido.

Es así que la pregunta que tú hacías Reyna, sensibilizar a los titulares para empoderarlos en el control de sus datos, y a los responsables en su tratamiento, esto hay que hacerlo ver para los responsables, no solo como un deber jurídico, sino ético, y además con un activo o un valor agregado de la Organización o de la empresa, pero también del Estado, porque el estado de sitio es estado de derecho y tiene que hacer las cosas como debe.

No es por ejemplo ahora en el caso de la situación de la pandemia que sea un obstáculo, sino que se hagan las cosas bien.

Tal el objetivo de la sensibilización, evidentemente la seguridad implica una serie de medidas que yo creo que no puede ingresar a ellas, porque después de la exposición de Jorge Pérez, yo no me animo a hablar, pero evidentemente los controles de acceso el cifrado de datos y de dispositivos portátiles, es un etcétera que incluye aspectos que podría yo algo señalarles, pero luego de su excelente exposición, no lo puedo hacer.

Pero con respecto a las medidas internacionales para la sensibilización; Uruguay está presidiendo hasta este año la Red Iberoamericana de Protección de Datos Personales, que incluye a México y que incluye a Uruguay, con motivo de que lo está percibiendo.

Pero es Iberoamericana, porque inclusive también España, Portugal y Andorra.

Y ella, la red, tiene entre sus fines, programar programas de capacitaciones de sus miembros y de información a los ciudadanos y en su ámbito se ha creado un foro de la sociedad civil, en el que participan organizaciones que no son como las autoridades públicas, sino que son, puede ser de otra índole, sociales, sí, pero vinculadas a la protección de datos.

Además, participan entonces en actividades múltiples, y la red ha emitido unos estándares de protección de datos, que son un verdadero documento y que incluso en este momento, yo no voy a entrar en temas de la OEA, después de la excelente exposición de Yurel, pero el Comité Jurídico Interamericano, órgano de asesoramiento de otra índole, por supuesto que la Comisión, ha trabajado en materia de principios y hoy en día se está en eso, o sea, en tratar de acercar los principios de la OEA, que en su momento tuvo en cuenta ese Comité, con los estándares de protección de datos, para quizás llegar a una Ley Modelo de este tema como la hay en otros.

La Red Iberoamericana de más desarrollo, programas de capacitación e información online, y presenciales, iniciativa de todo tipo para el desarrollo de la educación digital, porque acá yo creo que es un tema fundamental, que esté lo educativo, o sea, creo que acá no es un tema de medida internacional, Reyna, sino de globalización; o sea, la educación es fundamental en todo ámbito, y creo que ahí es donde tenemos primero que nada, sensibilizar.

Siguiendo con la red, ha emitido documentos importantes, por ejemplo, muy recientemente recomendaciones y orientaciones para la protección de datos en la inteligencia artificial.

En la página web de la Red, se pueden ver los documentos emitidos por todas las autoridades iberoamericanas, a los efectos del tratamiento adecuado de protección de datos y la actual situación de pandemia, que pone justamente relación a la salud pública y los datos de salud que son sensibles.

Porque hoy dije, para tratar datos sensibles se requiere el principio de consentimiento, y consentimiento escrito en países como en Uruguay.

Pero hay excepciones, por ejemplo, para mantener el valor de la seguridad pública, que es la vida nuestra; pero de todas maneras eso debe que hacerse manteniendo los otros principios de protección de datos, no usar esos datos de salud para otra finalidad, trasladar de salud para otra cosa o que sean desproporcionados, que sean adecuados, el principio de minimización en este sentido.

Las medidas de sensibilización también incluyen a veces cooperación entre autoridades. Por ejemplo, la autoridad nuestra uruguaya que integro, junto con la similar argentina, ha realizado una guía de evaluación de impacto en protección de datos, porque este es un tema vinculado con la seguridad.

Porque lo incluye el Reglamento Europeo de Protección de Datos y nuestra ley lo ha tomado, una actualización de nuestra ley que rige desde el año pasado, que las empresas que tienen en su cometido especial o principal los datos sensibles o se maneja grandes volúmenes de datos, tiene que realizar evaluación de impacto de protección de datos, incluidos temas de seguridad obviamente.

Y también tener un delegado de protección de datos, o sea, alguien que sea funcionario, dependiente o forma independiente que esté dedicado o maneje; no es el responsable, porque el responsable será el titular de la empresa en el caso que corresponde, sino alguien que esté dedicado a este tema.

Como medida de responsabilidad proactiva y entonces con la autoridad argentina se ha hecho una guía de evaluación de impacto en este sentido.

Se trata, entonces, de un tema fundamental. Y también hoy hablamos con un colega del INAI de materia internacional, cómo tanto México como Uruguay integran el Consejo de Europa, perdón, me equivoqué, el Convenio 108 del Consejo de Europa para ahorrar, para no perder minutos dije mal, el Convenio 108 que es para la protección de los datos personales de tratamientos automatizados y su protocolo posterior, que ahora se ha actualizado ese Convenio.

Pero bueno, México y Uruguay integran, porque el Convenio 108 está abierto a todos los países del mundo, es el único Convenio, yo diría, global, porque no es de Europa, aunque emitió, surgió de Europa, pero está abierto a otros países.

Como acabo de decir, y tú Reyna, hablamos hoy, Argentina, Uruguay y México lo integran.

Este Consejo ha también permanentemente emitido de forma, documentos para la actualización. El 28 de enero es el Día Internacional de Protección de Datos, ¿por qué es el 28 de enero? Porque es el día del Convenio 108 que acabo de mencionar y que en esa oportunidad se aprovecha, por otra parte, para hacer una cantidad de actividades de sensibilización.

Yo quisiera referirme a tu otra pregunta, porque tú ya hiciste la otra pregunta, de la situación de funcionarios también o de servidores.

Entonces, yo creo que es fundamental esa capacitación de servidores públicos y de empresas a nivel nacional e internacional.

En Uruguay hay una línea de capacitación permanente en distintos niveles, también de seguridad. Para mí el que sería un experto de primera sería Jorge Pérez obviamente, yo lo estaría convocando ya si estuviera más cerca, pero lo podemos hacer por medios virtuales.

En esos cursos de capacitación permanente hay básicos donde se dan principios, los conceptos, basándose en casos prácticos.

Los hay a requerimientos de los ministerios o de entes autónomos o de los gobiernos departamentales, o nuestra unidad, que es la que tiene la iniciativa si se presentan denuncias contra empresas o si hay consultan, se hacen cursos para delegados de protección de datos; delegados que, como creo que se dice deben tener hoy las entidades públicas, sean estatales o no estatales y las privadas que traten datos sensibles como el negocio principal o que efectúen tratamientos de gran volumen de datos.

La unidad nuestra ha emitido también días, digo por el tema de la capacitación, de la pregunta (…) de administración pública, el uso de videovigilancia con las distintas facetas que tienen la videovigilancia en materia de seguridad precisamente, mecanismos para anonimizar porque también son en el fondo vinculados a la seguridad mecanismos de bloqueo o de revisión periódica frente a las posibles subversiones, vinculado al famoso derecho al olvido que no me gusta el nombre porque hay que tener cuidado porque no hay que olvidar lo que no se debe olvidar, sino que es el mal curso a veces que se pueden hacer de los datos.

De manera que el tema de la sensibilización y de la capacitación son básicos porque, y yo creo que la exposición del doctor Joel Hernández a mí me resultó muy interesante, porque en Europa, el Tribunal Europeo de Protección de Datos, hace muchos años que yo trabajaba en este tema, ¿por qué? Porque el tema de protección de datos en Europa yo diría tiene una antigüedad mucho más grande, ya empezó en Alemania en la década del 70, la Ley Española es del 92, por ejemplo cuando nuestros países, estamos en leyes mucho más nuevas, y países de nuestro continente todavía no tienen legislación, no voy a nombrar porque ya se ha querido hacerlo, pero algunos por ejemplo como Brasil entró a regir ahora bien recientemente y Panamá también, pero hay algunos que todavía no tienen.

Entonces, creo que sería importantísimo el marcar que tanto por la Comisión, como por la Corte Interamericana se enfatizara en este tema. Creo que sería, trato de unir lo que yo estoy hablando con la primera exposición en el sentido de hacer notar la relevancia para la dignidad del ser humano que tiene estos datos, o sea la Constitución uruguaya no prevé expresamente este derecho como otras constituciones, como la brasileña, por ejemplo, la de Chile, desde hace poco, etcétera.

Pero la Ley de Protección de Datos de Uruguay dice que está incluido en una norma genérica abierta. Nuestra Constitución reconoce los derechos, deberes y garantías inherentes a la personalidad humana, y la ley ha dicho, bueno, la protección de datos personales está allí, es un derecho inherente a la personalidad humana.

Creo que entonces tenemos que unir valores esenciales, y la seguridad es básico. Si ustedes leen el reglamento europeo, los estándares, que yo nombré antes de la red, es un principio que ahora, con el carácter de la responsabilidad proactiva se impone como deber, no como para para tener un elemento burocrático y contar con un documento y tenerlo allí, sino para vivirlo el derecho, y también en materia de seguridad sirve para la vida, en este caso, para el reconocimiento de la dignidad del ser humano, y si no, perdón la terminología no muy adecuada, no sirve para nada.

De manera que, Reyna, yo creo que dejaría por acá, para no sé si estoy en tiempo todavía, pero no quiero tampoco pasarme del debido, que yo por mi reloj era el debido.

Reyna Lizbeth Ortega Silva: Muchísimas gracias, doctor.

Sin duda todo lo mencionado es muy interesante, y con toda la certeza del mundo. No nos podemos olvidar que existen principios y deberes en la materia de protección de datos personales. Que si bien estamos en una situación de excepción, y desde luego hay que salvaguardar el derecho fundamental, que es la vida y la salud.

No nos podemos olvidar de los otros derechos humanos y fundamentales que tenemos.

Y, desde luego, sin duda, capacitar, sensibilizar, concientizar a los servidores públicos, tanto a la ciudadanía es fundamental en el tema de protección de datos personales.

Y un tema que resaltó el doctor al principio de su exposición, ya el petróleo pasó a segundo plano. Ahora las bases de datos son el verdadero oro que tenemos en este mundo y que hay que cuidar más que nunca.

Muchísimas gracias, doctor Felipe.

Y continuando con el programa, ahora le toca el turno al maestro José Antonio Vázquez Acosta, quien es director de Ciberseguridad de Microsoft México.

De quien me permitiré decir también que con mucha experiencia, mucha trayectoria en el sector privado y, desde luego, con todo este tema de electrónica y comunicaciones, además de tecnología.

Maestro José Antonio, muchísimas gracias por regalarnos un espacio y lo escuchamos con atención.

Muchas gracias.

José Antonio Vázquez Acosta: Muchísimas gracias.

Gracias al INAI. Gracias, Comisionada Presidenta Reyna Ortega, muchas gracias por esta invitación; a mis distinguidos colegas panelistas.

Yo quisiera platicar un poco, Microsoft al ser una empresa global y que tenemos visibilidad de mucho de lo que pasa en términos de cumplimiento y en términos de todo este entorno regulatorio alrededor de la protección de datos personales, es bien importante también mencionar un poco el cómo.

Estamos de acuerdo y no puedo estar más de acuerdo con lo que han comentado los panelistas, en cuanto a que hoy en día estamos en la era de la información.

Muchos de los datos personales, que nosotros como individuos, como parte de una organización, como parte de una sociedad, cada vez estamos más inmersos en el tema de las herramientas digitales, y prueba de ello es este mismo foro en donde estamos haciendo uso de los canales digitales, para poder comunicarnos y para poder seguir avanzando en esta etapa tan complicada, que es la pandemia.

Y para las organizaciones y los gobiernos tampoco es algo fácil, es algo que representa muchos retos y para muestra un botón. Aquí lo que estoy mostrando son algunas estadísticas muy interesantes, donde nos dicen que el 88 por ciento de las organizaciones, no tienen confianza en detectar y prevenir pérdidas de información sensible o sensitiva, esto quiere decir que les cuesta mucho trabajo y que no se siente lo suficientemente fuertes para poder atender estos temas de protección de datos personales.

También, otro número importante es que más de 80 por ciento de la información corporativa, está en tinieblas.

¿Qué quiere decir esto? Que muchas veces las organizaciones no tienen claridad de dónde están sus datos, de quién tiene acceso a ellos, de cómo se procesan, cómo fluyen en todos sus procesos internos o externos, y eso es realmente grave, porque no podemos proteger lo que no controlamos y donde no tenemos visibilidad.

Y también, otro tercer dato importante, es que en el top on mine, una de las grandes prioridades que tienen en las organizaciones, es precisamente poder proteger y gobernar estos datos sensibles, estos datos personales, y es una de las preocupaciones más importantes que tienen los altos directivos de las organizaciones.

Y si esto no fuera suficiente, pues también tenemos dentro de este lance create y estas problemáticas, que existen muchísimas regulaciones, muchísimos estándares que también nos requieren tener ciertos controles, ciertas políticas, educación y una serie de actividades para que nosotros podamos garantizar que esta protección de datos va a ser muy relevante.

Y para empresas, por ejemplo, multinacionales, que son uno de nuestros tantos clientes que tenemos en Microsoft, realmente es un reto importante, porque cada regulación, cada país, tiene su propia regulación local, pero a la vez al ser un holding global, pues tiene que cumplir con reglamentos globales y esto obviamente representa un gran reto para este tipo de empresas.

Y hablando un poquito más de este tema de los retos, pues tenemos estos cuatro puntos que ya se han mencionado, un crecimiento acelerado de datos.

Hoy en día, no existe manera de que nuestros datos personales no estén en alguna plataforma digital, desde nuestras redes sociales, en donde podemos o no poner información personal, datos por ejemplo, que se pueden compartir con algunas instituciones; ahorita también comentaba nuestro panelista de la Ciudad de México, en estas herramientas digitales que ponen al servicio de la ciudadanía, pue también nosotros como ciudadanos ponemos datos importantes, y ya no digamos las empresas.

Desde que una empresa nos contrata, enviamos nuestro currículum, somos parte de la nómina, somos parte de los sistemas de información, etcétera.

Todo este mundo de información está en formatos digitales y tenemos que establecer esos mecanismos que nos permitan protegerlos adecuadamente.

La creciente complejidad del negocio. Hoy en esta dinámica en donde la tecnología nos ha permitido salir adelante y ser más competitivos y estar conectados en este mundo global, también implica complejidad.

Y sabemos que esa complejidad también representa riesgos a la seguridad de los datos y las organizaciones cada vez más están preocupadas y están ocupadas en poder definir los mecanismos que les permitan proteger adecuadamente.

También hay un poco adaptación a los constantes cambios normativos. Esto por supuesto que celebro que existan este tipo de leyes, de regulaciones, porque es un derecho, un derecho humano como ya lo han expresado; pero también, hay que decirlo, muchas de estas regulaciones son muy cambiantes y cambian drásticamente en muchos casos.

Y es muy complicado para las organizaciones seguir el ritmo, seguir el paso de este tipo de cambios y representa un reto importante.

Y por último, el tema del cumplimiento continuo de normativas. En el caso de ciertas regulaciones que tienen un impacto no solamente en términos de multas, que es una de las preocupaciones más importantes, pero también en términos de la reputación.

Un periodicazo, una mala noticia por una fuga de datos personales o algún incidente relacionado a este tipo de situaciones, afecta gravemente o puede afectar gravemente la reputación de una organización, y esto le puede representar grandes daños.

Este es como el panorama. Pero la siguiente pregunta importante es: ¿qué estamos haciendo como organizaciones, como países, como individuos para proteger los datos?

Y aquí hay tres preguntas iniciales. ¿Sabemos dónde reside nuestra información crítica y qué se está haciendo con ella?

Tenemos que partir de estas preguntas que son fundamentales para poder dar los siguientes pasos.

La segunda sería. ¿Tenemos control de estos datos tanto al interior, como al exterior de nuestra organización?

En este mundo conectado tenemos una diversidad de socios de negocio en donde intercambiamos información, en donde nuestra información no solamente se mueve al interior de nuestro entorno, sino también hacia el exterior a través de estas herramientas digitales y el internet.

Y la tercera pregunta podría ser: ¿estamos utilizando soluciones digitales para clasificar, etiquetar y proteger esos datos?

Porque algo que es cierto es que es humanamente imposible que nosotros podamos hacer esta protección de datos, sino es a través del uso de las tecnologías.

¿Por qué? Porque son muchísimos datos, muchísimos procesos, muchísimas fuentes de información, y si no es a través de la tecnología, francamente va a ser una tarea que no vamos a poder realizar.

Ahora, es bien importante que las organizaciones definan un programa de protección de datos basado en las regulaciones, basado en los *frameworks*, que afortunadamente también existen muchos y muy buenos y que básicamente estos plantean los mismos principios.

Esa es una lámina de un socio de negocio de nosotros que es TWC, en donde plantea estos cinco pasos que por supuesto podemos hacer un zoom a cada uno de ellos y puede salir muchísima información, pero esto nada más como para dar un panorama general.

Necesitamos manejar perfectamente los datos de terceros, identificar cómo y de qué manera intercambiamos información con estas entidades, socios, clientes, gobiernos, ciudadanos, etcétera, y cómo vamos a tener este mapeo de esa información y esos datos que podemos compartir.

Segundo, analizar el impacto a la privacidad. Estos datos que yo genero o que yo obtengo de alguna fuente cómo me va a afectar y cómo puede afectar la privacidad de las personas en ese sentido y en ese proceso.

Después tener claridad en las políticas de privacidad, cómo voy a proteger esos datos una vez que ya los identifiqué y una vez que ya supe qué impacto puede tener en temas de privacidad.

Cuarto, designar a un oficial de protección de datos. Es súper importante tener dentro de las organizaciones una persona que pueda rendir cuentas en términos de los datos personales, y de ahí por supuesto generar un programa de protección de datos que puede incluir ciertos niveles de controles que puede ser a nivel de políticas, a nivel de procesos y a nivel de tecnologías como muy bien nos explicaba nuestro colega de la Ciudad de México.

Ahora, dentro de esta estrategia de protección y de gobierno de datos tampoco es algo tan complejo que no podamos hacer.

Esta es un poco la propuesta que tenemos en Microsoft de cómo poder empezar a tener un panorama claro y un programa que podamos implementar.

Primero y súper importante, tenemos que conocer nuestros datos, en dónde viven, en qué bases de datos, en qué documentos, en qué plataformas, porque nuevamente yo no puedo proteger lo que no conozco, donde no tengo visibilidad y nuevamente la tecnología nos tiene que dar estas capacidades de búsqueda automatizada y de manera masiva para que podamos identificar qué información y en dónde reciben.

Segundo, cómo voy a proteger esa data, cómo voy a proteger esos datos una vez que yo ya los identifiqué. Entonces, yo necesito identificar qué tipo de dato es, clasificarlo con base en las regulaciones y con base en las mejores prácticas a las cuales me apliquen, para que entonces sí yo pueda aplicar el control que me va a permitir proteger ese dato de manera adecuada.

Y dentro de los controles que también algunos los comentaban está el tema de la encripción, marcas visuales o marcas de agua por ejemplo en los documentos, o incluso algunas reglas de prevención de fuga de información. Todo esto lo podemos hacer a través de la tecnología afortunadamente ya existen este tipo de herramientas y que, sin duda, va a ser la mejor manera de poder enfrentar estos retos.

Y, tres, ¿cómo gobernamos esos datos? Porque no nada más se trata de identificarlos y protegerlos, tenemos que gobernar todo el ciclo de vida de la información, desde que se genera, desde que la capto, después cómo la clasifico, cómo la etiqueto, cómo la resguardo y cómo la destruyo porque incluso y toda la red y todas las regulaciones hablan de ese ciclo de vida de la información e incluso al momento de destruir información necesitamos garantizar ciertos controles y ciertos mecanismos que nos den certeza de que esa información realmente fue desechada de una manera adecuada, que nos dé tranquilidad que están resguardados nuestros derechos.

Y, por último, nada más comentar que dentro de este enfoque empresas tecnológicas como Microsoft que hemos identificado y que incluso tenemos dentro de nuestras líneas de negocio y dentro de nuestras líneas de negocio y dentro de nuestros servicios muchísima información de muchísimos clientes alrededor del mundo.

Entonces, lo primero es que nosotros tenemos que garantizar que toda esa información está protegida, y lo hacemos a través de un enfoque unificado, esto quiere decir que este descubrimiento y clasificación de datos lo tenemos claramente automatizado.

Segundo, que esos mecanismos de protección también los automatizamos, de tal manera que esto tenga una rapidez y una cobertura mayor a todos los datos que nosotros podemos tener, un monitoreo proactivo de qué está pasando con esa información, de que no esté siendo usada de una manera indebida, y todo esto también a través de mecanismos digitales y, por supuesto, esto nos da una cobertura realmente importante que nos pueda garantizar primeramente a nosotros, como empresa, que nuestros datos están protegidos, pero también hacia nuestros clientes y hacia nuestros socios de negocio que evidentemente es una preocupación y es algo que tienen que atender.

Entonces, hasta aquí mi participación.

Nuevamente gracias y gracias por la atención.

Reyna Lizbeth Ortega Silva: Muchísimas gracias, maestro José Antonio.

Pues sí, habla de temas muy interesantes que recordando un poco también ahorita la exposición del doctor Felipe, lo mencionó también, allá por el tema de delegados de protección de datos personales, y aquí por el tema de oficial de datos personales.

Entonces, tenemos mucho tema aún que trabajar por esa parte, y desde luego el punto de partida: conocer qué son los datos, cuáles son nuestros datos, cómo vamos a proteger nuestros datos y, desde luego, nuestros retos. Seguimos teniendo muchos retos y ahorita con el tema sanitario se dispararon esos retos, porque ahora son retos y desafíos que tenemos que cumplir, y cómo lo vamos a hacer, es justamente toda esa parte.

Muchísimas gracias.

Y continuando con el programa, ahora vamos a una segunda ronda, no sin antes comentarles que el doctor Joel se tuvo que retirar por temas de agenda. Nos deja un abrazo, un saludo a todas y a todos ustedes.

Y continuamos con nuestros tres panelistas. Tengo una preguntas de las personas que están siguiendo este panel, y que me voy a permitir realizar, quien la quiera contestar, por favor, el uso de la voz se lo daré.

La primer pregunta, que por cierto es muy interesante dice: ¿qué tratamiento se le dará a un dato sensible, esta de salud presente y futuro de una persona que tuvo COVID-19, sintomático o asintomático, por las secuelas que pudiera tener y que pretenda acceder a un seguro de vida o a un trabajo?

Una pregunta muy interesante. No sé quién de ustedes la quiera contestar.

Doctor Felipe, maestro José Antonio, Jorge. Lo escuchamos.

Felipe Rotondo: La pregunta es muy interesante y requiere como siempre sucede en muchos de estos temas ponderación. O sea, el criterio de qué datos realmente se necesitan.

El criterio de ponderación es una forma de proporcionalidad; qué datos son necesarios para algo, porque por ejemplo, yo acredito datos sensibles y accesibles.

Si son, por ejemplo, con un tratamiento de salud, evidentemente tiene que darse el dato de salud, pero para contratar un seguro, evidentemente puede incidir, pero hasta qué grado, qué detalle, todo eso es lo que hay que ver, y el caso a través de los principios de ponderación, que se nos fue el doctor Joel, pero lo manejan, se maneja mucho a todo nivel, tanto doctrinario, como jurisprudencial y en materia de la práctica administrativa.

O sea, principios de criterios de proporcionalidad, ¿cuáles son? La necesidad, qué es necesario, si no es necesario no hay que darlo, la finalidad legitima, está el propio interesado queriendo que se entregue, es conveniencia para él, por ejemplo, y luego la proporcionalidad propiamente dicha, digamos.

O sea, no sé si está clara mi respuesta, estimada doctora Reyna, pero no estoy contestando sí o no, sino estoy viendo que tenemos que ver desde la situación concreta, cuáles son las condiciones que se establecen para ese contrato de seguros y quién lo está haciendo, quién lo solicita, cómo ahora mismo pasa.

O sea, con respecto, perdón, voy a cambiar de tema, así que mejor no hablo, porque iba a poner otro ejemplo, o sea, el tema con determinados usos de aplicaciones que se vienen haciendo, acá en el Uruguay se está haciendo, nuestra unidad emitió orientaciones a sus edictos, en la medida que, es otro tema, otro tema y no quiero cambiar de tema Reyna, pero si depende de mi consentimiento, soy yo el que quiero que me controlen, y no implica geolocalización, etcétera, y se cumplen los otros principios, los otros principios siempre tienen que estar presentes.

O sea, porque el consentimiento no será necesario para dar determinados datos de salud, pero por qué hay que decirle a cualquiera, que fulanito está teniendo tal enfermedad, no.

Solamente hay que avisar a aquellos que puedan estar involucrados o que puedan contagiarse, pero sin necesidad de saber el origen, o con

quién estuvo cerca, y eso es lo que se ha hecho con la aplicación que se está utilizando en el Uruguay.

O sea, estoy cambiando de tema, y traté de responder la pregunta, porque para contestarla bien, bien, tendría que tenerla escrita y bien meditada cuáles son las condiciones.

Reyna Lizbeth Ortega Silva: Muchísimas gracias, doctor Felipe.

Y continuando con las preguntas, tengo una que está muy interesante, que seguramente nos van a poder ayudar, no sé si el maestro Jorge o el maestro José Antonio, pero dice: Ahora que se están pidiendo un registro de clientes con código QR, en los negocios de la Ciudad de México para rastrear contagios, ¿deben señalar un aviso de privacidad y protección de datos personales?

Jorge Luis Pérez Hernández: Sí, es correcto.

De hecho, esta pregunta tiene más que ver con lo que respondía al final el doctor Felipe.

En Uruguay es por medio de una APP que gestiona contactos cercanos a través de bluetooth.

En la Ciudad de México, es diferente, si bien esa APP se desarrolló, nunca salió a la luz, está disponible, pero nunca salió precisamente por temas de protección de datos; es algo que quedó ahí detenido.

En este caso en la lectura del QR, recordemos, llegas a un establecimiento, lo lees, y únicamente te va a abrir un portal y tú ingresas tu número telefónico; no hay ningún otro dato y ahí viene el aviso de privacidad, no hay ningún otro dato, pero sí entendamos que el número telefónico ya es un dato personal, no se vaya a confundir la gente con que nada más estoy dando mi número, no estoy dando mi nombre, no es un dato personal; no es así.

Es el número, pero ese número ya es un dato personal y es todo lo que se pide, únicamente se pide el número telefónico.

Y abonando un poquito a esto y con relación a lo que comentaba hace unos momentos el ex panelista, se borran estos datos cada 15 días precisamente porque son únicamente para ubicar las zonas donde estuvieron los casos positivos y que pudieron haber contagiado a alguien más, únicamente se resguardan por 15 días, no se necesita más tiempo esta información.

Reyna Lizbeth Ortega Silva: Muchísimas gracias, maestro Jorge.

No sé si quiera comentar algo algún otro de nuestros panelistas. José Antonio, doctor Felipe.

Adelante.

Felipe Rotondo: Quisiera acentuar de lo que acaba de decir el expositor recién, que me pareció muy bien, él acaba de señalar un tema importante: el tiempo.

La finalidad, hay un responsable que en el caso uruguayo quién tiene que ser, el Ministerio de Salud Pública; hay un responsable, no puede ser sino otro, o sea, es el Estado el responsable.

Los otros principios siguen existiendo y ahí Jorge acaba de decir justamente uno: hasta cuándo es necesario mantener ese dato.

Eso está incluido dentro del principio de razonabilidad en el uso de los datos, y más si son sensibles.

Simplemente quería decir algo que no sé si vamos a perder el minuto final, pero frente a lo que se expuso también y que se tiene la razón, estoy cambiando de tema, Reyna, si no me callo y lo digo después.

Reyna Lizbeth Ortega Silva: Adelante, doctor.

Felipe Rotondo: Lo que iba a decir es que hay una realidad que hizo referencia el último participante que es el tema de los constantes cambios normativos.

Y esos son temas muy importantes, porque claro, en Europa hay un Reglamento General obligatorio para todos los países europeos que integran la Unión Europea.

Nosotros no lo tenemos en América, ese es un tema, los estándares son como una especie de *softlow*, pero no son obligatorios.

Y por eso ustedes verán que yo reitere tantas veces el tema de principios, porque creo que los principios siempre son permanentes. Cambiarán las leyes, cambiarán las tecnologías, muchas veces la ley va detrás de la tecnología, no siempre, pero muchas veces; pero los principios de razonabilidad, de finalidad, de la veracidad, de la exactitud de los datos, no voy a cansarlos, etcétera, seguridad, tienen que ir siempre, son permanentes y, por lo tanto, la empresa cuando lo hace lo tiene que hacer ya sabiéndolo eso, asumiéndolo como tal.

De manera que por eso tú bien decías la importancia de lo que nosotros llamamos delegados, ustedes llaman oficial de protección de datos, pero es la figura clave dentro de una empresa o una entidad en esta materia.

Subrayo entonces que el derecho no está cambiando permanentemente, sino en algunos aspectos. Pero el que hace un diseño tiene que saber ya al diseñarse una aplicación que existe estos principios que no cambian.

Si es para determinar finalidad, por ejemplo, el uso médico, es para eso y no para otra cosa.

Perdón, no quiero robar tiempo.

Reyna Lizbeth Ortega Silva: Muchas gracias, doctor.

Maestro José Antonio, te escuchamos.

José Antonio Vásquez Acosta: Gracias.

No puedo estar más de acuerdo con lo que dice el doctor Felipe. Yo creo que nosotros como ciudadanos tenemos que ser conscientes y saber que existen estos mecanismos, muchas veces no nos gusta leer

los avisos de privacidad, esa es una realidad, pero es bien importante que busquemos en nuestros avisos de privacidad ese rubro de finalidad, porque es en sí la que nos va a dar la certeza razonable de cuál va a ser el uso que le van a dar a nuestros datos personales, y una vez teniendo claridad de cuál es esa finalidad nosotros podemos decidir si damos ese dato personal o no.

Eso es algo muy importante y muy interesante.

Y como también reforzaba el doctor Felipe, los principios se mantienen.

Yo en mi intervención que platicaba un poco el cómo, que a través de la tecnología ya nosotros podemos automatizar mucho de estos principios que están en nuestras políticas y que nosotros los traducimos a un lenguaje digital y que estas herramientas digitales nos permiten ejecutar ese principio de una manera mucho más automatizada.

Pero, sin duda, es bien importante saber que detrás de todas estas soluciones y detrás de todas estas herramientas están esos principios fundamentales y que, por supuesto, que también están bajo el escrutinio de auditorías y de revisiones de terceras partes, de organismos independientes, que realmente pueden dar fe de que esos principios están debidamente aplicados y que también existen los mecanismos de auditoría y de control para garantizar en todo momento la integridad y seguridad de esa información.

Reyna Lizbeth Ortega Silva: Muchísimas gracias, maestro José Antonio.

Y si me permiten por cuestión de tiempo tenemos mucho tema de qué hablar, sin duda este es un tema muy importante, nuestros ponentes son magníficos y quisiéramos seguir escuchando pero tenemos que continuar con el programa de la Semana Nacional de Transparencia.

Sin duda, como lo escuchamos, los datos personales, la privacidad, la intimidad, el honor y, desde luego, todos estos derechos fundamentales que tenemos las y los ciudadanos son fundamentales y debemos seguir cuidándonos y protegiéndonos.

Hemos visto este tema sanitario que nos ha complicado mucho las cuestiones de vivir día a día, pero también por otro parte, y lo acaban de mencionar todos nuestros panelistas qué está pasando con la tecnología que nos está aligerando la vida, pero que ahora tenemos otro gran reto, cuidarnos dentro de esta tecnología y desarrollo de las acciones que desarrollamos día a día todas nuestras medidas de privacidad e intimidad y, desde luego, cuidar nuestra información digital que está en las plataformas digitales.

Muchísimas gracias a todas y a todos los que están siguiendo esta transmisión en vivo. Muchas gracias al INAI por el espacio y muchísimas gracias, desde luego, a nuestros ponentes.

Doctor Felipe, un fuerte abrazo hasta Uruguay, es un honor haber compartido mesa con usted.

Maestro José Antonio, muchísimas gracias, un fuerte abrazo y, desde luego, maestro Jorge, un gran, gran abrazo.

Muy buenas tardes a todas y a todos.

Presentadora: De esta manera concluye el panel *Herramientas y medidas de seguridad para resguardar datos personales sensibles.*

Agradecemos a nuestros distinguidos participantes, así como a la moderadora del panel, la Comisionada Presidenta del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, y Coordinadora de la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia, Reyna Lizbeth Ortega Silva.

Solicitamos a todos los presentes permanecer conectados, ya que en unos minutos dará inicio la Ceremonia de Clausura.

Muchas gracias.

- - -o0o- - -