Ciudad de México, 26 de enero de 2018.

Versión estenográfica del Panel 3 "La Protección de Datos Personales en el Contexto Internacional, Perspectiva de los Expertos y las Implicaciones del Principio de Responsabilidad Demostrada en el Tratamiento de Datos Personales, en el marco del Seminario Internacional de Protección de Datos Personales 2018, del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, celebrado en el Centro Cultural San Ángel.

Presentador: Para continuar con las actividades de este Seminario Internacional de Protección de Datos Personales 2018, dará inicio al panel: "La Protección de Datos Personales en el Contexto Internacional. Perspectiva de los Expertos y las Implicaciones del Principio de Responsabilidad Demostrada en el Tratamiento de Datos Personales.

Para lo cual cedemos el uso de la palabra a la Elsa Bibiana Peralta Hernández, quien modera este panel.

Elsa Bibiana Peralta Hernández: Buenos días.

Les agradecemos nuevamente que estén acá con nosotros para llevar a cabo el segundo día de los trabajos.

Muy buena fluencia, eso quiere decir que ha sido de su interés y que ha despertado el gusto por seguir escuchando a nuestros excelentes invitados internacionales.

Yo la verdad, no me restea más que agradecerles a los que nos acompañan ahora aquí, a ustedes que también les digo, se dan ese tiempo dentro de tantas actividades, en este lugar tan cálido, que me da mucho gusto que aquí haga calorcito, porque sí está un poco fuerte el fío y uno como ya está viejito, pues ya afecta. No dije la edad, nada más hice una referencia.

Pero muy bien, esto es para despertarnos y ponernos en sintonía en esto.

Voy a explicarles la dinámica de esta mesa que ya de alguna manera han visto cómo las hemos ido desarrollando. Creo que se ha hecho un tanto ameno y fácil también para ustedes y también para quienes nos están escuchando que, desde luego, ya saben que pueden participar, a interactuar con nosotros haciendo llegar sus preguntas.

La dinámica es que contamos con 15 minutos cada quien.

La idea es que en 10 minutos cada uno de ustedes hable. Pero me decía, por ejemplo, Laura, que ella sí quiere utilizar el tiempo de corrido.

Si alguno de ustedes quiere hacerlo así, no se detenga. Yo voy a poner una alarmita, suena la alarma a los 10 minutos, pero si quieren seguir hablando, les doy los otros cinco minutos y ya cuando suene por segunda vez, pues ya saben que se agotaron los 15.

Si quieren cortar a los 10 minutos, está bien. De todas maneras en la siguiente ronda damos el tiempo restante y también de acuerdo con las inquietudes que nos hagan llegar ustedes de todas las exposiciones pues vamos desarrollando una plática para poder interactuar con el público. ¿Les parece?

Entonces, esa es la alarma fatal que ya conocen el sonido, para que sepan que ya se agotó el tiempo y no salga una mano gigante, mecánica, que así se lleva a la gente cuando no obedece.

Dentro de la tecnología, no saben, este teatro tiene eso. Es algo que sale atrás del espejo, porque hay una obra aquí que tiene que ver con eso.

Y ya me dijeron que aquí espantan. Sí, hay unos recintos también donde asustan bastante en el Centro. Pero bueno, eso es aquí.

Damos inicio, voy a leer rápidamente para no agotar los tiempos, voy a leer rápidamente una síntesis de las semblanzas de quienes nos acompañan y es de verdad una síntesis muy breve, pero la experiencia de ellos es muy vasta, a muchos de ellos ya los conocemos, son ya un referente, están inventariados en nuestros eventos del Instituto, porque la verdad, siempre es un gusto

escucharlos y algunos son invitados por primera ocasión, pero que también nos van a hacer un aporte y estoy segura que se van a inventariar en la lista de panelistas.

Muchas gracias.

Bienvenidos a todos.

Primero que nada, menciono a la doctora Laura Nahabetián.

Ella es Doctora en Derecho y Ciencias Sociales, egresada de la Facultad de Derecho de la Universidad Mayor de la República Oriental de Uruguay.

Es Magíster en Ciencias de la Legislación y Gobernanza Política, por la Universidad de Pisa.

Doctora en Ciencias Jurídicas, por la Universidad Católica de Argentina.

Profesora Adjunta, entre otras materias, de Derecho Informático, Derecho Constitucional y Ética Profesional en las Facultades de Derecho de Uruguay, respectivamente.

Integrante del Centro de Derecho Informático y del Departamento de Derecho Constitucional y Derechos Humanos de la Facultad de Derecho, igual de la Universidad Católica de Uruguay y de la Universidad Mayor de la misma república.

Asesor en el Parlamento Nacional de la República desde 2005.

Ha escrito varios libros, numerosos artículos, dictado numerosas conferencias y ha trabajado en múltiples proyectos colaborativos con los temas que nos ocupan a lo largo del mundo. Además, así lo manifestó ella en su síntesis curricular, está enamorada de México.

Gracias, Laura.

También es un honor recibir a Rafael Pérez Colón, Consultor Internacional en TICS Para el Desarrollo y Relaciones con Sector Público.

Es Director Mundial de Microsoft Corporation para Organismos Internacionales.

Rafael es Consultor Internacional en TICS para el desarrollo de Relaciones con Sector Público.

Colabora como Asesor Senior en organismos internacionales como el Banco Interamericano de Desarrollo y el Banco de Desarrollo en Asia.

También es Secretario y Miembro de la Junta Asesora de la Red Española de Servicios Sostenible adscrita a la Red Global de Desarrollo Sostenible de las Naciones Unidas.

Cuenta con más de 30 años de experiencia en el campo de las tecnologías, de la información y es reconocido mundialmente como experto en TICS y su impacto en desarrollo económico.

A lo largo de su carrera ha ocupado diversas posiciones como Director de Centros de Computación y Asesor para universidades y gobiernos, Profesor Universitario, Investigador en la Comunidad Europea, Presentador en Radio y TV y Colaborador de Prensa, Emprendedor Tecnológico y Ejecutivo y Corporativo Internacional.

Durante 18 años se desempeñó en diversos puestos en Microsoft Corporation, como Gerente para Sector Educación en Puerto Rico y el Caribe, Director Regional para el Sector Gobierno y Sector Educción en América Latina y el Caribe, también Director Senior para Organismos Internacionales en América Latina y el Caribe y lo mismo para organismos internacionales.

También es coautor de diversos libros y artículos publicados internacionalmente.

Miembro de Juntas, equipos y grupos de asesores en diversos programas universitarios y de gobierno.

Él no puso que estaba enamorado de México, pero estoy segura que sí.

Continúo con el de Nelson Remolina Angarita.

Es Profesor Investigador de la Facultad de Derecho de la Universidad de los Andes.

Doctor Summa Cum Laude en Ciencias Jurídicas de la Pontificia Universidad Javeriana.

Máster del London School de Economía y Ciencias Políticas.

Especialista en Derecho Comercial y Abogado por la Universidad de los Andes.

Es Director de la Especialización en Derecho Comercial de la Universidad de los Andes.

Experto invitado en la Red Iberoamericana de Protección de Datos Personales.

Cofundador de la Red Académica Internacional de Protección de Datos Personales.

Es ganador del Premio Internacional “Protección de Datos Personales de Investigación 2014”, conferido por la Agencia Española de Protección de Datos Sobre Trabajos Originales e Inéditos, que tratan a cerca del Derecho a la Protección de Datos en Países Iberoamericanos.

Sus investigaciones más recientes se centran en los siguientes temas: Protección de los Derechos Humanos en el Ciberespacio, La Economía Digital y el Internet de las Empresas, La Regulación Latinoamericana Frente a la Recolección Internacional de Datos Personales a través de Internet.

Los títulos: Valores Electrónicos, El Derecho al Olvido en el Ciberespacio, La Protección de Datos Personales en Latinoamérica,

La Neutralidad Tecnológica y las Alternativas de Identificación Electrónicas, entre otras.

También es coautor y autor de libros, artículos sobre Protección de Datos Personales, Desmaterialización de Títulos, Valores e Instrumentos Financieros y Comercio Electrónico, Conferencista también a nivel nacional e internacional sobre múltiples temas como los que nos ocupan y también particularmente en Comercio Electrónico.

Él también está enamorado de México.

Finalmente, Ana Brian Noguéres, que nos acompaña aquí también, una gran amiga. Gracias, Ana.

Ella es Doctora en Derecho y Ciencias Sociales por la Facultad de Derecho en la Universidad de la República Oriental de Uruguay.

Docente en la Cátedra de Informática Jurídica de la Facultad de Derecho y Universidad de la misma república y en la Cátedra de Derecho Telemático de la Facultad de Ingeniería de la Universidad de Montevideo.

Es cofundador del Centro de Derecho Informático y de su antecesor Instituto de Derecho Informático.

Facultad de Derecho, Universidad de la República, Asesor Letrado en el Parlamento de la República, en la Cámara de Senadores y en la Cámara de Representantes.

Ejerce la profesión de manera independiente y también como consultante.

Ha sido entre esas funciones Consultante en el Colegio de Abogados de Uruguay.

Sus áreas corrientes de investigación e interés son el Derecho Informático y la Protección de Datos Personales.

Ha participado en múltiples proyectos de Adecuación Informática, así como Proyectos de Iniciación de Sistemas Informáticos nuevos, de implementación de “Privacy by Desing”, coadyuvando a una adecuada interacción entre los técnicos de sistemas y los niveles gerenciales y de resolución estratégica.

En su campo de expertise acostumbra a dar charlas y conferencias tanto en su país, como en el exterior.

Ha participado en numerosos programas de educación y ha escrito más de 80 artículos y contribuciones en Uruguay.

Integra la Red Iberoamericana de Protección de Datos Personales desde su creación en el 2003 y en el Capítulo “Uruguay desde la FIADI desde 2006”.

Es miembro también de otras organizaciones como en Berlín, Embajadora de Privacidad por Diseño y Miembro de la Mesa Directiva de la Red Académica Internacional de Protección de Datos de Nuevo León.

También tiene una amplia exposición aquí sobre diferentes ponencias y conferencias dictadas a lo largo del mundo.

Autora de diversos trabajos científicos y diversas publicaciones periódicas en su país, entre otras, en el Anuario del Instituto de Derecho Informático y la colaborado también en diversas publicaciones en Uruguay, en Colombia, en Italia, en Japón, en Estados Unidos, en Perú, en España, en Panamá, etcétera.

Ella no puso tampoco que está enamorada de México, pero nosotros sí estamos enamorados de Uruguay y de México y de Colombia y de España y de Argentina. Y la verdad, es que conocer en la Red Iberoamericana a tantos y tantos colaboradores interesados en el tema de Protección de Datos, es para nosotros muy enriquecedor.

Quisiéramos llevar a cabo más eventos donde pudieran venir todos los expertos que hemos tenido ocasión de conocer en la Red, para que ustedes pudieran también conocer las voces de otras personas también involucradas en esto.

Pero bueno, a veces no alcanzan los tiempos, pero vamos a ir trayendo expertos tan geniales como los que ahora nos acompañan en esta mesa y como los que también nos acompañaron el día de ayer, que aquí hay algunos presentes que les agradecemos también su presencia.

Y no me queda más que pasarles el micrófono y reiterarles a ustedes mi agradecimiento por su presencia, por el interés que han demostrado en la realización de este evento que el Info lleva a cabo con muchos esfuerzos en apoyo de todo el personal del Instituto, a quien aprovecho ahorita en este momento para agradecer a todas las áreas involucradas por su trabajo, por haber hecho posible que todos los que están aquí pudieran disfrutar de este evento.

Les pido un aplauso, por favor, a todo el personal del Info.

Gracias.

Entonces, ahora cedo el uso de la voz a Laura Nahabetián, hasta por 15 minutos.

Gracias, Laura.

Laura Nahabetián: Muy buenos días para todos.

Lo del enamoramiento de México es verdad, pero además es un intento de que la alarma fatal se retrase un poquito. Capaz que con eso puedo comprar algún minuto más, no lo sé.

De todas maneras es un gusto.

Primero que nada, voy a agradecer a InfoDF por este placer que es estar nuevamente en México, un año más para conmemorar este Día Internacional de la Protección de Datos Personales, que en definitiva es una excusa fantástica para poder conversar sobre nosotros mismos.

En la medida en que nosotros somos nuestros datos, lo que estamos hablando es de cómo nos protegemos nosotros y de alguna manera

también hace a nuestra propia esencia un tanto y un cuanto también hace al ejercicio de nuestra libertad.

Por tanto, celebro que año a año InfoDF realice estas actividades que nos permitan juntarnos a compartir algunas ideas, algunas reflexiones sobre este tema tan importante.

Para ir comenzando, me gustaría afirmar que, como todos sabemos, diariamente se recogen cantidades de información personal que además va en aumento y que es procesada cada vez más en opacas y complejas formas.

A partir del despliegue progresivo de las empresas y las entidades públicas en los años 80, se considera que se ha iniciado un proceso en que se percibe que las prácticas en el procesamiento de datos, en general, implica la reducción de los derechos de las personas en tanto les confiere un papel de mero sujeto de datos, siendo sus derechos amenazados y sus libertades comprometidas.

La diferencia entre eso tiempos y los años 80 y los de hoy con la actual ola de información y de comunicación integradas a la tecnología, es ni más ni menos que su ubicuidad y poder de expansión.

De hecho, los informes decían que, dicen que ya desde el 2008 hay más dispositivos conectados que personas en el planeta.

Este incremento de las capacidades de los procesadores, el almacenamiento y el ancho de banda de transmisión progresivamente van verificando menos restricciones técnicas en el procesamiento de información personal. No es ninguna novedad.

Así es que hoy día están convergiendo con escasas restricciones internet de las cosas, las grandes bases de datos analíticas, la inteligencia artificial, los mecanismos de procesamientos del lenguaje, los sistemas biométricos, entre otras tecnologías a los efectos de la potenciación de las aplicaciones de manera de obtener mecanismos para el aprendizaje de máquinas que cuentan con inteligencia avanzada. Todo depende de lo que consideremos la inteligencia.

Se dice por ahí que en realidad la inteligencia es una capacidad de los humanos. Si la empezamos a transferir capacidades humanas a la tecnología, yo creo que estamos en problemas. Pero bueno, es una consideración.

“Big Data” conjuntamente con internet de las cosas y la computación en la nube pueden ser una fuente de valor sustantivo para el desarrollo de la innovación en la sociedad, sin lugar a dudas, en la medida que su pretensión o por lo menos la pretensión primaria es la mejora de la productividad, el desempeño óptimo de diferentes sectores sociales y la participación social.

Frente a todo esto, entonces lo que a mí me gustaría efectivamente reflexionar con ustedes, es si esto de los datos y la tecnología en perspectiva Datos Personales es un riesgo o una oportunidad para la Protección de Datos.

En la medida de las posibilidades de los diversos avances tecnológicos se amplían, se incrementan las preocupaciones vinculadas con los mecanismos de actuación de las diferentes partes involucradas.

Indudablemente, la Protección de Datos es una responsabilidad compartida. De eso no cabe duda.

La colaboración de la industria permite la aceleración del apoyo del ecosistema tecnológico a través del alineamiento de los estándares actuales de la industria informática con el ecosistema de seguridad más utilizado a nivel internacional.

A partir de esto es posible afirmar la necesidad de un equilibrio entre innovación, seguridad y privacidad, siendo en sustancia entonces, desde mi punto de vista, la consideración por lo menos de los siguientes elementos.

Primero y fundamental. Las personas deben ser consideradas en su dimensión de tales. Y, por tanto, sus datos como parte inherente a su personalidad y no como meros dueños de sus propios datos.

Ustedes me van a decir: “Laura, no descubriste la pólvora sin ruido”.

No, por supuesto que no. sin embargo, esta afirmación la hago a propósito para que sea el eje de nuestra conversación.

La persona en el centro, la dignidad de la persona en el centro.

Por tanto, sus datos, también en el centro de la discusión.

Los datos impulsan el desarrollo económico generando, por tanto, una multitud de beneficios sociales e individuales. Esto es cierto.

No todos los datos verifican la misma sensibilidad. Lo hemos visto estos días también.

Los consumidores deben confiar en cómo se usan, almacenan y transfieren sus datos. La tecnología es una parte fundamental de la solución, sin duda, pero no la única.

La tecnología es una herramienta, por lo que la interdisciplina se impone.

Es imprescindible el desarrollo de un marco de tratamiento de datos que permita una nueva clasificación de los diferentes tipos, indicando nuevas estrategias de gestión que se puedan verificar unidas para la liberación del potencial de las diferentes tecnologías.

Políticas orientadas a los datos especialmente protegidos, por ejemplo, los sanitarios, los financieros, las comunicaciones de carácter individual deben unirse a requerimientos de privacidad y seguridad más estrictos que los datos que han sido entregados en forma voluntaria.

En caso de registrarse adhesión a esto que yo acabo de decir y existiendo un manejo riguroso de los datos, será posible entonces que los responsables políticos puedan desarrollar disposiciones normativas que analizan las preocupaciones de seguridad y de privacidad plante y de esta manera asegurar que los beneficios sociales y económicos no estén acotados.

Es por esta razón que además se entiende necesario realizar algunas consideraciones de contexto.

Primero. Contralor de los datos.

Uno de los grandes desafíos que existen en términos de regulación y de manejo de información.

El control se desarrolla, desde mi punto de vista, de manera escasa y en términos generalmente asimétricos.

La información es recabada mediante dispositivos como consecuencia del rápido flujo de datos que se genera.

Generalmente el flujo de información obtenida de diferentes dispositivos conjuntamente con la necesidad de concreción de accesibilidad y amigabilidad en lo que hace a la utilización de los sistemas informáticos que los contienen, determina que pierdan su efectividad, incluso resulten poco adecuados.

Esto hace incluso posible el uso de métodos tradicionales para la protección del derecho a la privacidad.

Segunda cuestión. Consentimiento informado del usuario para el tratamiento y gestión de los datos personales.

Dependiendo del tipo de tecnología que simplemente es posible que ni el propio usuario tenga conciencia cabal del tipo de procesamiento que se efectúa con sus datos que se introducen en determinado dispositivo.

De hecho, Miguel nos decía hace un rato que los informes indican que para poder leer todos los avisos de privacidad y las políticas de privacidad se necesitan algo así como 73 días.

Ninguno de nosotros se va a golpear el pecho y va a decir: “Yo voy a usar 73 días de mi vida para analizar esto”.

Entonces, como decimos en el campo de mi país: “Hay que bajarle un poquito el copete al consentimiento”, en el sentido de, bueno,

busquemos mecanismos más novedosos para que la gente cuando consienta sepa lo que efectivamente está haciendo.

Luego otra cuestión. Posibilidad de utilización relevada para finalidades diferentes a las que fueron notificadas al usuario. Esto sucede.

El importante cúmulo de información que se puede recabar por medio de los dispositivos, sumado a la utilización de novedosas y modernas técnicas de análisis de datos y cruce de información habilita que este tipo de datos sea utilizado para propósitos secundarios, en muchos casos distintos al propósito inicial en acceder a información ya recabada de las personas.

Otro tema importante. El desarrollo de perfiles es poco razonable pensar que los datos se recaben en forma aislada y por separado.

Estos tienen vocación de asociación a un usuario, lo que indudablemente facilita con los mecanismos adecuados el análisis de hábitos, comportamientos, preferencias, posibilitando la habilitación de perfiles más detallados de los usuarios. Hay que tener cuidado.

Límites en la posibilidad de permanecer anónimos ante la utilización de determinados dispositivos o servicios.

Existe la chance, es cierta, de incrementar las posibilidades de identificación frente a la utilización de términos de fácil localización, ya que la dirección del dispositivo es una herramienta de importante utilidad para la creación de huellas digitales de localización de los usuarios.

Entonces, los niveles de seguridad y los niveles de privacidad dependen en definitiva de los imperativos determinados por los marcos jurídicos.

Sin duda, pero también dependen del ejercicio de las autoridades en el marco de sus competencias con órganos de control fuertes, que además se animen a avanzar en el control de las empresas y en la indicación hacia los gobiernos de las cosas que no deben hacer de la manera que se hacen con los datos de esos ciudadanos.

Otros elementos además que hay que tener en cuenta.

Está de moda esto del “Wearable Computing”, de los dispositivos que registran información sobre la actividad de las personas.

Si ustedes se fijan, hay mucha gente que está fascinada con tener un “Smart Watch”, es decir, in reloj inteligente.

Sí está buenísimo y es súper coqueto, pero el tema es que eso nos genera dificultades con la privacidad ciertamente importantes.

Tenemos puestos en nuestra muñeca una cosa, porque no deja de ser una cosa, que le transmite información a otro absolutamente de todos nosotros, sin que nosotros tengamos control y además hay que estar alineado a la locura que implica que el relojito te avisa que caminaste un kilómetro, que subiste 10 pisos, que tienes que irte a dormir porque estar es una locura.

Y esto de todas maneras, bien por el que ejerza su libertad de tenerlo, de todas maneras que ejerza también su libertad para entender que está entregando sus datos hacia una corporación que vaya uno a saber en definitiva qué es lo que va a hacer después con eso.

Y eso que yo no estoy en contra de la tecnología. Por el contrario, sólo me interesa plantear algunas cuestiones que a mí me parecen un tanto importantes.

Otra cuestión vinculada con esto, la Domótica. ¿Qué es la Domótica?

Es la posibilidad de colocar en las oficinas o en las viviendas elementos tales como electrodomésticos que pueden ser controlados de forma remota a través de internet.

Tal es así que las cosas que contienen sensores de movimiento pueden detectar y registrar cuando un usuario está en casa, cuáles son sus patrones de movimiento y preindicar un criterio de acciones.

La mayoría de los dispositivos domóticos están constantemente conectados y pueden transmitir datos al fabricante.

La Domótica plantea desafíos específicos en la Protección de Datos, ya que un análisis del uso de patrones en este contexto es probable que revele detalles del estilo de vida, los hábitos o las opciones de los habitantes o su presencia en la casa.

Ayer Isabel Lara, decía: “Bueno, hay determinadas cosas que a priori pareciera que no son cuestiones de datos personales. Entonces, la basura no importa”.

Y sí, vaya que importa. La basura importa y si nosotros tenemos nuestros electrodomésticos absolutamente conectados, van a tener también una forma de conocer cuáles son nuestros hábitos y en esa línea alguien va a saber qué es lo que consumimos y qué es lo que no.

Bueno, en todo este marco a nosotros también se nos decía: “El principio de responsabilidad demostrada”. Uno de los principios que ahora se está poniendo más fuertemente de manifiesto.

¿Qué viene queriendo decir esto?

Esto en definitiva, lo que tenemos que afirmar es que es imprescindible la rendición de cuentas y ésta implica el funcionamiento de una serie de políticas internas y sistemas de control que aseguren conformidad, por un lado, y la entrega de documentación acreditante de las diferentes situaciones, por otro; sin perjuicio que el requerimiento de burocracia nunca es una situación beneficiosa si es innecesaria.

¿Queremos documentar? Sí, pero lo que es necesario, no cuestiones innecesarias.

De hecho, parece interesante la minimización de requerimientos de documentación innecesaria para maximizar el espacio para iniciativas de las empresas apoyadas por la orientación de las autoridades de Protección de Datos.

El principio que establece que los Datos Personales deben ser tratados únicamente de forma compatible con el objetivo específico

para el que fuero recolectados, es esencial para respetar las expectativas legítimas de las personas.

De hecho, la creación de códigos de conducta, auditorias, certificaciones, conjuntamente con una nueva generación de cláusulas contractuales y reglas corporativas vinculantes pueden ayudar a construir un mercado sólido.

En esta línea argumental debe indicarse, en consecuencia, que los responsables de la entrega de información personal deberían ser mucho más dinámicos y proactivos alejándose de las llamadas “cajas negras”. Esto es tendencias de secreto y opacidad de las prácticas empresariales.

Al mismo tiempo, deberían exigir cada vez más transparencia también de alguna manera de parte de los clientes.

En este contexto entonces, es posible señalar que el principio de responsabilidad demostrada puede aportar concreción y coherencia a la efectividad del tratamiento de los Datos Personales.

Fue la OCDE por allá por los años 80 quien estableció este principio, según el cual una entidad que recogía Datos Personales debía ser responsable del cumplimiento efectivo de las medidas que implementen los principios de Privacidad y de Protección de Datos.

Ha corrido bastante agua bajo el puente, pero de todas maneras es muy importante que tengamos en cuenta que los responsables del tratamiento deben determinar la existencia de un programa integral de gestión de Datos Personales y, al mismo tiempo, estar preparados adecuadamente para demostrar a la autoridad, en caso que lo requiera, la implementación efectiva de sus medidas dentro de la organización y lo que determina el cumplimiento de la normativa vigente sobre Protección de Datos.

Esto genera como contrapartida, en forma inmediata, que el regulador deba antes de la determinación de una sanción verificar la existencia de medidas y políticas adecuadas que garanticen en forma idónea los tratamientos que se efectúen y el reconocimiento expreso que debe hacer en relación a las organizaciones que tengan posibilidad de

verificar una demostración de que la vulneración al sistema sólo obedecería a una situación excepcional y aislada y no generalizable dentro de un Programa Integral de Gestión de Datos Personales.

En este orden de ideas, las medidas que deben adoptarse tendrán en cuenta diversos factores que hacen a la idiosincrasia -eso es fundamental- de cada organización, entre los que se consideran, por supuesto, su tamaño, su naturaleza jurídica, la naturaleza de los datos que son tratados, el tipo de tratamiento al que se somete la información y los riesgos que implica para los titulares la obtención y posterior uso o tratamiento de sus datos.

Se exige consecuentemente que las organizaciones establezcan políticas internas efectivas, a efecto de garantizar distintos aspectos.

Un primer aspecto, es una estructura administrativa proporcional a la estructura de responsabilidad para la implementación de las medidas.

Un segundo aspecto, es la adopción de mecanismos internos para la puesta en práctica de políticas que incluyan herramientas de implementación, entrenamiento y programas de educación y formación en el conjunto de la organización.

Y un tercer aspecto, es la adopción de procesos de respuesta a posibles reclamos y consultas de parte de los titulares de los Datos.

La finalidad de incluir estos elementos en el funcionamiento de la organización no es otro que la generación de una situación beneficiosa para las partes y también para el regulador, el que sin olvidarse de sus competencias de investigación verificará otros factores adicionales para el desarrollo de evaluaciones en el seno de la organización, particularmente enfocados en la implementación de sus políticas y su cumplimiento efectivo.

Para que esto sea así, las políticas de “Accountability” deberán responder al menos a dos criterios.

Uno. Generación de datos cuantitativa y cualitativamente medibles, que permitan la acreditación de un grado de diligencia particular en

relación con las disposiciones normativas en materia de Protección de Datos.

Dos. La concreción de los ciclos internos de gestión de los datos en la organización en el marco de un Programa Integral de Gestión de Datos.

Y, para terminar, antes de que me saquen al roja definitivamente, dos o tres afirmaciones más.

Lo primero. Los Datos Personales, como todos sabemos, han desempeñado un papel central en la evolución de los mercados digitales, algunos de los cuales ahora pueden considerarse servicios esenciales.

El ágil desenvolvimiento de las tecnologías basadas en Datos Personales y en las operaciones de procesamiento de datos permitidas por estas tecnologías han colocado al Derecho a la Protección de Datos, así como a varios otros derechos, en un lugar de importancia sin precedentes, sobre todo en mérito a las factibles vulneraciones que pudieren sufrir.

De hecho, algunos derechos fundamentales clásicos establecidos en los instrumentos de derechos humanos, la privacidad, la libertad de expresión, el derecho a la no discriminación, fueron concebidos originalmente como protecciones contra la interferencia del estado.

Sin embargo, hoy está claro que en la era digital las salvaguardias son igualmente imprescindibles contra posibles interferencias por entidades no estatales e incluso por personas físicas, lo que conduce a una protección específica del derecho a la Protección de Datos.

La aparente fragmentación de la web de acuerdo con las fronteras estatales y la segregación de las experiencias en línea de la persona, en un número limitado de jardines amurallados, amenaza la privacidad de la información personal, la libertad de expresión, la libertad de innovar en medio de la concentración de ganancias, el poder de mercado y las interferencias del estado.

Las autoridades de Protección de Datos, en consecuencia, deben hacer cumplir la minimización de datos, lo que implica que la información sólo sea tratada cuando sea adecuada, pertinente y limitada en relación con los fines para los que son procesados y el derecho de las personas a recibir información relativa a la lógica de la toma de decisiones automatizada y la elaboración de perfiles.

En consecuencia, la información personal no puede concebirse como un mero activo. Ahí veíamos que el supervisor europeo habla de que no puede ser un activo económico, mucho menos un activo económico según lo han establecido los tribunales de justicia en distintas instancias y lugares del planeta.

Y esto no quiere decir que no tengan un valor económico. Lo que implica es que la persona no debe ser considerada cuantitativamente en términos numéricos y de plata.

El tratamiento de los Datos Personales es imprescindible e implica la protección del derecho al respeto de la vida privada, ya que la libertad de expresión y, por tanto, ambos son garantía de la república.

Muchas gracias.

Elsa Bibiana Peralta Hernández: Muchas gracias, Laura.

La verdad es que sí fue interesante.

Platicábamos aquí Ana yo mientras Laura exponía brillantemente, que sí, la verdad es que creo que la mayoría no estamos en contra de la tecnología, la tecnología nos encanta.

De hecho, estamos acá escuchando y estamos por allá usando el teléfono y estamos atentos. Podemos estar gracias a la tecnología en varios puntos a la vez.

La verdad, nos encanta y esto es algo que viene a desarrollar un aspecto, que voy a decir, con todo respeto para los caballeros, pero si decían que las mujeres podíamos hacer varias cosas a la vez, esto lo comprueba.

O sea, estamos en todas partes, estamos aquí escuchando la conferencia, tomando notas, hablando a casa, hablando a la oficina y mandándole el chisme a alguien. Y la tecnología nos encanta.

Creo que esto ya no lo vamos a poder dejar de lado, pero como bien dice Ana, poner en foros como este estos temas de alerta, nos hace conscientes del uso de la tecnología y de cómo debemos evitar que este tipo de mecanismos nos conviertan en robots o como dijo muy bien Laura en su exposición, vaya más allá del tema humano. No debemos deshumanizarnos frente al tema tecnológico.

Entonces, la verdad, me parece muy interesante este inicio por parte de Laura y creo que Ana tendrá más que comentarnos también al respecto.

En segundo lugar, le voy a ceder el uso de la voz a Rafael Pérez Colón, especialista de España y quien les mencionábamos, pues es muy inquieto también en el tema.

Adelante.

Rafael Pérez Colón: Buenos días.

Antes que nada, muchísimas gracias al InfoDF por la invitación, en particular a la Comisionada, a Bibiana por invitarme a estar aquí.

De hecho, nos conocimos en un evento de la Red Iberoamericana que fue en Montevideo, en noviembre del año pasado y a partir de ahí he tenido el honor de la invitación a compartir en este evento aquí en México.

Así que les agradezco muchísimo.

Durante el día de ayer y el día de hoy he estado haciendo un repaso de muchísimas cosas en la media en que veía cada una de las presentaciones y sentía un poco la dimensión de la tarea que están llevando a cabo todos los que están aquí y que tienen que ver con la Transparencia, con la Protección de Datos Personales y con promover todos estos marcos de tanta importancia para el desarrollo de nuestra sociedad.

En esa línea, ya casi lo estoy haciendo como práctica, preparo los mensajes en función de lo que estaba viendo y de dónde creo que puedo aportar parte de mi experiencia. De manera que agregue valor a la discusión que nos trae.

Para comentarles algunas cosas que ya irán entendiendo a lo largo de la presentación, este año yo cumplo 40 años de estar en la industria tecnológica.

Son muchos años, ¿no? He tenido la suerte de haber estado involucrado en iniciativas increíbles y he tenido la suerte de ver cómo hemos recorrido unas velocidades impresionantes, cómo hemos generado e impulsado transformaciones importantes en la vida de la gente a lo largo de todos estos años a partir de la innovación tecnológica y a partir de esas nuevas tecnologías que han ido aterrizando e integrándose a la vida de cada uno de nosotros.

Comentarles dos de las actividades en las que he tenido la oportunidad de estar involucrado en estos 40 años.

A finales de los 80 estuve trabajando por toda América Latina en el mundo de las universidades promoviendo lo que luego fue el internet, el internet básicamente en el mundo.

El internet, como saben, salió de las universidades y yo tuve la suerte de crear lo que fue el Primer Grupo Iberoamericano de Coordinación y Colaboración entre Universidades que estaban trabajando con todo este tema de las conexiones en redes de computadoras, como lo llamábamos en aquella época.

Mi primera visita a México fue en ese marco de aquel proyecto que lo trabajé desde España en el año 80 y durante esos años trabajé bastante con el CONACyT, con la UNAM y otras universidades mexicanas en lo que fueron los orígenes del internet de América Latina y todas las cosas buenas y los dolores de cabeza que nos ha traído todo eso a lo largo de los años.

Más tarde, estando con Microsoft, tuve también la suerte en el año 2000 en arrancar una gran aventura, que fue la ventura de promover

todo el desarrollo y la transformación de los gobiernos en la región de América Latina.

Básicamente lanzar las iniciativas de Gobierno Electrónico, ahora le llamamos Gobierno Digital con todos los países y ahí colaboramos con todos los gobiernos en la región.

Particularmente en México trabajamos muy directamente con el gobierno en lo que fue la Ley de Transparencia. Y bueno, creo que todos los que están aquí de alguna manera tienen mucho que ver con el resultado de ese trabajo que se hizo en México en aquellos momentos con la creación de esa Ley de Transparencia que ha dado paso a todo el trabajo que se está realizando en esta línea.

Así que bueno, durante el día de ayer lo que he sentido es el peso de la responsabilidad de ser parte de las cosas buenas, pero también de ser responsable y corresponsable de los retos que estamos enfrentando.

Y básicamente me quedaba la conclusión casi desesperante ayer y esta mañana, de que nos queda muchísimo por hacer.

Entonces, yo le comentaba a algunos de los colegas esta mañana, que yo que pensaba jubilarme pronto, pero veo que queda tanto por hacer que parece que vamos a seguir en esto por unos, no sé si aguante 40 años más o si me soporten por 40 años más.

Así que bueno, les voy a comentar los puntos, vamos a hablar un poco de “La Cuarta Revolución Industrial”, vamos a hablar algo del nuevo ecosistema digital, la economía digital, la sociedad digital, los nuevos escenarios, cuáles son las oportunidades y los riesgos, la Protección de Datos Personales en el contexto internacional, retos persistentes y algunas recomendaciones.

La “Cuarta Revolución Industrial” es un término que se ha hecho muy popular desde el año 2016, a través de un libro, un libro que se conoce como “La Cuarta Revolución Industrial”, que lo publicó Klaus Schwab, Clos es el Presidente del Foro Económico Mundial, que de hecho esta semana está celebrándose en Davos, les recomiendo visitar y ver las presentaciones. Hay una cantidad de presentaciones excelente y

espacios de debates. Están todas disponibles “On Demand” en internet las presentaciones. Esta mañana estaba hablando el presidente de Estados Unidos, creo que esa se la pueden saltar y hay otras, muchísimas, muy valiosas.

Esa, yo creo que con que vean los titulares de la prensa, que van a ser muchos, van a tener suficiente.

“La Cuarta Revolución Industrial” básicamente plantea que estamos en una etapa de transición muy importante en nuestras economías y en nuestras sociedades, en donde hemos podido medir e identificar grandes saltos.

Lo que llamamos “La Primera Gran Revolución Industrial” la ubicamos en el año 1784 y básicamente se debe al desarrollo de la tecnología de vapor y de combustión con vapor, la Máquina de Vapor, que da paso a todo un desarrollo de producción industrial a partir de esa tecnología aplicada.

El segundo gran salto lo vemos en el año 1870, lo llamamos “La Segunda Revolución Industrial” que parte del ofrecimiento de los servicios de la electricidad en forma masiva a las personas y a la industria.

Ésta transforma la forma de producir, la forma de generar servicios y la forma de vivir de forma muy importante.

Y una tercera transformación de la economía y de la industria, que es “La Tercera Revolución Industrial”, que la ubicamos en 1969 básicamente, es la Revolución Digital que comienza a partir de ese año y llega hasta el internet que transforman no solamente la forma en que hacemos las cosas, la forma en que producimos, la forma en que trabajamos y la forma en que vivimos, compartimos, aprendemos, nos divertimos, etcétera.

Uno de los elementos que vemos a lo largo de estas revoluciones, que hemos llamado “La Revolución Industrial” y en particular “La Revolución Tecnológica”, es que cada vez impacta más personas y a cada una de esas personas le impacta de forma mucho mayor, en más dimensiones impacta la vida de las personas.

Eso es algo que yo he visto, he padecido, he sufrido y he disfrutado a lo largo de estos años de trabajo alrededor de la industria tecnológica, cómo cada vez llegamos a más gente y cómo cada vez tenemos un impacto mucho mayor en la vida de esas personas.

“La Cuarta Revolución Industrial”, es una revolución que comienza en algún punto, todavía no estamos de acuerdo en qué momento la ubicamos, pero básicamente estamos en ese momento actualmente y básicamente parte a partir de un gran salto en los desarrollos de las tecnologías de la información que hacen posible hacer una cantidad de operaciones con la información sobre la que teníamos enormes limitaciones hasta épocas muy recientes.

Básicamente voy a pasar al siguiente “slide”, donde resumo algunas de esas tecnologías.

En este cuadro quiero ir pedacito a pedacito, espero que lo puedan ver bien, porque ahí resumimos bastante los pilares de esta nueva revolución que da paso a “La Cuarta Revolución Industrial”.

Y ese es el nuevo ecosistema digital que básicamente resume la etapa en la que estamos ahora, que es la etapa de la transformación digital de la economía, transformación digital de nuestra sociedad.

Hay una serie de elementos pilares de esa transformación y uno de los elementos principales o habilitador principal de esa gran transformación es la tecnología de “La Nube”.

La tecnología de “La Nube” nos permite algo que soñamos los que estamos en este campo desde el principio de la informática, desde el principio de la computación y es básicamente el poder ilimitado de cómputo.

Básicamente en eso podemos resumir de qué se trata la computación en la nube, poder ilimitado de cómputo u otros elementos más interesantes, o sea, poder ilimitado de cómputo a unos costos accesibles para la mayor parte de las personas y las organizaciones.

Ese es otro elemento muy importante sobre las características de este gran salto en el desarrollo de la tecnología, a través de la tecnología de “La Nube” o el “Cloud Computing”.

Segundo elemento, es el “Big Data” y el análisis de los datos.

Los datos han crecido a volúmenes inesperados, insospechados y siguen creciendo a una velocidad impresionante.

Sin embargo, tenemos hoy la capacidad de almacenar la información, de almacenar estos datos, de trabajar con estos datos utilizando estas capacidades ilimitadas de computación, que nos brinda la computación en “La Nube”.

Nunca antes tuvimos esa capacidad con un nivel de desempeño satisfactorio, con una experiencia satisfactoria para el usuario, para la empresa, para las organizaciones, ni para las personas.

Las redes sociales es el otro elemento que trae unos aspectos de transformación importantes como fundamento y ahí conocemos cómo la participación de las personas, los datos de las personas, la conexión y el intercambio han hecho una transformación dramática en nuestras vidas.

Y el cuarto elemento es la movilidad, el poder tener acceso a esos recursos de cómputo, a esas capacidades de computación, a esos servicios, a las personas, a esas conexiones en nuestra sociedad desde cualquier lugar, donde quiera que estemos, siempre que contemos con un acceso a internet. Y básicamente ahí entra la segunda tecnología, que junto con la computación en “La Nube”.

Sería la segunda gran tecnología habilitadora de esta gran revolución que ese la banda ancha, así como tenemos gran capacidad de alta velocidad para manejar video, voz, datos, de forma satisfactoria desde cualquier lugar en cualquier momento.

Ese cuadro, digamos, es el cuadro fundamental de los pilares de esta nueva generación de tecnología.

Y luego hay una serie de aplicaciones específicas y metodologías que se han ido desarrollando, que nos están dando un enorme poder y que nos facilitan y nos habilitan para asegurar, por ejemplo, la protección de la información, asegurar seguridad, dar ciertas garantías de servicio alrededor del tratamiento de información y de la computación.

La Tecnología “Blockchain”, si la han escuchado hablar, van a escuchar hablar muchísimo de la Tecnología “Blockchain”.

Básicamente se trata de una estructura de datos que nos da una garantía de seguridad de la información que hasta ahora no habíamos logrado alcanzar. Van a escuchar hablar muchísimo de la Tecnología “Blockchain”. Ya están escuchando seguramente hablar de inteligencia artificial.

La inteligencia artificial es otro de los grandes desarrollos tecnológicos que tuvo un gran impulso en los años 70, años 80 y, sin embargo, se detuvo porque no había la capacidad de cómputo a costos razonables que podemos tener hoy con la computación en “La Nube”.

A partir de la computación en “La Nube”, la tecnología de inteligencia artificial se ha disparado y hoy ustedes escuchan hablar de inteligencia artificial en términos genéricos, escuchan hablar de redes neuronales, escuchan hablar de “Deep Learning”.

Y básicamente son aspectos de la inteligencia artificial que facilitan el desarrollo de atención de tratamiento inteligente, análisis inteligente de la información y los datos que permiten y facilitan la toma de decisiones a través de los propios sistemas tecnológicos.

El internet de las cosas es el otro gran elemento. Es como todos los dispositivos hoy pueden estar conectados al internet. Hace un rato daba el ejemplo del reloj digital, pero bueno, podríamos tener las lámparas, las puertas, las sillas, todos estos dispositivos conectados “on line”.

De hecho, como comentaba también la compañera, hoy hay más dispositivos que personas conectados a internet, que personas en el planeta a través del internet de las cosas.

Y la seguridad, la seguridad avanzada. Es cómo aplicamos inteligencia artificial, redes neuronales y todos los nuevos recursos que nos da la computación actual para garantizar la protección de los datos con nuevas tecnologías aplicadas para la seguridad y obviamente eso nos da el paso a la confidencialidad.

La robótica que es de cierta forma una aplicación también de inteligencia artificial cuando le sumamos visión, para que máquinas puedan realizar trabajos que exhiben comportamiento que llamamos de alguna forma “inteligente”.

La realidad virtual, la realidad aumentada son también grandes de los elementos importantes que estamos viendo y la impresión en 3D.

Bueno, yo diría que eso resume bastante rápido como cuadro, ese que vemos en el área de la economía digital.

Los nuevos escenarios y los riesgos de la economía de la sociedad digital, básicamente lo voy a recorrer bastante rápido.

En Gobierno Digital. ¿De qué estamos hablando con estos nuevos escenarios?

De hecho, México ha hecho algunos avances espectaculares en Gobierno Digital en los últimos años. Y felicito mucho al trabajo del equipo de gobierno también por eso.

Menciono dos casos, el caso de Mullenguar.

Mullenguar es una municipalidad en Holanda, que luego de un ejercicio de integrar varios municipios que se habían despoblado en una región del país decidieron convertirlos en un solo municipio.

Cuando se sentaron a ver cómo organizaban el gobierno de ese nuevo municipio que juntaba a varias antiguas comunidades, pensaron en que tenían que construir un nuevo edificio de alcaldía para todos los servicios y el presupuesto no les daba.

¿Qué hicieron?

Con la tecnología de “La Nube” pusieron todo “On Line” y decidieron no construir un edificio de alcaldía. O sea, Mollenguar no tiene una alcaldía física, sino que tiene una alcaldía virtual y lógicamente todos los servicios se dan “On Line” y algunos servicios como la tarjeta de identificación, para eso va el funcionario de la alcandía, va a la casa de la persona que necesita ese trámite, que es el único trámite que tienen que hacer con presencia física.

Estonia.

Estonia se considera el país más avanzado hoy del mundo en la economía digital.

Básicamente ellos al ser una de las antiguas repúblicas soviéticas que salieron, luego entra a ser parte de la Unión Europea, estuvieron bajo amenaza supuestamente del sistema soviético por muchos años y hubo muchos ataques cibernéticos.

De hecho, uno de los ataques cibernéticos más documentados a un país en la última década, fue un ataque cibernético a Estonia que básicamente paralizó el sistema de bancos, paralizó al sistema de gobierno del país y casi todos los que estaba “On Line”.

A partir de ahí el gobierno de Estonia decidió que tenía que poner todas las capacidades de la Tecnología de la Información a servirle y asegurar que pudiesen proteger los servicios y la gestión de sus servicios para los ciudadanos en el entorno digital.

Y han desarrollado un sistema que hoy es de los más avanzados del mundo.

De hecho, pensando en Transparencia, por ejemplo, yo estuve el año pasado en varias ocasiones en Estonia, conociendo la experiencia de Estonia para un proyecto que estaba realizando para el Banco Interamericano de Desarrollo.

Y, por ejemplo, uno de los mecanismos que provee para los ciudadanos la plataforma tecnológica de Estonia, es que cada ciudadano tiene una página de Transparencia donde él puede ver quién está accediendo a la información que el gobierno tiene sobre él.

Y una de las cosas, por ejemplo, de entre las muchas anécdotas que hay, pues había una pareja, la chica era una policía y entonces ya quería conocer un poquito más del historial del candidato que estaba evaluando y se puso a estudiarlo “On Line”, a buscar su historial, expediente, etcétera.

El señor en algún momento entró a su página de Transparencia y vio que la policía lo estaba investigando.

Presenta un caso, se investiga, se encuentra que esta chica, la policía, no tenía autorización para estar investigándolo y el resultado es que, bueno, parece que la pareja del noviazgo no progresó, creo que ya está en la cárcel.

Pero demuestra cómo sí podemos tener mecanismos para garantizar la Transparencia.

Y creo que casos como los de Estonia nos da muchos ejemplos de estos elementos.

Lo otro, creo que los distintos aspectos que están ahí, no me va a dar mucho tiempo para recorrerlos, pero yo sí quiero entrar en el último punto, la huella digital.

Igual que cuando nos movemos vamos dejando nuestro ADN por todas partes, también en el internet, en el ciberespacio estamos dejando la huella digital por donde quiera que nos movemos.

Tenemos una gran preocupación, el tema sobre terrorismo es una de las grandes preocupaciones hoy en día.

El tema de los “Feck News” es una de las grandes preocupaciones hoy en día.

Las empresas están trabajando mucho con todo este tema, Facebook, Google, etcétera. Es un tema con el que están preocupados.

Amenazas a los procesos democráticos.

Hoy en Estados Unidos hay un debate enorme, como saben.

Las empresas como Google, Facebook han participado en las pistas en el senado americano donde han dado testimonios sobre cómo grupos rusos invirtieron en publicidad de “Feck News”, etcétera, durante la campaña de Estados Unidos.

El gobierno de Holanda decidió en las últimas elecciones no utilizar sistemas informáticos y hacer todo manual porque no tenían capacidad para en las fechas de las elecciones asegurar que no iba a haber una intervención y unos ataques a sus sistemas informáticos.

De esas dimensiones estamos hablando hoy en día.

La Unión Europea ha asignado un presupuesto importante para diseñar estrategias para protegerse contra los ataques informáticos al sistema democrático de la Unión Europea, supuestamente del espacio ruso.

Bueno, ahí tenemos bastante trabajo, bastantes restos que llevar a cabo, qué apuntar.

Aquí les daba un poco resumen cómo está el tema de las autoridades de Protección de Datos Personales.

Básicamente Europa es donde predomina la existencia formal de las agencias. Vemos que en América Latina ya hay bastantes países que cuentan con las agencias y obviamente en África hay mucho menos presencia y en Asia también queda mucho trabajo por hacer.

Y básicamente la conclusión ese que ahí nos queda muchísimo por hacer en términos del trabajo que están haciendo las agencias de Protección de Datos.

Voy a ir a mis recomendaciones y quizás durante el resto del debate podamos comentar algunos de los otros puntos.

Pero básicamente yo creo que hay una necesidad importante de mayor educación. Creo que las personas en general no conocemos los riesgos que tenemos, ni sabemos que hacer.

Yo creo que hay mucho que hacer de educación, tanto a los profesionales, como a las personas en general sobre los temas de Protección de Datos Personales y dar paso a una cultura de protección digital, que eso es en realidad de lo que se trata, que entendamos las implicaciones y que podamos tanto los usuarios, como las empresas y el gobierno ser parte de esa cultura digital.

Formalizar equipos multidisciplinario y un enfoque holístico.

Hasta ahora hay mucha desconexión entre las TICS, las políticas, los marcos legales, los usuarios y los consumidores.

Alianzas estratégicas.

Yo creo que se resumen en lo que yo llamo “movilización top down y movilización botton-up”.

Creo que ya el mundo del “top down” donde se deciden las cosas aquí arriba, tanto en los gobiernos, como en las corporaciones y en la sociedad está cambiando.

Ahora la participación de las personas de abajo hacia arriba está teniendo cada vez más peso, más impacto y mucho más valor y eso está ocurriendo tanto en las corporaciones, como gobierno y con los grupos de la sociedad civil.

A mí me gusta mucho cuando estamos viendo que en los países como en México, que haya ONG´s que están dedicándose a promover todo el tema de los Derechos de Protección de Datos Personales y he visto más países donde también hay organizaciones similares que están haciendo ese trabajo.

Entonces, bueno, creo que la movilización “top-dow y botton-up” puede ser parte de la clave del trabajo que nos queda por hacer.

Así que hasta ahí mis ideas.

Gracias.

Elsa Bibiana Peralta Hernández: Es realmente para mí muy penoso, Rafael, tener que estar monitoreando el tiempo, porque la verdad es que lo que exponen siempre nos deja con deseos de seguir escuchando más y aportando mucho más a esto.

Este tema es muy interesante y creo que hay que reflexionar mucho.

Decíamos hace rato, somos partidarios de la tecnología. El gobierno está ocupando mucha tecnología dentro de sus posibilidades presupuestales para implementar múltiples mecanismos para generar una gestión más eficiente.

Pero en ese tema de la gestión eficiente y el manejo de Datos Personales, estamos llevando a cabo una serie de trabajos que monitorean la vida de las personas y que se están convirtiendo también en vigilancia, que en gobiernos que pueden tener un corte un tanto, pues voy a ser extrema, totalitario, eso es muy peligroso y atenta.

Entonces, hay que poner en la balanza ahorita que estamos hablando en esos contextos, hay que poner en la balanza ese tema y lo que decíamos hace rato, ser muy cuidadosos en el manejo y procesamiento de la información, pero sobre todo, nosotros también ser muy atentos como ciudadanos, como organizados a través de diferentes agrupaciones para poder vigilar también que gobierno no haga esa vigilancia en perjuicio y límite de nuestros derechos humanos.

Eso es algo que hay que ponderar mucho y por eso a nosotros como encargados en las Unidades de Transparencia y en el gobierno encargados de estar cuidando estos temas, pues debemos poner un especial cuidado en ese tratamiento, en los fines para los cuales estamos recabando la información y demás.

Nosotros nos enfrentamos, vamos hacia un proceso electoral, ayer comentábamos algunos aspectos, vamos hacia un proceso electoral muy importante donde se han visto muy vulnerables las bases de datos y esto es algo que debemos todos tener mucho cuidado, decía, desde cuidar nosotros nuestros datos como ciudadanos y el uso adecuado en este tipo de contextos, que la tecnología realmente nos

garantice junto con el gobierno el cuidado de los mismos, para poder hacer que la tecnología se vuelva una herramienta muy útil y muy importante para el adecuado ejercicio de los derechos en una buena democracia y que esto sirva para que realmente la democracia se ejerza, que realmente haya este tipo de procesos.

Muy interesante.

Muchísimas gracias, la verdad nos gusta todo esto.

Vamos a seguir con Nelson Remolina.

Muchas gracias, Nelson. Bienvenido.

Él es especialista de Colombia.

Adelante.

Nelson Remolina Angarita: Muchísimas gracias por la invitación, por estar acá.

Yo no sólo soy enamorado de México, sino muy agradecido con México, porque me ha invitado y me ha dado oportunidad de compartir con ustedes en muchas ocasiones de manera realmente muy generosa estos temas de Protección de Datos.

Así que muchas gracias.

Yo voy a pasar muy rápidamente, traigo una presentación que luego van a consultar, queda a su disposición, para centrarme quizás en algunas ideas, porque ya se ha dicho otros temas muy importantes que por el tiempo no creo que sea importante volverlos a repetir porque ya estuvieron muy bien planteados.

Yo creo, simplemente el título que ustedes ven ahí, es que la mejor forma de proteger derechos humanos es prevenir su vulneración, prevenir su violación.

Por eso hay que enfocarse en el tema de enfoques preventivos de protección de derechos humanos.

Yo creo que este derecho de Protección de Datos hay que mirarlo desde varias cosas.

Primero. Hay muchos intereses sobre los datos, los Datos Personales.

Lo que está pasando es que hoy parece ser que es más importante el dato que la persona. Y eso es la realidad, el tema si queremos ir hacia allá o no, hasta dónde le vamos a poner límite a algunas cosas.

Para proteger los derechos humanos hay muchos enfoques, hay muchas herramientas. Ninguna es suficiente, ninguna es perfecta, pero tampoco son excluyentes.

A veces se hace una crítica a las normas. Desde luego, las normas no son mágicas. Sacar una norma de Protección de Datos no quiere decir: “Tranquilo México, tranquilo el mundo, que estamos protegidos”.

No, hay que ponerla en marcha y hacerla efectiva.

Pero lo mismo sucede con otras prácticas como la “Accountability”. A uno le venden la “Accountability” como la solución del tema y es importante, pero no es suficiente.

O sea, si alguien hace una gran guía de “Accountability”, bellísima, muy completa. Hay empresas expertas en eso, ahora miren si las están aplicando en la realidad.

Entonces, yo en últimas, cada vez concluyo, a medida que pasan los años y ya muy rápidamente, es que realmente la protección de nuestros derechos está en manos de quien tiene nuestros datos en últimas, de las empresas de las personas en el sector público y en últimas a veces de la buena fe, de la ética, la responsabilidad y la diligencia de esas personas.

Entonces, casi que el tratamiento de datos, uno como ciudadano, dice: “Es un acto de fe, no espera que quien tenga sus datos haga su tarea de manera muy sensata, responsable y ética”.

Y en esto con el tema de Tecnología también, y voy cerrando y dando ideas para de una vez dar las conclusiones en lo siguiente: Desde luego, el tema de Tecnología es totalmente bienvenido.

O sea, aquí no estamos hablando de innovación versus derechos humanos, de economía digital versus derechos humanos, sino de los unos y los otros.

Ustedes han escuchado la frase: “Que en estos temas no hay que hablar ni en términos de “tecnofobia”, ni “tecnofascinación”, sino “tecnoreflexión”. Y eso es algo que hay que tener ahí presente como tal.

En este tema también algo a propósito de lo que se planteó de lo que está sucediendo, no hablan de “Big Data”, “Cloud Shine”, internet de las cosas.

Muy bien, yo los invito a que reflexionen sobre el internet de las empresas.

¿Por qué?

Porque el internet de las empresas, que no es muy común, son las reglas que están básicamente emitiendo las empresas en todas partes del mundo a través de sus notas legales y que incluso tienen más efecto y extensión y aplicación transfronteriza que cualquier norma de un país en el mundo.

Ejemplo. Piensen en la nota legal de Facebook.

Como lo coge Facebook, simplemente porque es inevitable haber de Facebook, desde luego y porque es la red social digital más grande, tiene 2.1 billones de usuarios en el mundo, de todas partes del mundo, que proviene de todas las nacionalidades y sistemas jurídicos como tal. ¿Correcto?

Si uno pregunta: ¿Cuál es la Ley de Protección de Datos que más se aplica en el mundo o la que más infiere en la Protección de Datos en el mundo?

Pues la Ley del Estado de California.

¿Por qué?

Porque a través de la nota legal, si ustedes la leen, pues al final Facebook dice: “Que si hay algún conflicto, esto se rige ante jueces en San José California y por la Ley de California”.

Fíjense cómo una empresa desde una nota legal, desde un país y una ciudad convierte en global una norma local de la empresa. Y eso no lo ven como problemático.

Pero cuando un estado trata de sacar una norma local que vaya o tenga un ámbito extraterritorial, se vuelve un escándalo.

Aquí me preocupa, porque yo he visto eso en los congresos, hay empresas que están dedicadas básicamente a impedir normas con efectos extraterritoriales.

La razón. El internet de las empresas.

¿Qué pasa con las empresas?

Pues crean sus reglas basadas en su modelo de negocios. Y en ese modelo de negocio los datos son clave.

Es clave tener absoluta certeza de la legitimidad de que tenemos los datos, lo que pasa es que todas las empresas no tienen los datos, no los han obtenido debidamente.

Por eso hay una gran campaña para eliminar la autorización y el consentimiento. Es que con la autorización y el consentimiento no es una forma de proteger los derechos de las personas. Para nada.

Es una forma simplemente de reconocer que la persona como ser humano es el titular de sus datos y que, por lo tanto, por lo menos le preguntamos si podemos utilizar sus datos.

Es como cuando alguien llega a su casa. Pues si ustedes miran a quien dejan entrar a su hogar, no es que si Remolina llega, que es un

tipo buena gente, ético y diligente, entonces Remolina puede entrar a su casa. No.

Entonces, ojo, que el tema de consentimiento va en ese sentido, no en la forma de proteger, es la forma de reconocer que la persona es el titular de los derechos humanos. Entonces, es algo también que hay que tener presente.

Y por eso el tema acá es que esto de trabajar enfoques preventivos es algo muy importante.

Ya he ido a las conclusiones, de manera que quiero hablar más pausado. Yo aquí soy profesor ante todo, este es un grupo que trabajamos hace tiempo en algunos temas de Derecho y Tecnología que se llaman el GECTI. Los invito a que lo consulten.

Este es un Observatorio que llevamos 10 años mirando temas sobre Protección de Datos y es un enfoque netamente académico. Ahí hemos sido críticos incluso de muchos temas y decisiones de autoridades.

Yo personalmente he criticado mucho las decisiones que está tomando la autoridad de Protección de Datos de mi país, me preocupa que esa autoridad, yo siempre lo he dicho y es público, no está enfocado en proteger los derechos de los colombianos, sino derechos de otras entidades o empresas.

Eso a mí me preocupa enormemente y veo a veces en esto, y lo digo con toda preocupación, que las empresas están ganando todas las batallas porque son muy poderosas y el ciudadano no es poderoso, el ciudadano individual.

Si no se unen pues básicamente vamos a quedar sumisos a lo que definan las empresas por nosotros, los alcances de nuestros derechos casi que está definido en lo que defina alguien sobre el tema.

No quiero decir que eso sea malo, ni bueno per se, pero así es la realidad.

Y la reflexión que hago como académico es: ¿Si queremos llegar allá o no?

Todo esto que hemos conversado a lo largo de todas estas jornadas con la ocasión del Día Internacional de Protección de Datos, pues tiene que ver con este derecho que para mí es el derecho de los derechos o por lo menos el derecho del Siglo XXI.

La razón es que este derecho, aunque inicialmente surgió con una vocación muy humana, ahora tiene un enfoque muy económico, por el valor económico de los datos.

Comparto con Laura, que las personas seguimos siendo seres humamos y algo que tenemos en común aquí todos y todas al margen de dónde trabajemos, dónde estemos, es que somos seres humanos y tenemos unos derechos humanos.

Entonces, hay que pensar en los derechos humanos de los demás, de nuestros hijos y, desde luego, en nosotros estemos donde estemos.

Esa reflexión yo la hago a todas las personas, porque a veces alguien que tiene el poder se le olvida que es un ser humano que tiene hijos o que tiene abuelos o hay personas que esperan que sigan, digamos, que no desaparezca su condición de ser humano como tal.

Todos estos términos que ustedes ven ahí, ya los han visto, pues han hecho alusión a cómo lograr que cuando se recolecta, almacena y circula información de unas personas y, sobre todo, se usa, no se comprometa o ponga en riesgo los derechos de los miembros; derechos que van desde el buen nombre, la intimidad, desde luego, pero también la vida de las personas.

Mirábamos el ejemplo de sólo el manejo de una historia clínica.

En una historia clínica hay que ser muy delicados o muy diligentes en manejarla, porque si no está bien actualizada diariamente y cuando uno está hospitalizado y van a pasar por tres grupos de jornada de equipos médicos y no anotan todo, pues de pronto omitieron una información que no vio el otro equipo médico y cuando llegan le aplican a ese paciente precisamente el medicamento por el cual tiene

algún efecto negativo en su organismo, por ejemplo. Cosas así, insisto, aquí a veces también se ve afectada incluso la vida de las personas, la libertad de las personas, etcétera.

Ya comentaron esto, pero creo que una cosa es hablar de derechos humanos antes de internet, de Protección de Datos y después de internet.

Cuando se habla de una revolución es porque hay grandes cambios profundos. Y aquí creo que los hay y por eso hablaban de la cuarta generación, sin duda, sobre el tema.

El punto es que internet ha hecho al mundo transfronterizo y veo que nosotros seguimos jurídicamente, nosotros estoy hablando de los abogados, de los que regulan, mirando y regulando el mundo y actuando en el mundo como si fuera interfronterizos.

Entonces, estamos haciendo más de lo mismo en un contexto totalmente diferente. De manera que no estamos haciendo nada o casi nada.

Si seguimos pensando en regular internet con vocación interfronteras, con autoridades con competencias interfronteras, pues perdónenme, como dicen en Colombia: “Lo que estamos haciendo es el oso”. Es decir, nada, el ridículo, es la expresión.

¿Y qué pasa?

Yo siempre lo he planteado, no hay que dejar que el elemento transfronterizo en internet se convierta en impunidad.

Cada vez que hay un juicio, un proceso legal contra una empresa que no está domiciliada en un país, lo primero que llega y dice: “Qué pena, su ley no me aplica y usted no es competente. Chao”.

Yo entro a su país, desde internet recolecto los datos de todos sus ciudadanos, pero no respondo por sus leyes, ni ante sus autoridades.

No sé si a ustedes les parece que eso está bien, pero un poco es lo que está sucediendo.

En internet la extraterritorialidad se está convirtiendo en factor de impunidad.

Bien, estos son datos simplemente del mundo en que estamos. Ya se ha hablado de internet, yo les propongo la palabra, como ya está “el ciberespacio”. Es un “ciberespacio” de más de 3.8 billones de personas, vienen los datos de páginas web 1.2 billones; miden el tema de usuarios de Facebook, casi 2.1 billones.

En fin, aquí las cifras son todas enormes y en ese tema está lo que ya les comenté sobre economía digital, el valor de los datos. Se dice que hoy día permanentemente o mejor cada año, el porcentaje de la economía digital en el mundo crece 20 por ciento.

Es un gran negocio, eso está bien. Aquí hay unas cifras, por ejemplo, de Facebook, de cuánto facturó ya el año pasado o antepasado 2016, la cantidad de 26 billones de dólares.

Es una cifra significativa, de manera que como ustedes como bien saben, pues el servicio de Facebook no es gratuito, como dijo Laura, es a cambio de nuestra información.

Aquí simplemente para terminar y cerrar y de pronto hacer comentarios posteriores, es que hay un informe de economía digital, como muchos o hay varios de la OCDE y ahí un poco el tema de Privacidad, que lo engloban dentro del concepto de confianza al consumidor, toma algunos aspectos.

Pero los datos que muestran ahí es: ¿Qué están haciendo los estados?

Estos son resultados de las encuestas que hacen los diferentes estados de la OCDE sobre el tema de Privacidad.

Y si ustedes ven esas gráficas, que no sé si alcanzan a ver la letra, pero quisiera dos cosas destacar.

Uno. Es básicamente el tema de concientización a las personas. De si los estados le están jugando a que primero hablemos con la gente para que entiendan primero que sus datos son importantes.

Porque si la gente no sabe eso, no lo entiende así, pero no le va a importar el tema como tal, pero son importantes los datos de ustedes y de sus hijos.

Segundo. El tema de empoderar a los ciudadanos con herramientas para que ellos casi que se conviertan en sujetos activos y muy activos sobre la protección de sus derechos y no que el ciudadano esté siempre esperando la reacción del estado como tal.

Tercero. De pronto es el tema de investigación y utilización de tecnologías y procesos que, de entrada, ya incorporen el tema en el ADN informático de los procesos y el tema de la Protección de Datos.

Cuarto. El tema de responsabilidad demostrada.

Voy a dejar una gráfica. Quizás esta gráfica, para terminar.

La “Accountability” ya lo he mencionado, simplemente ustedes ven como un resumen de los documentos internacionales, algunos, desde luego, no todos los que han hecho en relación a este aspecto.

Esto viene, son temas, yo siempre veo que cuando hablan de “Accountability”, yo creo que en Latinoamérica se hizo en Santa Cruz de la Sierra, un documento importante que no es de “Accountability”, es de autorregulación, pero ahí ya empezaba a tener el tema de “Accountability” y se hablaba básicamente de medidas eficaces, medibles y verificables que aumentaran el nivel de protección de los derechos de las personas. Esa la gran meta en esto.

Esto implica tener buenas políticas de gobierno corporativo en tratamiento de datos en una organización.

Esto implica como lo ve en la Conferencia Internacional de Autoridades en la Resolución precisamente de Madrid, ahora en el documento de la OCDE 2012-2013 en el Nuevo Reglamento Europeo y en los estándares iberoamericanos de 2017, que pues ya se

convirtió en un documento, en algo que primero era una medida proactiva y en otros países ya se convirtió en un principio. Pero todo apunta a enviar ese gran mensaje.

Seamos responsables con el tratamiento de datos, pero ustedes me dicen: “Oiga, pero ser responsable de eso desde pequeños nuestros papás nos han enseñado a ser responsables”.

¿Qué hay de nuevo aquí? ¿Ser responsable es un gran mensaje?

Yo diría: “No, lo que pasa es que nos lo recuerdan”. No se les olvide ser responsables con el tratamiento de los datos de la gente.

¿Y qué implica eso?

Usted en su organización adopte medidas útiles, verificables y eficientes sobre la protección de los derechos de las personas.

Para eso hay muchas guías.

Yo voy a pasar rápidamente, pero simplemente quisiera darles un ejemplo sobre esto para en aras del tiempo.

Hay una gráfica que muestra que, por ejemplo: ¿En Colombia por qué se queja la gente de Protección de Datos ante la Corte Constitucional y la autoridad de Protección de Datos?

Por el tema de calidad de la información.

Es decir, y eso es muy importante mirar nuestras bases de datos.

Si tenemos bases de datos donde la información no es de calidad, hay que mirar si tenemos una base de datos o un basurero de datos, porque eso afecta a los derechos de la gente y tampoco le sirve a la organización como tal.

Bueno, el caso es que por la Corte Constitucional son 80 por ciento el motivo de las acciones de tutela, es por calidad de la información y las multas 52 por ciento.

Si estamos nosotros en un escenario de “Accountability” implica esta pregunta: ¿Qué está haciendo usted responsable del tratamiento para que la información que tenga usted en sus bases de datos sea de calidad? ¿Está siendo un mero recolector de información sin ningunos filtros de calidad, está actualizando la información o no?

Pero ese es sólo un ejemplo en temas de “Accountability”. ¿Qué estamos haciendo por eso? ¿Lo que se está haciendo es útil si o no?

Porque esos temas no nos tomaron la medida hoy, sino mirar mañana o pasado mañana, si es que hicimos, funciona y si podemos mejorarlo permanentemente.

Básicamente esos son como los mensajes.

Yo voy a terminar acá para darle la palabra a mi colega y quizás mejor si hay preguntas, pues tener la oportunidad de hablar de algún punto específico.

Muchísimas gracias.

Muy amables.

Elsa Bibiana Peralta Hernández: Muchas gracias, Nelson.

Otra vez muchos temas sobre los cuales reflexionar.

Nunca como ahora el derecho internacional público y privado tienen mucho que ver, las competencias concurrentes y una serie de circunstancias para poder valorar y regular este tema al que se enfrentan los estados con el poderío de las empresas y la influencia internacional que generan a través de todo esto. La verdad es que sí.

Y bueno, yo tengo una esperanza. El poderío de las empresas en estas etapas que tú marcaste de la revolución, de las diferentes revoluciones, recordemos cuando el bum industrial generó ese poderío económico donde los derechos laborales quedaron nulificados y con el tiempo se fue trabajando para generar la normatividad que posicionara a los trabajadores con una gran cantidad de derechos.

Yo creo que frente a las empresas también debemos ir trabajando en generar toda esa normatividad, que defienda nuestros derechos y que aunque se tarde 100 años, como se tardó en el caso del Derecho Laboral y se sigue tardando, pues en el caso de todos estos contextos podamos ir defendiendo nuestros derechos pronto, pero sobre todo, este tema de generar cómo somos responsables, primero que nada y qué estamos haciendo los gobiernos para hacer que los ciudadanos sean responsables, creo que es lo que puede ayudar a ir impulsando este tema.

Muchas gracias.

Finalmente, en el orden establecido meramente para poder desahogar la mesa, voy a ceder el uso de la voz a Ana Brian, de Uruguay.

Gracias, Ana.

Bienvenida.

Ana Brian Norgéres: Hola. Buenos días a todos.

Agradezco en primer lugar, no puedo menos que agradecer al InfoDF la posibilidad que me da estar aquí compartiendo con ustedes estos días y en especial a los señores comisionados y a la Elsa Bibiana Peralta. Gracias.

El tema que nos trae hoy a colación y además la posibilidad de disfrutar de esta linda ciudad, que si no fuera por la invitación de ustedes no estaríamos hoy acá disfrutando.

El tema que me trae acá y que nos trae como panel completo, tiene que ver con el contexto internacional en Protección de Datos.

Es un tema en realidad amplio, que habla también de responsabilidad demostrada.

Yo tomé el aspecto que tiene que ver con contexto y vamos a analizar lo que es la realidad iberoamericana en Protección de Datos Personales.

Voy a hacer un análisis breve, pero para ver cómo ha sido el proceso en Protección de Datos Personales en lo que es Iberoamérica.

Sobre los albores del Siglo XXI teníamos la Protección de Datos. Si analizamos desde el punto de vista de las constituciones en los estados, tenemos que no existía un reconocimiento expreso de la Protección de Datos.

La mayoría de los países iberoamericanos tenían mecanismos constitucionales que nos permitían defender la privacidad y había algunas constituciones que tenían también mecanismos en Frostvent, como el caso del “Habeas Data” en Brasil y otros lados.

En lo que tiene que ver con la Protección de Datos y la ley, no existían leyes con carácter general que consagraran la Protección de Datos Personales, con la excepción de Chile y de Argentina que aprobaron leyes en 1999 y en el 2000.

Se consideraba la Protección de Datos como un derecho inherente a la personalidad humana y, por tanto, dentro del concepto general estaba incluida la protección.

En ese entendido, el derecho humano a la Protección de Dato, debe ser tutelado y punible en el ordenamiento jurídico. Así lo dice la Constitución chilena y también la peruana, pero siempre en términos generales.

O sea, el individuo que veía violentados sus derechos personales estaba un poco en manos de lo que era un bue bufete de abogados que podía llevar eso a la realidad y plantearlo en tribunales.

En lo que tiene que ver con instrumentos internacionales, bueno, teníamos todos estos y muchos otros, no vamos a entrar a relaciones, a relacionarnos ahora porque ya se ha hablado mucho de ellos.

Y en lo que tiene que ver con leyes, lo que sí había muchos países en leyes específicas para determinados sectores y actividades, léase salud, datos genéticos, datos crediticios, secreto profesional.

Hay tres sitios fundamentales que cuando Iberoamérica se va acercando al Sistema Europeo de Protección de Datos Personales.

El primero está en la Declaración de Santa Cruz de la Sierra.

En Santa Cruz de la Sierra hay una Cumbre Iberoamericana de Jefes de Estado y de Gobierno y se declara como derecho fundamental el Derecho a la Protección de Datos Personales.

A continuación, hay un segundo hito. Lo que se hace es generar conciencia del Derecho Fundamental a la Protección de Datos Personales.

El segundo hito, está constituido por la Declaración de la Antigua Guatemala, en el Segundo Encuentro Iberoamericano de Protección de Datos, en el cual se crea la Red Iberoamericana de Protección de Datos.

Y el tercero, así lo consideramos, en Cartagena de Indias, cuando en una reunión de la Red Iberoamericana de Protección de Datos se coloca lo que son las funciones o los cometidos de la Red Iberoamericana de Protección.

Lo que entendemos es que la Red marcó un antes y un después y fue trayendo el sistema europeo hacia Iberoamérica.

Entonces, se coloca lo que son las funciones, los elementos de trabajo dentro de lo que es la Red Iberoamericana de Protección de Datos con una integración con la finalidad de proveer de consultas, proveer de intercambio de información.

Estos son los tres elementos que son lo que constituye la labor de la Red Iberoamericana de Protección de Datos y con esto estamos hablando lo que es el tercer hito, que entendemos en lo que es el proceso de Iberoamérica acercarse al Sistema de Protección de Datos Europeo.

¿Cómo está funcionando hoy por hoy, actualmente en el día de hoy la Protección de Datos Personales como sistema iberoamericano?

Tenemos países que tienen Leyes Generales de Protección de Datos, es el caso de Argentina, Uruguay, México. Esto pretende ser una idea macro.

Perú, Costa Rica, Nicaragua, Colombia y República Dominicana y otros países que tienen proyectos en análisis que están avanzados, como es el caso de Brasil y Chile.

Hemos sabido recientemente también que tenemos el caso de Panamá y que también tiene un proyecto de ley en análisis y que está en funcionamiento a nivel parlamentario.

De todos estos países solamente Argentina y Uruguay fueron declarados como países dentro de lo que es el sistema adecuado de Protección de Datos de acuerdo con la Directiva 25-46.

Asimismo, Uruguay es el único que ha ratificado la Convención 108, transformándose en ese momento como el país número 45 en ser país del Convenio 108 y el primer país no europeo.

¿Cuáles son las novedades últimas en lo que es la visión de Iberoamérica en Protección de Datos?

Tenemos cambios en lo que tiene que ver con Argentina y tenemos cambios en lo que tiene que ver con Perú.

En Argentina por decreto de necesidad y urgencia se incorporó como función de jefe de gobierno y ministros, la de garantizar el efectivo ejercicio del Derecho al Acceso a la Información Pública y controlar la aplicación de la Ley de Protección de Datos Personales.

O sea, se estableció la autoridad y lo que existía era una autoridad específica viniendo del Ministerio de Judiciales pasó a depender de la Jefatura del Gabinete de Ministros.

O sea, que se quitó lo que es una relativa autonomía que podía tener la Protección de Datos y pasó a estar funcionando operativamente y conjuntamente con la Oficina de Acceso a la Información.

En Perú, por su parte, el proceso que se hizo es más o menos similar por decreto legislativo se manifestó que se creaba la Autoridad de Transparencia y Acceso a la Información Pública, como una forma de fortalecer el régimen de Protección de Datos y de regular los intereses de Acceso y de Protección.

Y luego, a posteriori, lo que se hizo fue generar un órgano que dependía directamente del Despacho Viceministerial de Justicia.

En lo que tiene que ver con Uruguay, tres puntos.

En el 2008, cuando se aprobó la Ley de Protección de Datos, con carácter general, en el 2012 que salió la Declaración de Adecuación, conforme a la directiva y en el 2013, la Ley 19030 que ratificó el Convenio 108.

A grandes líneas es lo que está sucediendo con Protección de Datos.

¿Esto específicamente qué significa?

Significa que existe la Declaración de la Protección de Datos Personales como derecho fundamental, están establecidos claramente cuáles son los principios, las obligaciones, los derechos de los ciudadanos y los residentes y además hay una Agencia de Protección de Datos que se entiende autónoma e independiente.

Hay una serie de decretos también que marcan la tónica de cómo ha estado trabajando el gobierno uruguayo.

O sea, en la presentación que estoy trayendo a colación en este momento tiene que ver con aspectos normativos exclusivamente.

Pero bueno, por el Decreto 92 del 2014, los nombres y dominio de la Administración Central pasaron a ser obligatoriamente Gug O´Neil, cosa que no existía anteriormente, pero luego empezó a irse implementando.

Luego la regulación que tiene que ver con los incidentes de seguridad que se buscó que estuviera canalizada por medio del órgano de Gobierno Electrónico que se llama AGESIC, en Uruguay.

Se dictaminó también por la Ley 19179, que los organismos del estado preferirían el licenciamiento de software libres.

También resolvió que debía existir una política de privacidad de Protección de Datos en toda página que se publicara la política de privacidad.

Entonces, planteado lo que es el aspecto normativo específico de Uruguay, también queremos plantear un poco lo que son nuestras preocupaciones.

Somos conscientes de algunos defectos y queremos plantear las preocupaciones que nos trae a colación el régimen normativo uruguayo.

En primer lugar, como bien decía la Comisionada Ciudadana, la expansión de la vigilancia es algo que preocupa en todos lados, pero en Uruguay también.

Por otro lado, la colaboración entre el gobierno y los vendedores de tecnologías de vigilancia que se ha dado en los últimos tiempos, la decisión es que pueden hacerse tomadas analizando los comportamientos, los datos abiertos cuando se trata de Datos Personales en Salud, con todos los riesgos que esto implica.

La Protección de Datos en organismos públicos, que se entiende que está tal vez más descuidada de lo que quisiéramos, las amenazas a la privacidad en los sistemas de comunicaciones, la falta de un control social a todos estos elementos, las amenazas a la libertad de expresión, al Acceso a la Información y todo este tipo de amenazas que tienen que ver con Protección de Datos Personales y que nos inducen a la discriminación.

En términos generales, entonces lo que vemos a raíz de todo esto que hemos venido conservando, es que la Protección de Datos ha cambiado en los últimos años considerablemente en América Latina.

Todo el panorama general de Protección de Datos se ha diversificado totalmente de lo que era anteriormente. Como que parecería que

vamos hacia un sistema que se ha ido perfeccionando y que provee de mayores posibilidades de defender sus derechos a los ciudadanos.

Europa, por un lado, aparece con un grado de integración importante y aparece como líder de América Latina y actúa proactivamente tratando de imponer lo que es su sistema.

América Latina, por otra parte, se ve con déficits en lo que tiene que ver con integración y con déficits en lo que tiene que ver con trabajar hacia la integración.

Por otro lado, tenemos la importancia de Estados Unidos, que trata de ejercer influencia en todo lo que es América Central y América Latina y en los aspectos que tienen que ver con Protección de Datos, como lo que es las transferencias sin las nacionalidades de datos o el consentimiento. Esto trae especiales consideraciones porque hay diferencias importantes.

¿Cuáles son las dificultades principales entonces?

Son varias.

Lo que tiene que ver con las Agencias de Protección de Datos, entendemos que la idea sería poder seguir trabajando y llegar a tener un punto de un grado superior de autonomía y de independencia.

¿Por qué?

Porque esto va a colaborar y coadyuvar hacia que tengan mejores recursos administrativos y económicos y mayor autoridad para poder ejercer el régimen de Protección de Datos y hacerlo cumplir.

Entendemos que la autonomía también va a otorgar a las Agencias de Protección de Datos, medios para organizar formas de cooperación nuevas que tenemos, que son importantes para poder hacer funcionar el Sistema de Protección de Datos en internet y en el extranjero.

La segunda dificultad está porque hay un sistema de Protección de Datos, como todos sabemos, que es diferente cuando hablamos de

Estados Unidos de Norteamérica y cuando hablamos de la Unión Europea.

Y ambos regímenes tienen una importancia fundamental en lo que tiene que ver con América Latina.

Se crea ahí un problema, que es un problema analizar y un problema de ver de cuál forma se puede funcionar operativamente para que ambos puedan seguir teniendo las empresas, de ambas partes puedan seguir teniendo su funcionamiento fluido en Iberoamérica.

¿Cuáles son los desafíos entonces?

Los desafíos son varios. Los desafíos para las empresas tienen que ver con asumir un rol proactivo, con tener claro qué es lo que van a hacer con los datos, con cumplir con las normas, con pedir asesoramientos a los bufetes de los países a los que van a trabajar, con generar confianza y contratar, demostrar un perfil de Protección del Dato que lo diferencien de otros competidores.

Cuando hablamos de América Latina, entendemos que los sistemas de integración pasarían a tener algo muy importante, o sea, serían un punto fundamental para que el Sistema de Protección de Datos sea efectivo, sea bueno y que tenemos que estar conscientes también de que la seguridad de la información es un punto fundamental. No hay Protección de Datos si no hay seguridad.

En lo que tiene que ver con cada país en concreto, creemos que proveer de un marco normativo claro y ver que éste se ha cumplido, es fundamental, como una manera de que la Protección de Datos sea realmente aprendida.

Y dar a las agencias todas las formas y los medios necesarios para poder actuar con verdadera autoridad y aplicar el “Enforcement” también es muy importante, sin descuidar la importancia de la educación y la concientización, como bien decían los compañeros.

Entonces, en definitiva, ¿qué necesita el Sistema Iberoamericano de Protección de Datos?

Educar, concientizar, imponer más multas posiblemente, por lo menos en algunos casos, llevar a cabo más juicios tanto civiles, como penales; medios de cooperación y medios de integración y de armonización.

Les agradezco su atención.

Elsa Bibiana Peralta Hernández: Muchas gracias, Ana.

Te pedimos mil disculpas por los inconvenientes tecnológicos. La tecnología ya ven que sí es falible.

Entonces, aun así el ser humano sale adelante con ellas, se las arregla siempre, de verdad.

He visto que se arreglan cuestiones tecnológicas con siempre cuestiones manuales, o sea, te regresa siempre a algo manual.

El clásico caso del informático, que lo llamas porque está trabada la computadora y lo primero que hace al llegar es apagarla con el dedo, que se reinicie. Así es.

La verdad, es que con independencia de todo eso, lo destacable es que lo que tú expones en la mesa esa manera.

Fíjate que curiosamente, no lo habíamos previsto así, pero a manera de conclusión tú cierras muy bien con lo que expones.

Muchas gracias.

Podríamos manejarlo de esa manera.

Tenemos rápidamente unos minutitos extra, unos dos minutos y medio para cada quien con unas preguntas que nos hicieron llegar nuestros seguidores que nos están viendo por Facebook y ésta es de manera concreta para Rafael, pero sin perjuicio de esto, pues también la puede contestar quien desee agregar algo.

Preguntan: ¿Qué están haciendo en Europa con el tema de las criptomonedas o “Bitcoin”? Ya que como su nombre lo indica, está encriptada y, por tal motivo, es anónima.

Rafael Pérez Colón: La respuesta concreta no la sé, específicamente qué están haciendo en Europa.

En realidad, el fenómeno de las criptomonedas es un fenómeno global en este momento. La mayor parte de las personas la van como una burbuja donde hay una especulación impresionante.

La moneda principal más conocida es el “Bitcoin” y hay otras como “Ethereum” y otras que se han ido desarrollando, se basan en la tecnología de “Blockchain” que les comentaba y es lo que permite que el cifrado de la información y la seguridad sea tal, que digamos, se pueda mantener mucho el anonimato alrededor de esas transacciones.

Entonces, el país que ha comenzado a poner mucha atención en este último año, de hecho, en los últimos meses, es Corea del Sur.

Corea del Sur anunció que va a comenzar a trabajar probablemente en reglamentación, o sea, en regulación alrededor de las criptomonedas.

De hecho, eso ha sido parte del impacto que ha bajado la cotización de todas las criptomonedas en las últimas semanas a partir de eso.

En Europa, no tengo los datos precisos para decir exactamente qué se está haciendo.

Sí en el caso del gobierno español. En particular, justo esta semana pasada el Ministerio de Hacienda anunció que va a incorporar todo el tema de las criptomonedas como parte del seguimiento de los manejos de inversiones de las personas.

Eso es un debate que recién esta semana o semana pasada en España.

En el resto de los países no estoy seguro, pero creo que también es un tema que ya comienza a ponerse en la agenda política, en la agenda regulatoria y en la agenda legislativa.

Elsa Bibiana Peralta Hernández: ¿Alguien que quiera comentar algo al respecto?

La siguiente pregunta es para todos, no la personalizan y cuestionan: Si nos pueden hablar del avance del uso de Datos Biométricos, su incremento, su legalidad y protección como Datos Personales.

¿Quién desea contestar?

Nelson Remolina Angarita: Quizás sobre los datos biométricos, plantear que ya en algunas regulaciones expresamente están considerados como información sensible y cuando estamos frente a información sensible lo que piden algunas regulaciones expresamente y/o sino algunos jueces, es una responsabilidad reforzada.

Ya lo comentada, reforzada implica mayores medidas de seguridad, mayores restricciones de acceso, uso y circulación de esa información.

Hay países, por ejemplo, que por regla general en cuanto a datos sensibles la regla es la prohibición, pero vía excepciones se permite.

Hay casos que he encontrado ya extremos, eso es la regulación colombiana, porque cuando uno coloca una regulación en términos absolutos, por ser extremista creo que ya es errónea. Pero hay un artículo de la regulación colombiana que dice: “Que ninguna actividad podrá condicionarse a la entrega de datos sensibles”. Ninguna actividad.

Entonces, si uno va al médico y le dicen: “¿Qué le pasa?”. -Y dice: “No, no le quiero decir porque son datos sensibles”. Puede llegar a esos extremos ridículos como tal.

Y así quedó redactada, o sea, no ha cambiado la norma, pero quedó que hay que plantearlo a títulos anecdóticos. Desde luego, el tratamiento de datos sensibles, como los biométricos es necesario, es importante, pero obviamente también es una gran responsabilidad.

No sé qué suceda en este México y en otros países, pero cada día más el sistema de identificación nuestro son nuestras huellas particularmente.

Fíjense en los temas de voto electrónico, todas esas cuestiones están acá con nuestras huellas. Entonces, se está convirtiendo en una información de vital importancia estratégica no sólo para los titulares del dato, sino para otras cuestiones que pueden suceder, como por ejemplo, como suplantaciones de identidad.

Lo dejo ahí.

Nelson Remolina Angarita: A ver, desde la perspectiva de la tecnología, básicamente lo que son los datos biométricos, son datos y los tratamos igual que todos los datos y le aplicamos todas las técnicas y la metodología que tengamos.

Pero en línea, con todos los trabajos de Protección de Datos Personales, con todos los nuevos retos que nos plantea, por ejemplo, la computación en “La Nube”, donde los datos pueden salir para ser tratados en cualquier lugar donde haya la capacidad en ese momento disponible en “La Nube”, eso nos plantea una serie de retos que hace que cuando lleguemos a los datos se hayan comenzado a desarrollar una serie de disciplinas.

Y la disciplina o la práctica que más se está utilizando es lo que llamamos “Datta Clasification”. Clasificación de los datos.

Entonces, van clasificando los datos por su nivel de relevancia, criticidad o por su nivel de críticos como tal de los datos y se le da un perfil de tratamiento por categorías donde hay datos que se dice: “Este dato no sale de esta institución”, por ejemplo. Y otros datos que sí se permite que se puedan mover, que puedan salir a “La Nube”, que puedan ser tratados y regresar como resultados, con unas condiciones muy específicas, con anónimos, etcétera.

Todo eso es un área muy interesante que se está desarrollando, se están aplicando en instituciones de gobierno y en empresas, que es la

clasificación de los datos para asegurar que el tratamiento de los datos sea arreglado en función de cuan crítico sea el dato.

Creo que los datos biométricos, en general, son datos de alta sensibilidad. Por lo tanto, en los modelos y estos criterios se le aplican generalmente el máximo de rigor.

Laura Nahabetián: Me gustaría solamente agregar un par de cosas.

En Uruguay nosotros a los datos biométricos los tratamos en igual que en Colombia, como datos sensibles, por supuesto.

Pero de hecho, nuestra ley actual vigente de Protección de Datos no tiene ninguna referencia a los datos biométricos.

Por tanto, en la medida que estamos embarcados en la suerte de modificación normativa, los efectos de tener una cercanía mayor con el Reglamento Europeo de Protección de Datos, entre las cosas que en este momento se están planteando para incluir, está precisamente el tema de los datos biométricos en forma específica, en tanto conceptualmente hablando, para que hablemos todos de lo mismo cuando hablamos de datos biométricos, o mejor dicho, para que en el Uruguay todos quienes quieran determinar qué es la normativa legal prevé como dato biométrico pensemos igual, además de alguna regulación particular vinculada con estos.

Estos es una cuestión que está en proceso de elaboración y esperamos que más-menos a mitad de año ya esté con tratamiento legislativo.

Elsa Bibiana Peralta Hernández: Esas son las preguntas que nos hicieron llegar. Realmente los temas que desarrollaron todos y cada uno de ustedes fueron muy precisos.

El tiempo desgraciadamente siempre es corto para tan brillantes ideas ponerlas exponer de una manera más extensa, pues a veces estos foros no lo permiten. Pero en la medida de lo posible hemos podido dejar aquí muchos conocimientos y muchas inquietudes de la mano de estos expertos que nos acompañaron hoy en esta mesa.

Les agradezco de manera particular a todos y cada uno de ustedes, que se hayan tomado el tiempo de estar aquí con nosotros en México, que México también está después de sus exposiciones ahora enamorado de ustedes.

Muchas gracias.

---oo0oo---