Panel 2: “Esquemas de Protección de Datos Personales”.

Presentador: Para continuar con los trabajos del Día Internacional de Protección de Datos Personales 2019, daremos inicio al panel número 2 denominado “Esquemas de protección de datos personales”, para lo cual cedemos el uso del micrófono a la Comisionada Ciudadana del InfoDF Marina Alicia San Martín Rebolloso, quien moderará este panel.

Marina Alicia San Martín Rebolloso: Muchísimas gracias, muy buenas tardes, bienvenidos.

Gracias a todos por volver después de la comida, son unos guerreros en este evento, espero lo estén disfrutando, porque ahora vamos a un tema y me honra mucho estar en esta mesa con destacados, digamos, litigantes, académicos y que nos van a dar un enfoque muy interesante de lo que hemos visto el día de hoy.

Vamos a tratar el tema de “Esquemas de protección de datos personales”. Agradezco mucho la presencia de Rebeca Servín, de Microsoft; de Carmen Quijano Decanini, de la Barra de Abogados; Cynthia Solís Arredondo, de Barra de Abogados; Mauricio Hernández Aguilar, de Barra de Abogados. No pongo títulos nobiliarios, los leeré en sus currículums, pero para que estemos en charla y en confianza.

Les pido y les comento la dinámica de la mesa. Tenemos poco tiempo pero lo vamos a hacer lo más efectivo posible, siéntanse con libertad de hacer cualquier tipo de pregunta y nos las hacen llegar para que yo pueda con los ponentes empezar a socializarlas.

Y lo que pondría en la mesa para todos los que están aquí acompañándonos de panelistas, antes de iniciar y presentar a cada uno y dar su reseña, en todo el día hemos trabajado el tema de datos personales desde distintos enfoques. En la mesa de en la mañana comentamos temas de implementación: cuáles han sido los retos, dónde estamos parados en México, cómo hemos venido avanzando y cómo hemos podido llevar en la parte de sujetos obligados la aplicación de la norma que en privados, a nivel federal, ya está mucho más avanzado.

Posteriormente tuvimos la oportunidad de escuchar ponencias sobre portabilidad, con la presencia de la agencia digital y del Comisionado Guerra, hablándonos un poco de cómo el ciudadano tiene que ser el centro, y empezaríamos por ahí, y cómo él no tiene que sufrir, tiene que ejercer su derecho de manera libre e ir a un solo sitio, una sola ventanilla y ahí que le resuelvan todos sus trámites, pero atrás de eso, atrás de eso tenemos un tema de garantizar ciertas medidas de seguridad, y por eso el tema de “Esquemas de protección”.

Y en el último tramo el doctor Puccinelli nos dijo todo un recuento de la revolución que hemos tenido de internet, las problemáticas que ha habido, derechos futuristas ya prácticamente irreales en pensar, de la mente y que ya el internet de las cosas nos tiene perfectamente identificados, perfiles y demás, y esas problemáticas quisiera que ustedes lo echo a la mesa, con su experiencia pudieran compartirnos temas de medidas de seguridad, cómo podemos garantizar que este derecho sea efectivo y que efectivamente el ciudadano no batalle o no le generemos cargas en su ejercicio, pero a la vez blindemos la y exista un tema de confianza, dándonos cuenta de las prácticas que han ustedes vivido como usuarios o como litigantes, y ese enfoque creo que será muy enriquecedor.

Y cedería la palabra, bueno, les pediría que tengamos como 15 minutos para que podamos tener chance de debatir, si les parece bien. Y cedería la palabra a Rebeca Servín.

Te doy un breve *briefing* para que sepan quién está aquí al lado mío y el orgullo que es compartir mesa contigo.

Ella es Directora de Asuntos Jurídicos y de Filantropía de Microsoft México, egresada de la Universidad Panamericana, abogada *senior* con más de 20 años de experiencia brindando asesoría legal a subsidiarias mexicanas de corporaciones globales como Microsoft, British Telecom, COMSAT y Telmex. Cuenta con muchísima experiencia como abogada transnacional, en equipos de redacción y negociación de acuerdos, incluyendo de transformación digital.

Colaboradora de relaciones con clientes y colegas, oradora versada que trabaja con autoridades, campañas y organizaciones de la compañía.

Más que bienvenida. Te cedo el uso de la palabra.

Rebeca Servín Lewis: Muchísimas gracias, Marina.

Quiero agradecer a InfoDF por invitarme a este evento que sé que es muy importante. Para nosotros como industria es muy, muy importante que nos inviten para que nosotros les demos nuestro punto de vista.

El tema de la protección de datos, Microsoft mucha gente la tiene ubicada como una empresa que se dedica a diseñar solo programas de cómputo.

Realmente Microsoft en los últimos años se ha transformado. Entonces, además de seguir haciendo y desarrollando software, en realidad Microsoft ahora es una empresa de plataformas y lo que presta principalmente son servicios en la nube.

Me parece que esa discusión ya se tuvo antes de la comida entonces no voy a entrar al tema, lo que les quiero platicar es cuál es la visión de Microsoft como empresa transnacional, con presencia en 194 países en el mundo; cómo ve el tema de la protección de datos.

Bueno, la realidad es que primero, la protección de datos ¿por qué nosotros la vemos como que se tiene que cumplir? ¿Por qué nosotros cumplimos con las leyes locales? En primer lugar porque es un derecho fundamental, está reconocido, seguramente ya lo platicaron anteriormente en la Constitución, también en la Declaración Universal de los Derechos Humanos del 48, pero además también por un tema muy práctico, que es que este tipo de legislación y de regulación tiene sanciones súper elevadas.

En el caso de México hay multas altísimas, pero en el caso del Reglamento General de Protección de Datos Europeo, que seguramente ya también lo han platicado, tiene unas multas que son impensables, que es un porcentaje de las utilidades mundiales.

¿Y por qué es importante hablar de este reglamento en estos foros? Porque el día de hoy es la vara más alta que tenemos en materia de protección de datos, y seguramente hacia donde toda la normativa mundial irá yendo, probablemente.

Ahora, no es malo que haya ese movimiento hacia esas normativas mundiales, porque al final el ciudadano queda en el centro de la protección de estas normativas. Adicionalmente porque es un tema también reputacional, nadie utiliza tecnologías o servicios en los que no confía. Entonces en Microsoft la realidad es que a nosotros nos preocupa muchísimo la reputación que tenemos porque nuestros clientes usarán nuestros servicios en tanto confíen en nuestras tecnologías y se sientan seguros.

Bueno, Microsoft tiene una estrategia de nube donde la persona, me encantó lo que dijo Marina de: el ciudadano tiene que estar en el centro, porque justamente es la filosofía de Microsoft respecto de la nube.

Los ciudadanos o la persona siempre estará en el centro. Y vamos a hablar de que Microsoft diseña sus productos y sus servicios pensando en la persona y en la protección de su información desde el diseño de sus productos.

Por ejemplo, vamos a pensar en un principio que se utiliza siempre que se hace un diseño, que es el uso mínimo de datos personales. Siempre se recabarán los datos personales que se requieran específicamente para diseñar algo, para comprobar algo, ahora con el tema de inteligencia artificial, que ya oí que también estuvieron platicando de él. Efectivamente, muchas veces para probar o para diseñar un algoritmo se requieren datos personales, uno necesita datos para que funcione el sistema, para que pueda tener o para que pueda hacer una predicción, ¿no?

Entonces, desde el diseño lo que Microsoft hace es diseñar sus productos tratando de tomar los principios de la protección de datos.

Otro ejemplo que les voy a dar es, por ejemplo, el uso de correo electrónico. Microsoft podría reservarse el dato de la dirección IP que

es un dato personal, y no lo toma, ¿por qué? Porque no es necesario conservarlo.

Bueno, compromisos por contrato ahora lo vamos a ver más adelante, y transparencia es el otro pilar.

Compromisos por contrato. Microsoft en sus contratos tiene un documento muy especial que se llama “Términos de los servicios en la nube”, que aplican a todos los servicios. Desde el principio se establece que en cada país Microsoft cumplirá con las leyes locales, entonces en el caso de México el contrato se adecua perfectamente bien a la Ley de Protección de Datos y cumple con los requisitos que para la prestación de servicios en la nube requiere el reglamento y la ley.

Cabe mencionar que Microsoft hemos subido la barra, como les decía, y cumplimos con el reglamento de la Unión Europea, porque nos parece que el ciudadano, las personas, nuestros clientes en general quedan más protegidos.

Nosotros transparentamos donde los datos de las personas se encuentran. La realidad es que en México no tenemos centros de datos el día de hoy, pero generalmente los servicios que se prestan a las empresas y a los ciudadanos mexicanos se sitúan generalmente, dependiendo del tipo de servicio de que se presente, en centros de datos que se encuentran ubicados en Estados Unidos.

Eso es muy importante porque la gente tiene que estar tranquila de que sus datos no van a ser transferidos a un país que no tenga niveles de protección de datos suficientes o que sea un país confiable en esa materia.

Adicionalmente, más adelante les voy a mencionar con qué tipo de estándares cumplen todas sus nubes, nosotros transparentamos quiénes son nuestros subcontratistas y tenemos las cláusulas contractuales tipo nuestros contratos, y estamos registrados en el *Privacy Shield.*

Ahora, en el caso de los prestadores de servicios en la nube, viendo la legislación mexicana ¿qué figura seríamos? Pues la de un encargado.

Entonces nosotros ¿por qué nos eligen los clientes? Porque siempre se respetan los roles. El responsable nos instruye para que nosotros prestemos un servicio, y nosotros como encargados del tratamiento seguimos las instrucciones, transparentamos a los subcontratistas y cumplimos con medidas de seguridad que más adelante les voy a decir dónde las pueden ver, porque transparentamos toda nuestra información.

Nuestros contratos específicamente cumplen con la ley mexicana, al establecer que los datos personales de los mexicanos nunca van a ser de Microsoft, nosotros no tomamos la titularidad de esos datos, de esta información, y nunca usaremos la información para ningún otro propósito diferente al que nos instruyó el responsable.

Es decir, nosotros no somos una empresa de publicidad que busca y mina y hace un *squinting*, o sea está viendo el contenido de su información para hacerles una oferta mercantil de productos y servicios en general.

Bueno, de GDPR, del reglamento de la Unión Europea, como les mencionaba, inclusive nosotros, bueno, ya les expliqué lo de las cláusulas modelo y del *Privacy Shield*, ahora, nosotros tenemos adicionalmente sistemas para que nuestros clientes cumplan con el reglamento de datos de la Unión Europea.

Por ejemplo, tenemos este sistema que se llama *content search*, donde estos cuadritos van escogiendo, es propio de nuestros sistemas y el otro servicio que les, a ver, nuestro sistema tiene funcionalidades que protegen sus datos y que los ayuda a cumplir con la normativa. Este producto en particular lo que hace es que clasifica la normativa y las políticas no solo del GDPR, del reglamento de la Unión Europea, sino de otras normativas internas de protección de datos.

Y va monitoreando que efectivamente el uso que se da a través de *Office 365* vaya cumpliendo, y va calificando qué tan buen uso de esos datos se hace.

Este es el *compliance manager*, abajo ven los cuadritos que va monitoreando cada una de las normas aplicables y de las políticas corporativas que le aplican al cliente. Esto se va diseñando conforme

el cliente lo va utilizando y se va seleccionando qué funcionalidad o qué norma, qué condición se tiene que cumplir para que el propio sistema vaya calificando ese uso.

Respecto a la transparencia, esto es muy importante porque nosotros tenemos en un sitio que se llama el *Trust Center*, o sea, el centro de confianza, todas las certificaciones que le aplican a las nubes de Microsoft, que son tres; todas las auditorías, nosotros transparentamos respecto de cada compromiso contractual se hace una auditoría por un tercero independiente, y ese reporte de auditoría que se publica anualmente se encuentra en este *Trust Center*. Adicionalmente a este tipo de transparencia, bueno, estas son todas las certificaciones, si se fijan en la parte de abajo está certificado por muchos entes reguladores de datos personales.

Entonces ¿eso qué nos da? Que nuestros clientes pueden estar tranquilos, que Microsoft de verdad lo que se refleja en el contrato es lo que se va cumpliendo en el tiempo.

Otra cosa que les quería platicar pero creo que no viene en la liga, es mucha gente está muy nerviosa generalmente respecto del acceso de los datos, no solo los datos personales que podría tener una autoridad, en el caso particular tal vez una autoridad en Estados Unidos.

Esta discusión la verdad es que es bien difícil porque al final todos los países tienen leyes que les permiten acceder a comunicaciones. En México la Ley de Seguridad Nacional tiene un capítulo que permite a un juez de distrito generar una orden para que intervenga una comunicación, lo mismo pasa en Estados Unidos.

Ahora, la diferencia de Microsoft con otras empresas es que nosotros transparentamos todas las solicitudes que nos hacen las diferentes autoridades, porque no necesariamente nos va a pedir una autoridad algún contenido.

Respecto de México cada seis meses se publica el Transparency Report, Reporte de Transparencia, donde cada seis meses Microsoft reporta a sus clientes y transparenta cuántas solicitudes de diversas autoridades del mundo se requirieron respecto de sus clientes corporativos.

El día de hoy les puedo decir que generalmente son temas del registro del cliente, nombre del usuario de una cuenta de correo, dirección IP a la que está asociada ese tipo de correo, pero en el caso de México generalmente no entregamos, al día de hoy nunca se ha entregado ninguna información de contenido.

Entonces, yo lo que les quiero transmitir con esta breve presentación es que los servicios en la nube son buenos, la verdad es que generan eficiencias, nuestro mundo ya no se puede entender sin este tipo de capacidades. La gente tiene que quitarse el miedo y dejar de pensar que la nube es un concepto etéreo de “mis datos están en la nube, por ahí andan”. No, están en un servidor que no está dentro de las instalaciones de la institución para la que ustedes trabajan.

Eso no quiere decir que no haya seguridad. Al revés, una empresa como esta invierte billones de dólares en seguridad, sus centros de datos tienen los más altos estándares de seguridad para que ustedes y su información esté siempre disponible y que ustedes siempre puedan accesar, siempre la puedan borrar, siempre puedan disponer y siempre la puedan portar a otro proveedor.

Si no existieran los servicios en la nube, no se podrían hacer grandes transacciones, no tendría una computadora, una PC o un servidor o un centro de datos propio de una institución; no tendría la capacidad para comparar o para procesar esas cantidades de información que nos pide el día a día, y para tener eficiencias, hasta para tener ahorros.

Entonces yo lo que les pido es que consideren que los servicios en la nube son buenos, simplemente nos tenemos que fijar en que la empresa que está prestando el servicio tiene las medidas de seguridad suficientes, es una empresa que cumple con la ley mexicana, y si tiene todavía una barra más arriba, como sería el Reglamento de la Unión Europea, qué mejor, porque vamos a tener una mejor protección.

Yo les agradezco este tiempo que me dieron la oportunidad que compartir con ustedes un poco lo que Microsoft ofrece en general a sus clientes corporativos.

Muchísimas gracias.

Marina Alicia San Martín Rebolloso: Muchas gracias, Rebeca.

Tomando el ejemplo que nos da Rebeca rescato de su ponencia, y obviamente para generar el debate y entrar ahí, trasladado a sujetos obligados, la parte de confianza y la finalidad para lo que recabamos. Creo que el tema de confianza es un eje para que nosotros como ciudadanos nos sintamos con la libertad de poder dar con tranquilidad nuestros datos y efectivamente que la nube no es mala, que generar servicios que faciliten nuestra vida es bueno, solamente que garantizar esa autodeterminación. Es decir, yo decido qué sí y qué no y que no me estén vigilando o que eso esté en riesgo y demás.

Y doy la palabra, para seguir con estos temas, a Carmen Quijano. Carmen Quijano es abogada egresada de la Universidad Iberoamericana, maestra en Derecho Comparado por la Universidad de Nueva York y candidata al grado de doctor por el Instituto de Investigaciones Jurídicas.

Fue miembro del Consejo Técnico de la Facultad de Derecho de la Universidad Americana, y actualmente imparte la cátedra de Protección de Datos Personales en esta Universidad Panamericana.

Es miembro del Comité Jurídico de la Asociación Mexicana de Internet y asociada de la Barra Mexicana, Colegio de Abogados A.C.

Actualmente coordina la Comisión de Transparencia y Protección de Datos de dicho Consejo. Socia fundadora del Bufete Quijano, que ha desarrollado su práctica profesional como abogada corporativa de empresas privadas, especialmente en tecnologías de la información-

Bienvenida y adelante, muchas gracias.

Carmen Quijano Decanini: Gracias.

Gracias al InfoDF, es un honor y me encanta estar aquí con colegas a los que conozco bien y a los que admiro. Vale la pena decir que seguramente voy a hablar muy bien de ellos y de Microsoft especialmente, y ahorita les voy a contar por qué. Pero tengo la

seguridad de que es una empresa seria y sobre todo participativa y comprometida. Va a parecer anuncio de Microsoft, qué horror, pero se los tengo que decir porque es verdad que es una empresa comprometida con los datos personales.

Bueno, yo les quiero hablar muy rápidamente pero creo que es un tema súper, pareciera básico pero es súper importante, sobre la diferencia entre la privacidad y la protección de datos, que son dos cosas muy distintas, y que viene mucho al caso ahora que la inclusión del derecho fundamental a la protección de datos personales en nuestra Constitución cumple 10 años, porque fue en 2009 que se incluyó el derecho fundamental a la protección de datos personales como un derecho humano autónomo en el artículo 16 constitucional.

Entonces ya cumplimos 10 años. Y siempre me ha intrigado y siempre lo digo y me encanta seguir analizando ese tema, cómo es que llegamos a consagrar en nuestra Constitución este derecho y no expresamente el de la privacidad.

Entonces primero quiero entrar por qué es la privacidad y qué es la protección de datos personales. La privacidad es el derecho que tenemos todos de decidir qué parte de mi vida quiero compartir con los demás, pero no se refiere solo a información sino se refiere a espacios, a creencias, al cuerpo humano, a todo lo que tiene que ver con mi ser, qué parte de mi ser humano quiero mantener en la intimidad y qué parte quiero compartir.

En cambio, la protección de datos se refiere a la información, qué parte de mi información quiero controlar y quién quiero que la vea, quién quiero que no la vea. Y en eso son distintos, la privacidad abarca mucho más, podríamos decir que es el género, y la protección de datos es la especie.

Aquí el tema es que el tema de la protección de datos surgió con los inicios del internet, con la red 1.0, cuando el internet era unidireccional. A los inicios del internet, si ustedes se acuerdan, se tenía acceso a las páginas con las que no se podía interactuar, era simplemente como una presentación en la computadora, donde las empresas, la industria, las universidades daban cierta información sobre su empresa y uno

podía consultarla y de ahí usarla, pero no podíamos interactuar con esa información, no era bidireccional.

Y es ahí en los años 70's cuando inicia la protección de datos, porque para poder, además de que yo obtenía información también teníamos que dar muchísima información; aunque todavía no había información, vaciábamos información o dábamos información físicamente a muchísimas autoridades, y las autoridades la capturaban en ficheros y tenían un acceso a una cantidad enorme de datos. Había una proliferación de expedientes y de datos, y de ahí surge que se tengan que proteger los datos de las personas, porque se estaban haciendo ficheros en cantidades muy importantes y de fácil acceso. Esa es la red 1.0, ahí es donde nace en los años 70's las normas de protección de datos.

¿Y por qué es importante? Porque en esa época, cuando nace la legislación de protección de datos no existían redes sociales. Facebook es de 2005, y su auge, auge, es en 2007. Y las leyes de protección de datos son de 1970.

México empieza esa lucha por tener una ley que se adecue para que sus empresas puedan invertir en otros países y de otros países acá, que venga la inversión extranjera para tener un lugar seguro de inversión, pero todo esto de la protección de datos se empieza a dar en los 80's, en los 90's, y nosotros no teníamos una ley.

Empiezan las normativas, el convenio 108 de Europa, que es de 1981, la de la OCDE, de 1981; luego la de la ONU, de 90, y luego, el primer reglamento, el anterior a este, de 1995. Ahí no estamos hablando para nada del internet de las cosas ni de la computación en la nube ni nada, y México empieza en 2000, en el año 2000, a querer tener una ley para adecuarse al modelo internacional de protección.

Y se tarda 10 años, desde el año 2000, por eso te decía que tú nos vas a poder decir porque tú estabas en el INAI, Marina, en el 2008, o sea, todavía no entraba en vigor la ley, nos tardamos 10 años en crear una ley que fuera en ese momento disque muy moderna.

Entonces fue desde el 2000 hasta el 2009, que entró en la Constitución ese derecho, y claro, fue una discusión importante,

porque teníamos que primero adaptar todo lo de transparencia también.

Entonces, se agregaron todas las leyes de transparencia, se trabajó muchísimo pero la protección de datos ya para cuando llegó nuestra ley en 2010, la verdad en muchas partes ya era anacrónica porque no preveía, por ejemplo, el derecho al olvido, no preveía las redes sociales, y creo que incluso es ahorita donde me atrevo a ser todavía más aventada en decir que incluso el reglamento, como el nuevo reglamento europeo también ha sido discutido, todavía el faltaron algunas cosas que en mi opinión habría que adecuar a la realidad de las redes sociales de la interactiva y de la inteligencia artificial.

Lo de las fechas es muy importante para que veamos cómo es que queremos aplicar hoy una Ley de Protección de Datos cuando ya tenemos una tecnología absolutamente diferente. Y un gran ejemplo que les queremos decir es, si ustedes se fijan el INAI y el InfoDF ponen publicidad diciendo “cuídate en las redes sociales”, “cuida tu información”, “no respondas a gente desconocida”, cuando en realidad la Ley de Protección de Datos no protege a los particulares en sus actividades domésticas.

Si ustedes quieren hacer el ejercicio y tienen por ahí su ley o pueden agarrar su celular y ver su ley, en el artículo 1º de la Ley de Protección de Datos en posesión de los particulares dice claramente. Perdón, en el artículo 2º: “Son sujetos regulados por esta ley los particulares, sean personas físicas o morales, de carácter privado, que lleven a cabo el tratamiento de datos personales con excepción de -y dice la fracción tercera- las personas que lleven a cabo la recolección y almacenamiento de datos personales que sea para su uso exclusivamente personal”. Y el reglamento europeo dice “o doméstico”, le agrega esa palabra, “sin fines de divulgación o de utilización comercial”.

Y claro, porque en los años 70, 80’s y 90’s, incluso en los 2000, estas leyes estaban destinadas a las empresas e instituciones que recababan información de los ciudadanos para divulgarla o para usarla para fines comerciales, pero no estaba pensada para quienes en redes sociales, para usos particulares de mi casa, domésticos, recabamos información.

Pero con la tecnología que existe actualmente, nosotros, cada uno en nuestra casa tenemos no la misma pero una posibilidad casi similar de difundir información sobre una persona de manera rápida, masiva y sin retorno. O sea, con la tecnología que gracias a Dios, porque la verdad es que sí nos ha beneficiado muchísimo, tenemos la posibilidad de hacer negocios como si lo hiciera quien tiene una inversión muy importante en medios, pero yo tengo mi Facebook, tengo mi Instagram y mi Twitter y con eso ya puedo hacer mucho más y ya puedo difundir información de una persona en forma masiva, aunque la persona no esté de acuerdo.

Y esto no lo protege esta ley, porque yo, en mi actividad doméstica, ahorita dije de los negocios pero olvídense de los negocios, si yo fuera una persona física que no hago negocios pero quiero difundir algo sobre otra, lo puedo hacer de forma masiva sin necesidad de estar regulada por la Ley de Protección de Datos, y resulta que no hay una regulación sobre la privacidad porque en la época en que todo esto se empezó a regular se decía: en virtud de la revolución informática se deja a los órganos garantes y a las leyes de protección de datos la esfera de la privacidad informacional, y se deja al ámbito jurisdiccional o de los jueces la esfera privada de las personas en el ámbito no informacional.

Sí, porque en realidad no había necesidad de abarcar la parte informacional para cuestiones meramente domésticas.

Pero ahorita con la tecnología que existe hoy, claro que es importantísimo proteger la esfera privada informacional en la parte doméstica. Podríamos forzar la ley y decir, bueno, aquí dice “y sin fines de divulgación”, cualquiera que difunda información hay un fin de divulgación. Pero ese no es el objetivo de la ley porque imagínense que yo le voy a decir a Cynthia: “Oye, Cynthia, antes de que digas algo de mí que estuvimos en la mañana en un desayuno, y pongas cualquier información que no vaya a estar de acuerdo, dame el aviso de privacidad y si estoy de acuerdo en que tú vas a poner que vas a usar mi foto, entonces sí te firmo y te doy mi consentimiento”. Pues claro que no, porque ese no era el objetivo de la ley.

Entonces ¿qué nos está faltando en México? O utilizamos los principios de la Ley de Protección de Datos Personales para algunas otras cosas en la parte doméstica o ponemos otra ley totalmente distinta que se refiera a la privacidad en internet o en medios electrónicos, que no tengan nada que ver con datos personales.

Eso fue lo que pasó, si se fijan, en el caso del derecho al olvido, en el caso Costeja, que fue el caso que hizo más famoso este derecho al olvido, la verdad es que pidieron a Google que retirara del motor de búsqueda el nombre de la persona, argumentando que Google era responsable de protección de datos. Y Google dice “yo nunca le pedí los datos, él nunca me contrató, yo no tengo sus datos, yo solo soy un medio, como es un periódico y en realidad el responsable es quien subió los datos a la plataforma”. Y tenía absolutamente toda la razón.

Sin embargo la persona fue a la agencia porque no sabía a dónde ir, es como si ahorita dos personas en el ámbito doméstico tienen un problema de privacidad y vienen al INAI, el INAI les va a decir “qué pena, no te puedo ayudar porque yo aplico esta ley y esta ley no es para ti”.

Entonces lo que hizo la agencia, al ver que se trataba de Google y decir “bueno, quiero proteger la privacidad en medios electrónicos en esta era” tomó el caso. Y forzaron la ley, que no era aplicable, la verdad es que la agencia debió haber dicho “vete al juez y que el juez decida porque mi ley no aplica”. Pero era de tal relevancia el caso para el mundo y la protección de la privacidad en internet, que tomó el caso y adaptó la ley como pudo y eso hemos ido haciendo en el mundo y aquí también.

Entonces yo digo: ¿vamos a seguir torciendo nuestras leyes para tener que aplicarlas? Pues nos van a salir las empresas a decir “oye, no, es que yo cómo voy a ser, al contrario estoy ayudando a los usuarios, yo les estoy dando una herramienta para que hagan mejores negocios y todo, ¿y me vas a mí a exigir daños y perjuicios porque se pelearon entre ellos dos? No tiene sentido”. Yo creo que no tenemos seguir forzando la ley, y ya sea quela dividamos para que parte de la ley sea aplicable a particulares o en el ámbito doméstico, sobre todo la parte de los principios y de la lealtad y de la responsabilidad. O

hacemos algunas adecuaciones en la normatividad, en materia de derechos de la personalidad para garantizar eso.

Entonces, en realidad lo que siempre me gusta decir es que efectivamente donde está la solución, tanto en el ámbito comercial como en el ámbito privado, es en la confianza, y creo que debemos de dejar de ponerle la carga de la defensa de la información al usuario.

Un usuario común y corriente para leer las políticas de privacidad de los servicios que utiliza en un año se tardaría 244 horas. ¿Imagínense si cada año yo tuviera que invertir 244 horas para protegerme? Pero eso sí, las empresas, salvo Microsoft, van a decir: “Yo te di el aviso de privacidad y tú consentiste y ahí me pusiste un *check* y me dijiste que sí podía usar tu información”.

Uno de los beneficios, por ejemplo, del reglamento o las novedades, es que ya no hay consentimiento tácito, como lo hay en México, el consentimiento tiene que ser expreso.

Y bueno, ¿por qué iba a felicitar a Microsoft? Porque yo he llegado a estas conclusiones en virtud de estar haciendo un doctorado en el Instituto de Investigaciones Jurídicas de Protección de Datos, y entre todo mi tema, yo para argumentar y poderles decir “son 244 horas exactas las que tiene que leer”, yo quería saber qué pensamos los mexicanos y no tener la información de Estados Unidos, que la hay, o de otras partes del mundo.

Yo necesito saber si los mexicanos estamos leyendo los avisos de privacidad o si nos importa o si no, y fui y pedí recursos a las empresas, y a varias, no nada más a Microsoft, y la única que dijo: “Sí, yo te apoyo”, sin miedo, porque a las empresas obviamente les da miedo que las critiques, y lo que iba a salir en esa encuesta, que encuestamos a seis millones de mexicanos, tal vez no era del gusto de las empresas; pues fue Microsoft quien lo financió, y después de un año tuvimos cinco millones de usuarios que contestaron y pudimos tener muchísima información que pueden consultar en la red, se llama “La privacidad de internet”, por Espinoza y asociados, una servidora con apoyo de Microsoft.

Ahí viene qué piensan y qué han hecho sobre la privacidad los mexicanos, pero desde el municipio de Tlaxiaco, Oaxaca, hasta el que tú me digas y cómo lo usan. Y uno de lo que encontramos es que casi el 75 por ciento no lee los avisos de privacidad, del 25 por ciento que los lee la mayoría, más del 50 y tantos no los entiende. Entonces, la verdad es que algo, a pesar de que hemos hecho mucho y que hay estos foros y que qué bueno, o sea, no estoy menospreciando el trabajo que se ha hecho, porque es muy bueno, este trabajo requiere muchísimos más esfuerzos de todos nosotros.

Entonces, y creo que por donde debemos caminar, más que el consentimiento y los avisos de privacidad y todo, es en la confianza, en el principio de lealtad es la expectativa de confianza. Es decir, yo no tengo que esperar si tú me diste tu consentimiento o no; tengo que ponerme en tus zapatos y decir: si yo fuera tú, ¿usaría estos datos para lo que los voy a usar? Pero no desde mi perspectiva, sino de la perspectiva tuya. Porque tal vez me van a decir: “Si yo fuera Rebeca sí los compartiría porque soy muy tecnológica”. Pero Rebeca se tiene que poner en mis zapatos, pero si Rebeca fuera Carmen ¿los compartiría o no?

Y eso en una relación de tú a tú, que no tiene nada que ver con lo comercial, hasta en las empresas. Y ya si no se puede, entonces sí vamos a hacer una ponderación con juez que para eso están, pero bueno. Gracias, muchas gracias.

Marina Alicia San Martín Rebolloso: Muchas gracias, Carmen, rescato la parte de confianza, de nueva cuenta, y la parte efectivamente del principio de lealtad.

Más allá de que tenemos muchos retos normativos, también creo que es importante implementar lo que hay, efectivamente la tecnología nos gana en el ejercicio de derechos y en normas, pero en la mañana el propio doctor Oñate decía que aunque tengamos normas no nada más con la pura norma ya la arreglamos en una que regule A y B, y con eso mañana habrá otra tecnología y que eso funcionará.

Entonces, lo importante es: sí creo en la concientización, la sensibilización, de parte de los sujetos obligados también tocar o tomar estas experiencias que nos comparte la parte de privados en

trabajar los principios. Los principios son los mismos, siempre han sido los mismos y esos son los que vale la pena, ¿cómo genero yo como gobierno frente a la ciudadanía confianza? Y confianza también no solo es en la parte de acceso a la información sino en protección de datos y cómo hago que tú te sientas seguro -insisto- en que yo te los estoy cuidando, porque al final tenemos doble cachucha, somos servidores públicos pero siempre vamos a ser ciudadanos. Entonces cómo quiero que trataras tú mis datos si yo soy usuario de licencias de cosas médicas, y en ese tenor habría que ser el gobierno también ponerse la camiseta.

Carmen Quijano Decanini: Por eso el Convenio 108, desde el 81 hasta acá ha sido modificado muy poco, porque es muy pequeño y solo se concentra en principios y no al detalle.

Marina Alicia San Martín Rebolloso: Esa puede ser una alternativa y también no olvidar el tema de autorregulación, que existen esquemas de autorregulación que ayudan a estas nuevas prácticas y también, digamos, nos dan parámetros.

Pasando al mismo debate, por favor, querida Cynthia Solís, bienvenida. Te presento.

Ella es licenciada en Derecho por la Facultad de Derecho de la Universidad Nacional Autónoma de México, realizó estudios de la maestría en traducción, en el Colegio de México. Cuenta con una maestría en Derecho de la Innovación Técnica de las universidades de Panthéon-Sorbonne Paris I y París XI.

Doctorante en Derecho en el tema de Cibercriminalidad. Ha asistido a numerosos cursos y coloquios en materia de propiedad intelectual impartidos por el Instituto Mexicano de Propiedad Industrial y la Organización Mundial de la Propiedad Intelectual.

Ha dictado conferencias en materia de Tecnologías de la Información y Derecho Informático. Asesora jurídica de la Asociación Latinoamericana de Profesionales en Seguridad e Informática, y presidenta fundadora del Capítulo México de la Asociación Internacional de Derecho Informático.

Bienvenida. Te cedo la palabra. Gracias.

Cynthia Solís Arredondo: Gracias.

Primero que nada, quiero decirles a todos que me siento muy contenta de estar invitada aquí por una gran persona, amiga y heroína, que es la Comisionada Elsa Bibiana. Muchísimas gracias por la invitación, y por estar aquí compartiendo con grandes amigos que, tal cual, es muy interesante este debate porque como sea, cada uno de nosotros desde nuestra trinchera nos hemos estado peleando con estos temas. Y me gustaría rescatar algo que decía Marina en este momento: ¿cómo les hago sentir este tema de seguridad de los datos personales?

En el año de 2006, cuando estaba estudiando la maestría en Derecho a la Innovación Técnica, llegó uno de mis maestros y nos pregunta: "A ver, señores, ¿qué es la seguridad?". Y todos queriendo lucirnos sacábamos unas definiciones sofisticadas de qué es la seguridad. Y al final nos dice: "No, la seguridad es un estado del espíritu".

Y efectivamente, eso que comentas ¿cómo los hago sentir seguros? Tal cual así funciona.

La seguridad *per sé* o un entorno seguro no existe, es un ideal, es un sentimiento.

Una anécdota muy interesante. Hace como ocho años vinieron a visitarme unos amigos franceses y los dejé en Bellas Artes porque yo tenía unas juntas y les dije: "Miren, disfruten el Palacio de Bellas Artes, está increíble, nada más no se muevan".

Cuando regreso por ellos, tres o cuatro horas después me dicen: "Oye, está padrísimo México, fíjate que nos cruzamos la calle, llegamos a un lugar donde había unos vestidos impresionantes y un mercado donde vendían un montón de cosas y nos querían meter a unos pasillos". O sea, estos cuates se habían ido a La Lagunilla y a Tepito, y o sea, entonces yo me quedé, dije "híjole, para empezar qué bueno que no los asaltaron", si no, ya me imaginaba en "Esta noche en Hechos".

Pero ¿por qué no les pasó nada?, o ¿por qué ellos andaban felices por la calle? Porque se sentían seguros, porque no estaban conscientes de la inseguridad que a lo mejor nosotros tenemos más en mente.

¿Qué pasa en el momento de implementar las medidas de seguridad? Cuando ustedes a lo mejor compran una casa o un departamento o un coche, pues lo primero que hacen es: le compran el seguro. ¿Se acuerdan de que todos hace 10, 12 años traíamos bastones en los volantes? No servían para nada más que para agarrar así a bastonazos a un asaltante o lo que sea, pero nos hacían sentir seguros.

Lo mismo pasa. Cuando llegas y estrenas una casa o un departamento no vas a poder implementar correctamente medidas de seguridad en puertas ni ventanas, hasta que no entiendes cuáles son los puntos vulnerables.

Entonces, para implementar correctamente medidas de seguridad, ya sea en el tema de la protección de datos personales de los particulares o de los sujetos obligados, debemos de entender: uno, el tipo de información que estamos tratando y lo que eso conlleva.

Centrándonos en lo que es el ser humano, a mí algo que me gusta mucho del tema de protección de datos personales es que siento que además de ser un derecho humano, como decía Carmen, ya independiente, reconocido internacionalmente, está muy ligado con el tema de la dignidad.

¿A qué voy? Muchas veces esta divulgación irresponsable que se hace en redes sociales o incluso por medios de comunicación, de información de carácter personal, está de verdad estrechamente ligada.

Hemos tenido casos muy tristes donde, en virtud de la información o del derecho a la libertad de expresión, se vulneran la dignidad y la seguridad de las personas, un caso que tuvimos en su momento era, qué pasa cuando un hecho noticioso, o sea, hasta dónde yo puedo divulgar información de un hecho noticioso que incluso puede poner

en riesgo la vida, la seguridad y la dignidad de las personas que sobrevivieron a un asalto o a un homicidio.

Hubo un caso en el cual una persona, un padre de familia fue asesinado afuera de su casa, y el reportero, por qué no, dio el nombre completo de los dos, de la cónyuge superviviente y uno de los hijos, y dijo dónde estudiaba y a qué se dedicaba.

O sea, perdón, pero eso ya no es parte del hecho noticioso. ¿Qué sucedió? Bueno, acto siguiente ese chico fue acosado, sufre bullying, lo molestaban amenazas de quien había asesinado al padre y, bueno, fue un drama, de verdad un gran drama, la mamá se acabó suicidando; o sea, ese tipo de cosas que pueden pasar por no medir las consecuencias de una divulgación excesiva de información.

Entonces, regresando al tema de la seguridad, si yo no logro entender lo importante que es para un titular que su información esté segura o protegida, no puedo diseñar correctamente qué medidas de seguridad aplicar.

Aparte, recordemos que no solamente nos basamos en medidas de seguridad físicas o tecnológicas, sino también de procesos, cómo entra la información, cómo puedo saber o cómo puedo asegurar correctamente durante todo el ciclo de vida de la información que es desde que la recabo hasta que se destruye, si no sé o no estoy consciente por qué canales está entrando o ingresando esa información; y lo mismo, por qué canales va a salir.

Entonces, una vez que yo entiendo qué tipo de información trato, la clasifico correctamente para saber si es sensible o no es sensible, cuáles son los medios de acceso de esa información a mis sistemas, a lo mejor ya puede estar en virtud de poder empezar a diseñar procesos, procedimientos, contratos y elegir la tecnología, por ejemplo, como bien lo decía Rebeca.

La verdad es que hoy en día ponernos puristas y decir: “Sí queremos que todo, la soberanía del dato y que tiene que vivir en un lugar centralizado”, eso es imposible y realmente es un freno a la economía.

Cuántas empresas que hoy en día son exitosas nunca lo hubieran podido hacer si estuvieran con un esquema de gastos de información y almacenación centralizada, hubiera sido imposible. Y también es un mito.

Hace, ¿qué será?, 10 años estábamos en una conferencia donde un ponente español, que respeto mucho decía: “Es que en España está prohibido el almacenamiento en la nube”. Y yo le decía: “¿No tienes Hotmail?” O sea, es la nube, ¿desde cuándo usas Hotmail?, por ejemplo; no me vas a decir que no utilizamos la nube, pues todo mundo utilizamos servicios en la nube, Android, nuestro iPhone, toda la información está en la nube, eso es algo que no puedes detener.

Ahora, lo que sí puedes hacer es elegir una nube o un servicio en general, diferentes servicios que cumplan con los estándares de seguridad de la información en general; y les decía, hay que entender el tema de seguridad es una cosa mucho más amplia, no nada más es, le voy a poner un antivirus; es más, hay muchas empresas en la implementación que hacemos que te dicen, cifrado, de entrada, vamos a cifrar la información. No, espérate, no en todos los casos es la solución.

Porque luego sucede que tienes cifrada la información y quien tenía la llave para descifrar se fue, y entonces ahora ya no puedes cumplir con el derecho de acceso que te está pidiendo un solicitante o ya la información ya no está disponible. Entonces, ya estás violando la seguridad.

Y justo eso es algo que me gusta ejemplificar, como que el Sistema de Protección de Datos Personales es eso, es un sistema, es un engrane que obviamente el ser humano es la parte central donde todo debe de girar, pero están los principios y las medidas de seguridad, todo tiene que girar alrededor de, pero está en conjunto, están interrelacionados, no podemos diseñar una medida de seguridad si no entendemos qué principios podríamos violar, y que es un poco lo que el GDPR te obliga a hacer cuando están estos famosos PIAS, y el análisis de impacto, la privacidad.

Si yo quiero implementar una nueva tecnología primero tengo que analizar justamente cómo va a impactar la privacidad de los usuarios,

y si no estoy en virtud de un tema de seguridad violando la privacidad o viceversa, si no quiero cuidar la privacidad, pero estoy dejando de lado la seguridad o la accesibilidad, que son los pilares básicos de la seguridad de la información.

Entonces, yo creo que algo muy interesante es eso. Ahora que está tan de moda todo este tema de las brechas de seguridad de datos personales hay que implementar correctamente una medida de seguridad, que obviamente tiene que ser un traje a la medida.

Yo les podría decir, tienen que comprar la solución más sofisticada y la más cara. No, no es cierto, se los juro. Yo conozco a empresas que tienen implementadas o que compraron las licencias de las herramientas más caras que se puedan imaginar y un DLP y no sé qué, pero no lo saben configurar.

Entonces, si no lo saben configurar pues ahí está el problema, ahí está la brecha en el usuario. Entonces, no se trata de gastar, no se trata de hacer cosas tan sofisticadas, solamente hay que saber diseñar lo que nos corresponde, lo que nos queda mejor, el traje a la medida para que justamente el usuario además de que esté seguro se sienta seguro, que eso es algo muy importante, y que por qué no, hoy en día tanto para gobiernos, como para particulares esa es una decisión fundamental para que un usuario decida decantarse por una cosa o por la otra. Eso es fundamental.

Y creo que no tenga nada que agregar, pero muchas gracias por la invitación.

Marina Alicia San Martín Rebolloso: Muchas gracias, Cynthia.

Retomando, pues sí, volvemos a lo mismo, el tema de construir la confianza que tarda mucho en hacerse y en un minuto se puede perder. Entonces, esa parte como ciudadanía y gobierno es correcta.

Efectivamente el tipo de información eso lo comentamos en la mañana, el tipo de información, no es lo mismo la base de datos que tienes de seguridad de la gente que administra salud, y lo más importante es que los que están aquí de las unidades de transparencia son los que conocen qué tipo de datos son, no tienen que saber cómo

hacerle, para eso está la autoridad como estamos nosotros y el Info los va a ayudar y obviamente con el apoyo de expertos y tenemos que consultar igual para ir determinando qué es mejor para cada uno de sus datos, pero siempre sin perder de vista lo que comentaban ustedes, el ciudadano, una persona que es el usuario y generando esa confianza, efectivamente el tema de la dignidad también lo retomo, el derecho de datos personales nos ayuda justamente a potenciar otros derechos, pero protegerlos; es decir, si yo no me veo discriminado entonces puedo ejercer mejor otros derechos y esa parte también hay que tenerla en cuenta.

Y muchas gracias, Cynthia, por tu intervención.

Paso con el afortunado de la mesa porque está rodeado de mujeres y ahora quedó en menos en género, que es Mauricio.

Mauricio, muchas gracias, te presento.

Es licenciado en Derecho por la Universidad Marista, Campus de la Ciudad de México, realizó especialidad en comercio exterior y arbitraje en la División General de Postgrado de la UNAM, además de otros estudios de postgrado en el TEC y la Universidad de Cambridge sobre materias relacionadas con derecho corporativo, INCOTEMS y Tratados de Libre Comercio.

Se ha especializado en práctica del derecho corporativo y regulatorio, específicamente en protección de datos personales, transparencia, Tecnologías de la Información, prácticas antilavado, ética corporativa y propiedad industrial.

En Bufete Sony tiene a su cargo las áreas de protección de datos, regulatorio y *Compliance*, además de participar como asesor corporativo en proyectos especiales para empresa.

Ha diseñado en partido capacitaciones de transparencia y protección de datos para los sujetos obligados, es barrista y además de ANABE y de la Asociación Internacional de Profesionales de Privacidad, y ha participado en el Foro de Gobernanza en Internet de la ONU, así como en Asociaciones en Propiedad Industrial a nivel internacional.

Bienvenido, Mauricio. Muchas gracias.

Mauricio Hernández Aguilar: Gracias, buenas tardes a todos.

Gracias a las abogadas que me permitieron aquí compartir el panel.

Voy a hacer este cierre de sesión, no lo veo como un acto de discriminación, sino creo que como el derecho de réplica más bien que nos toca la parte masculina, y eso va a ser todavía más interesante.

Platicábamos hace rato de qué parte exponer, considerando que la mayor sección del cuerpo de protección de datos se ha discutido el día de hoy; y un tema que nos ha pedido la comisionada y el resto de los comisionados es hablar sobre los temas de medidas de seguridad.

Aprovecho, antes que se me pase el tiempo, para darle la bienvenida como ciudadano a los nuevos integrantes de este Instituto, a la Comisionada Bibiana, por la invitación que hizo a los miembros de la Barra, muchas gracias; a la Comisionada Moderadora de esta tarde, gracias por darnos la idea de tocar este tema porque es muy importante; y a mis compañeras que vamos a ver qué tal la hago frente a ellas.

Aquí quiero destacar un punto que he escuchado sobre la mesa y para el cual me gustaría nada más preguntarles cuántos de ustedes están en la figura de sujetos obligados. Levanten la mano sin miedo. O sea, que lo que hemos dicho no les sirve para mucho como hablamos como particulares. Se vale.

Entonces, lo importante es ver, sí está muy bonito lo que decimos en la Academia, y en la Iniciativa Privada, y en los Softwares; no, pero qué estamos haciendo por el gobierno. Y creo que aquí tenemos que rescatar cosas muy importantes.

Quienes hemos tenido la oportunidad de ver, y estoy seguro que Microsoft también lo ha hecho. Las leyes para gobierno se habrán dado cuenta que los requerimientos que tenemos en medidas de seguridad para una Secretaría de Estado como el SAT, no ha de ser la misma que la que pide mi despacho como sector privado, no puede serlo; y forzosamente el Software tendrá que estar adaptado en

medidas de seguridad, a dónde está la nube, quién tiene acceso, yo no recuerdo al Secretario de Hacienda o al Director del SAT diciéndonos dónde está nuestra nube. Y esa también puede ser o es una medida de seguridad, porque imagínense que alguien se entera de dónde le bajan el switch a la Secretaría de Hacienda para no tener nuestras declaraciones de impuestos.

¿Es una medida de seguridad? Sí, nos bajan el SIPOT en sector gobierno, entonces la confianza estoy de acuerdo con Cynthia y con Carmen, tiene que ver en un punto esencial de lo que espera el consumidor, el usuario de nuestras plataformas, el dueño de los datos, pero también basado en lo que yo estoy necesitando.

A ver, comentaba por aquí, tengo que pensar en función de cómo quisiera yo que trataran mis datos si fuera el usuario. Sí es lo ideal, pero en realidad no sucede. Y tenemos un ejemplo hace unos meses en Estados Unidos, ¿qué nos declaró el SO de Facebook cuando le dijeron en el Senado?: ¿“Nos puede decir con quién compartió la cena anoche? ¿Por qué fue a este hotel?” ¿Qué contestó? No, claro que no, a lo mejor no lo haría, pero bien que lo hizo con 87 millones de cuentas, dirían los demás.

Entonces, es un ejemplo de que no siempre pensamos como empresarios en ese sector.

Ahora vámonos en el sector público. Hay un artículo que lo pongo como ejemplo de los casos que ustedes están viviendo, en donde a veces las medidas de seguridad no nos cuadran a cada dependencia igual.

Secretaría de Salud, tenemos un expediente clínico y no lo hablo a nivel nacional, vamos a verlo a nivel local, y en ese caso nos piden que cuando la persona es mayor de edad le vamos subiendo la temperatura al asunto porque no sean datos regulares, sino sensibles simplemente porque es un expediente clínico, puede solicitar el ejercicio del derecho ARCO alguien que lo represente legalmente.

Cuántas personas conocen ustedes que tenga acceso a un notario público que otorgue un poder para ejercer un derecho ARCO. Suena

muy bonita la medida de seguridad, pero en la práctica a ustedes como unidades de transparencia les estamos atando la mano.

Entonces, es muy cierto, no estamos brindándoles a ustedes confianza, porque si a los titulares de los datos como autoridades se las ponemos tan complicada para que nos digan no quiero que uses los datos, pues simplemente por una cuestión de cansancio el usuario ya ni le hace caso. Dice: Tengo de dos sopas, o les entrego todo o no me dan el servicio.

Creo que ahí es donde mucho tenemos que mejorar o podemos mejorar desde el sector público los errores quizá que se hayan cometido en la Ley de Privados o las oportunidades, lo preciso, no es un error, sino simplemente que iniciamos una regulación muy ambiciosa que creo que si ahora lo comparamos con las leyes internacionales vemos que no es nada mala a la Mexicana, es bastante competente, pero que hay áreas de oportunidad que tenemos que ir mejorando.

Ahora, por otro lado, hablábamos de la parte de autorregulación. Creo que va vinculado a la confianza, porque si nosotros como funcionarios hacemos creíble que la dependencia protege la información del gobernado, hasta ustedes mismos, nosotros mismos como ciudadanos nos vamos a sentir mejor.

Quizás si alguien está aquí del SAT o de la Unidad de Inteligencia Financiera se habrá acordado que cuando surgió la Ley Antilavado, la famosa ley que tiene un nombre interminable, pero que la conocemos como Ley Federal de Lavado de Dinero, nos indicaba que la información nos prometían por nuestra mamá que de la Unidad de Financiera no salía, aunque en el escritorio de junto estuviera sentado el Secretario de Hacienda.

O sea, si yo lavo dinero te prometo que no te cae una auditoría fiscal. Pues es que una conlleva a la otra por simple naturaleza, entonces para qué me dices lo que no vas a hacer cuando sabes que por ley lo tendrías que hacer.

Es más, quién de ustedes piensa que la Secretaría de Hacienda no va a revisar lo que haga la inteligencia financiera. Yo creo que no.

Entonces, por qué no decimos las cosas como son, vamos a hacer las cosas así, tu información la podemos utilizar hasta este momento, y no nada más dejárselos.

Y aquí quiero hacer una acotación sobre las medidas de seguridad como yo las veo, Comisionada, no nada más hacia el exterior. Todo es lo que dice la ley y lo que dice la ley, y lo que dice la ley, pero la ley a veces no alcanza para la realidad y la ley tiene que ser un resultado de lo que la práctica nos está enseñando. Por eso creo tan importante que ustedes como Órganos Internos de Control, como Unidades de Transparencia se pronuncien y nos digan: ¿Saben qué, litigantes? Esto está mal. ¿Sabes qué, autoridad? Nos hace falta esta herramienta. Te informo, autoridad, que con lo que tengo no me está alcanzando.

Algo que hemos dejado de lado, y aquí lo reviso y lo uno con la parte de confianza, es la parte también de autorregulación.

Una medida de seguridad para mí tiene una óptica dual, se ve desde dos puntos: al interior del titular o dentro de la esfera del titular y desde la autoridad. ¿Por qué? Porque si el titular no está acostumbrado a proteger su información y eso tiene que ver con un principio de educación, y no es que ahora me ponga yo como cierta persona que ahora cree que todos somos buenos porque somos hijos de Dios, pero si no tiene que ver esto con un tema de educación, entonces estamos perdidos. Y esta es una materia que debería de estar ya a nivel de civismo.

¿Qué hacemos con la información? Cómo se vuelve esto transparente y cómo vinculamos esa responsabilidad de la protección que los de los datos para que no se malinterprete como la parte opuesta de la transparencia. Porque ustedes tienen que adoptar dos leyes, ahora tres, también la de archivos.

Ayer el Ministro Cossío comentaba algo muy interesante en el Instituto Nacional de Transparencia al momento que daba su ponencia, y lo cito más o menos, es lo que mencionaba: aquí al Poder Judicial le hace falta determina hasta dónde sí y hasta dónde no en la protección de los datos. Porque necesariamente necesitamos otros momentos en los que hay que publicarla.

Me voy a las versiones públicas del Poder Judicial. Desde fuera no se entienden, parecen formatos, en tal Ciudad de México, rayita, en el caso número tantos, de tanto contra tal por el delito de tal se determina lo siguiente. Pues parece receta de cocina, y yo necesito saber por qué se llega a una determinación en función de las agravantes, de las atenuantes, que fue el caso concreto; a lo mejor no necesito el nombre y el apellido, pero sí parte de los datos estadísticos. Creo que ahí estamos en una ley de péndulo donde tendremos que verlo.

¿Y cuál es la gran oportunidad que se tiene? El Sistema de Autorregulación.

Por suerte las leyes en México nos dicen no tiene que ser A o tiene que ser B; nos dicen: Hazlo como tú puedas, hazlo con las herramientas que tengas, como señala Cynthia, pero que se genere esa confianza, y como bien mencionaba Rebeca, que tengamos herramientas lo suficientemente robustas pensando en lo que ya se demostró que necesita el consumidor, estas herramientas, y tampoco me están pagando por el comercial, pero tampoco es la única, nos da esa gran ventaja.

Y aquí tenemos que irnos, y con esto cierro, a la parte final.

Si ustedes acudieran a un supermercado, lo pongo sobre todo para las personas que acuden a hacer las compras, que ahora también hay aquí donde ven eso; para quién tendrían más confianza de dejarle unos datos para un sistema de lealtad, el que sí les dice claramente qué van a hacer o el que no. El que sí y el que se los comprueben, porque todos podemos decir muchas cosas, pero es muy difícil poderlo comprobar y eso se llama nivel de cumplimiento.

Nosotros podemos poner lo que sea en los avisos de privacidad, pero vamos a demostrar, vamos a tener esa responsabilidad proactiva de llevarlo a cabo, y eso implica hacer transparentes también.

Y curiosamente la palabra transparencia no es un concepto que esté en nuestra Ley de Datos por alguna extraña razón, pero si nos vamos un poquito a la parte académica vemos que internacionalmente Japón

la tiene, Asia la tiene y nosotros tenemos un Instituto de Transparencia que no habla de transparencia en la Ley de Datos, no culpo al Instituto, si esta es una cuestión que tendrá que verse en el Legislativo, pero lo importante más que lo diga es que lo estén haciendo como se hace ahora: Academia, capacitaciones a los Órganos Internos de Control, que se tengan portales en donde se puede informar qué se tiene, cada cuándo se tiene, en qué se gasta, en qué momento se entrega una información y por qué podríamos exceptuarla; y lo que creo que también sería muy importante verla.

Y regreso al punto, la capacitación que tendremos en que esas medidas de seguridad se adapten a los criterios, que las escuelas lo sepan tener, pero que también una delegación las tenga, y que también la oficina que se encargue aquí de los permisos para los inmuebles comerciales en la Ciudad de México tenga esa transparencia, cuánto nos está costando, a quién se le está entregando la información, cómo lo va a utilizar, porque en la manera en que nosotros conjuntemos la protección de los datos en medidas lo hagamos con nuestra conveniencia como instituciones o con los requerimientos como autoridad y se lo demos a conocer a un usuario o al gobernado, va a sentir más confianza en el gobierno.

Creo que la falta de comunicación desde las autoridades hacia el gobernado es lo que ha causado mucho de esa disrupción de conocimientos en confianza.

Porque ustedes no me dejarán mentir, ustedes trabajan mucho, ustedes trabajan mucho desde dentro y esa también es una medida de seguridad que malamente no se está difundiendo. Tenemos que quitarnos el estigma como gobierno de que no hay medidas; claro que hay medidas y se tiene que implementar de cierta forma, diferentes a particulares, pero sí lo pueden hacer.

Y los felicito mucho porque estén en esto. Y no dejen de considerar, con esto cierro, la Ley de Archivos, porque algo que nos va a dar una adecuada gestión de los datos es cómo archivamos, si no hay archivos pues qué guardamos. Es así de simple.

Y es cierto, tenemos un correo de Hotmail, pero no necesariamente ese tiene que ser nuestro archivo, menos en el sector público.

Muchas gracias.

Marina Alicia San Martín Rebolloso: Muchas gracias, Mauricio.

Efectivamente retomo lo último que dijiste de la Ley de Archivos, tenemos esa triada de obligación como sujetos obligados; Archivos nos garantiza tanto el tema de protección de datos, como el tema de acceso a la información.

Sí es muy importante en el tema de confianza, que ha sido el eje un poco de esta mesa ligado a medidas de seguridad; la parte de comunicar nosotros como servidores públicos necesitamos comunicar a los ciudadanos lo que estamos haciendo, creo que es mejor siempre tener claridad, el aviso de privacidad efectivamente parece que está escrito en chino, y la lógica es hacer accesible para que te recabe, por qué te recabe, hasta dónde, a dónde me puedes decir tú que sí y qué no, si son datos sensibles o no, es digamos una guía que te da a ti una pauta para blindarte en qué estás haciendo el cumplimiento de tus atribuciones y así cada uno de los puntos.

Efectivamente en el tema de medidas de seguridad, tanto para el titular, que tenemos que aprender cómo los titulares de datos a qué damos y qué no y hasta dónde, tener esa conciencia de nuestros propios datos y como sujetos obligados al interior cómo estamos brindando esta información y en trajes a la medida, más allá de las buenas prácticas que aquí en esta mesa nos han compartido.

La experiencia del sector privado que siempre sirve como lección o referente a nosotros como sujetos obligados, eso creo que ayuda mucho, y agradecerles mucho su presencia.

No sé si hubo alguna pregunta de la audiencia; si no, les daríamos por cerrado o despedido el panel, entregando los reconocimientos para estar en tiempo comisionada de la clausura.

Y me permito si tienen a bien darles un reconocimiento a nombre de los comisionados del Instituto.

Muchas gracias.

Rebeca, aquí está este presente por parte del Info.

Muchas gracias, Carmen, también este presente.

Cynthia, muchísimas gracias.

Y Mauricio, muchísimas gracias también por tu intervención.

Les pido un aplauso final a los panelistas por tan buenas exposiciones y muchas gracias a ustedes para pasar.

Presentador: Invitamos a los panelistas tomarse la foto del evento.

Despidámoslos con un fuerte aplauso.