Manzanillo, Col, 1 de diciembre de 2016.

Versión Estenográfica del Panel 4 "Aplicación de la Ley. Verificación, Inspección y Sanción, Experiencias Comparadas. Vulneraciones de Seguridad", en el marco de los trabajos del 46 Foro de Autoridades de Privacidad Asia-Pacífico (Foro APPA), llevada a cabo en el Salón "Karmina", del Hotel Barceló Karmina Palace Deluxe en esta ciudad.

Presentador: Bienvenidos al segundo panel del día de hoy, titulado "Aplicación de la Ley. Verificación, inspección y sanción, experiencias comparadas. Vulneraciones de seguridad".

A continuación, hace uso de la voz el comisionado Andrés Miranda Guerrero, Instituto Sonorense de Transparencia, Acceso a la Información y Protección de Datos Personales.

Moderador, Mtro. Andrés Miranda Guerrero: Buenos días a todos.

En el marco de este Cuadragésimo Sexto Foro de Autoridades de Privacidad Asia-Pacífico, celebramos que la sede ha sido aquí, precisamente en estas tierras progresistas de Colima, en particular en este gran puerto de Manzanillo.

Por ello, me es muy grato darles nuevamente la bienvenida, en especial a este panel integrado por grandiosos especialistas, a quienes les agradezco su presencia y me conceden el gran honor de participar con ustedes en este evento como moderador, cosa que para mí es un privilegio que me anima a seguir impulsando este tema desde la instancia de la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia.

El tema que nos ocupa en este panel es: La aplicación de la ley. Verificación, inspección y sanción, experiencias comparadas. Vulneraciones de seguridad.

Para ponerlo en contexto diremos que la Ley es condición necesaria, pero no suficiente, falta la aplicación, porque muchas de las veces lo que necesitamos no son leyes perfectas, sino que éstas se apliquen

por las autoridades responsables y competentes, porque una ley sin sanción es simulación.

Con independencia de un estudio comparado de leyes, como la de Canadá, de 1980; de Australia, de 1988; de Hong Kong y la de México en 2010, denominada Ley Federal de Protección de Datos Personales en Posesión de los Particulares, aplicada por el INAI, donde es claro su procedimiento de verificación, el procedimiento de imposición de sanciones y sobre todo la prevención de las medidas de seguridad.

De ahí la importancia de este panel, porque sabemos que ningún derecho es absoluto, todos tienen límites y este derecho de la protección de datos personales, que tiene un asidero en el apartado A, del artículo 6º, y en el segundo párrafo, del artículo 16, de la Constitución Federal, no es la excepción.

Por ello, siempre resulta importante distinguir esos límites.

Como lo menciona Raymond Geuss, no existe algo así como la distinción entre público-privado; en todo caso, es un grave error pensar que existe una distinción real, sustantiva, que pueda servir para un verdadero trabajo filosófico y político.

Sin más preámbulo, la dinámica de este panel, que me honro en compartir con estas excelentes personalidades, será que cada exponente cuenta con un tiempo de 12 minutos y dos minutos más para conclusiones.

Desde noviembre de 2010 presta sus servicios en la Agencia Española de Protección de Datos, primero en el Gabinete de la Dirección y desde marzo de 2012 ocupando el puesto de Subdirector General del Registro General de Protección de Datos.

Ha ejercido como abogado y ha desempeñado diferentes puestos en la administración española, particularmente en el Ministerio del Interior, en donde trabajó durante más de 20 años con refugiados.

Licenciado en Derecho por la Universidad Complutense de Madrid.

Él es Julián Prieto Hergueta, quien nos hará el honor, al cederle el uso de la palabra, de hacer su exposición.

Muchas gracias y bienvenido.

Sr. Julián Prieto Hergueta: Hola, buenos días a todos.

En primer lugar, quiero agradecer muy sinceramente, muy cordialmente al INAI, por la invitación que nos ha cursado para poder estar en este foro.

Es la primera vez que la Agencia Española de Protección de Datos, que la autoridad de control participa en este foro de las autoridades de Asia-Pacífico. Estamos realmente encantados de estar aquí.

Luego, también agradecer la magnífica velada de anoche, el marco fue incomparable, y quiero dar las gracias por el tiempo tan maravilloso que ayer nos hicieron pasar.

Tengo 12 minutos, y la exposición que yo quiero en este caso emplear para exponer cuál es el sistema español de experiencias comparadas, y viene a ser una continuación de todo lo que hemos tratado.

Ayer se trató de la cooperación internacional, que tiene mucho que ver. Esta mañana se ha estado hablando de cuáles son los retos, aunado a los retos que se han hablado en el panel de esta mañana, precisamente cómo poder tratar con todas aquellas reclamaciones, con todas aquellas cuestiones que se nos plantean a las autoridades de control, y que estamos nosotros directamente, efectivamente metidos en ello para encontrar también vías de solución.

Pero antes de alguna conclusión que pudiéramos sacar yo sí quisiera adentrarme y explicarles cuál es nuestro sistema. Primero, somos el organismo de control de cumplimiento de la normativa de protección de datos.

Funcionamos como una agencia independiente y no estamos sometidos a las órdenes ni a las directrices de ninguna administración. Tenemos un presupuesto que está diferenciado.

Entre las características, son la de la duración de la agencia que dispone de un mandato de cuatro años y no puede ser revocado, salvo por causas excepcionales.

Y viendo o centrándonos en cuáles son los pilares que tiene la agencia para la protección de datos: Tenemos cuatro pilares fundamentales para llevar a cabo nuestro cometido.

El primero es la capacidad de aplicación de la ley. Aquí he querido remarcar dos de los aspectos que nos va llevar el panel de hoy: La auditoría e inspección, y la protección y tutela de los derechos.

Pero no podemos dejar de olvidar que también tenemos el derecho de asesoría, donde intentamos dar solución a aquellas cuestiones para que se puedan resolver antes que acaben en un conflicto y tengan que venir en una reclamación.

O el panel de comunicación, el apartado de comunicación a través de nuestra página web, de nuestros blocks que estamos incorporando en la agencia.

Y por último la cooperación internacional. La cooperación internacional, ayer se habló de ella, se ha determinado como una de las cuestiones fundamentales a la hora del *performance* de las normativas de protección de datos.

¿Qué competencias tenemos en materia de protección de datos de inspección, de poder verificar el cumplimiento?

Nos lo daba nuestra propia Ley, nuestra propia Ley nos permite inspeccionar todos aquellos ficheros a los que se refiere el ámbito normativo de protección de datos, y podemos recabar cuántos datos, informaciones estimamos por necesario.

Pero también la agencia tiene, aunque no voy a entrar en ello, tiene otros aspectos sancionadores que le atribuyen otras leyes.

La Ley General de Telecomunicaciones Española le atribuye competencias a la hora de poder determinar sus infracciones en vía de telecomunicaciones o en publicidad telefónica, a parte de las quiebras

de seguridad que aparecen por primera vez en el marco jurídico español.

O la Ley de Servicios de la Sociedad de la Sociedad de la Información, donde también la agencia puede llevar a cabo inspecciones en materias de cookies, o en materias de España.

El organigrama, y aquí quería solamente remarcar, irme a la parte de la derecha, la Subdirección General de Inspección y las personas que estamos dedicando a resolver las reclamaciones que nos llegan a la agencia.

En estos momentos, salvo que se haya podido producir un cambio de última hora, que nunca se sabe en la administración española. Más o menos estos son los recursos de los que disponemos.

Tenemos 23 personas que son las que se dedican a inspeccionar, a verificar los hechos de aquellas cuestiones, de aquellas quejas que se nos acaban planteando o que la agencia tiene conocimiento.

Tenemos a 29 personas que son los que hacen una determinación jurídica de esos hechos; y en el apartado de la tutela de derechos, el acceso, la cancelación, la rectificación y la posición, disponemos de 11 personas. Este es nuestro staff para aplicar la Ley y que nos viene a ser bastante justo como antes se ha ido diciendo.

Los recursos son muy escasos, y las posibilidades de aumentarlos no son fáciles.

La Subdirección General de Inspección establece, yo acabo de decir varias funciones: Estudia las reclamaciones formuladas por los ciudadanos, y tiene una actuación preventiva, y es que lleva a cabo funciones de inspecciones de oficio que son con carácter preventivo para conocer en qué determinados sectores cómo se están desempeñando, cuáles son las actuaciones que se están llevando a cabo, y si tienen que modificar sus tratamientos, y si tienen que modificar sus protocolos de actuación.

Y como procedimientos lleva a cabo tres tipos de procedimientos. Por un lado las infracciones que puedan cometer los responsables de

tratamientos de titularidad privada, las empresas privadas, las entidades privadas.

Aparte tenemos cuando la inflación la comete una administración pública con otro tipo de procedimiento que se diferencia en la parte final y el procedimiento de tutela de derechos.

Los apartados, los sectores que están ahí señalados son los grandes sectores que a todos nos concierne en esta materia, fundamentalmente, en un desarrollo exponencial, los que tienen relación con la tecnología y con la evolución de las telecomunicaciones.

En la actuación preventiva que con ella intentamos, que la Ley se acabe cumpliendo en aquellos sectores, tenemos varios criterios para elegirlos, fundamentalmente son aquellos en los que hay algún elemento que hace que la agencia se mueva en esa línea o porque los datos que se tratan son datos sensibles o porque hay tratamientos masivos de datos o porque puede haber una acumulación de denuncias en un determinado sector.

Así nos ha ocurrido, por ejemplo, con los casos de las subcontrataciones, las suplantaciones, la contratación de determinados servicios o la actuación de las entidades de recobro de deudas, los encargados del tratamiento.

Se han llevado a cabo actuaciones sectoriales de inspección que tienen como fundamento, sobre todo describir cuáles son las actuaciones que se llevan a cabo en el sector.

En este caso no hay ninguna identificación con una mala actuación y un responsable, sino simplemente se quiere describir al sector de cuáles son sus actuaciones.

Se establecen al final unas conclusiones y unas recomendaciones, no hay, no sigue a esta actuación ninguna línea sancionadora. Pudiera darse el caso, si fuera excepcional, pero no sigue ninguna línea sancionadora, simplemente de lo que se trata es de establecer unas orientaciones, unos criterios para que el sector se acomode y venga a

cumplir con lo que la normativa en materia de tratamiento de datos establece.

Los sectores que hasta ahora, esto es un ejemplo de las que hemos llevado a cabo; yo por señalar me fijaría en la última que se llevó a cabo el año pasado, es la utilización de servicios de cloud computing en el sector educativo, cada vez son más los colegios, los centros escolares, los institutos que utilizan herramientas de información en la nube y cuya observancia de la normatividad no siempre es cumplida como se debe.

Esto nos ha llevado durante todo el año pasado a un examen exhaustivo y se ha publicado en medidas relativamente poco, con una serie de conclusiones y de recomendaciones y que se irá actualizando según vaya funcionando esta materia.

Pero tienen otros sectores, que los pueden ustedes ver ahí, en hospitales también está pendiente para el año que viene una nueva inspección de oficio para ver el tratamiento en centros sanitarios.

Como potestad sancionadora, la Agencia ahí ya puede actuar y acabar en una sanción, pero tiene los apartados en donde se va a actuar; primero las actuaciones previas que van a servir para determinar los hechos y si a partir de esos hechos se puede seguir un procedimiento sancionador o se archivan los hechos.

Estas actuaciones previas siempre tienen lugar a instancias de los denunciantes, de los ciudadanos, fundamentalmente.

Puede ser también por iniciativa de la dirección o también por la motivación o la solicitud de algún órgano, pero fundamentalmente, y lo veremos luego en un cuadro, vienen, son consecuencia de denuncias que recibimos de los ciudadanos.

Solamente en estas actuaciones de lo que se trata es de determinar los hechos, no se va a hacer ningún análisis jurídico, sino qué hechos y quiénes pueden ser los responsables.

¿Y quiénes los llevan a cabo? Los llevan a cabo las 23 personas a las que antes hacía referencia, que son especializadas en la materia por

sectores, son competentes, tienen la consideración de autoridad pública, tienen la obligación de revelar el sector de imparcialidad y lo que es importante en el caso de obstrucción, porque nos hemos encontrado, me imagino que la experiencia todos la hemos tenido, una cierta oposición a inspecciones, una obstrucción.

La obstrucción a la inspección en este caso es considerada como una infracción grave y es objeto de sanción diferente.

El plazo que tenemos para estas actuaciones es de 12 meses. En estas actuaciones podemos actuar desde una posición, una perspectiva no presencial, es decir, directamente desde la Agencia, recabando toda aquella información, todos aquellos datos y hechos que nos sean necesarios, tanto de los denunciados como de los denunciantes y como de entidades terceras, registros públicos, incluso registros privados.

O podemos hacer las actuaciones presenciales, que consisten en el desplazamiento a los locales, en este caso del inspeccionado y la sede donde se encuentren los ficheros o el tratamiento.

La inspección alcanza no sólo a los documentos, alcanza también a los equipos físicos y lógicos, y podemos dar las instrucciones para que pongan en marcha un determinado tratamiento, registro o procedimiento de gestión de soportes.

Del resultado de la potestad sancionadora se pueden derivar, evidentemente, que dos cosas: Su archivo, porque no constituye una infracción o que pueda ser constitutiva de infracción, en cuyo caso se inicia un procedimiento sancionador.

Estamos hablando de 12 meses que se han podido consumir. Para estas actuaciones previas ya tenemos un procedimiento sancionador, que lo vamos a resolver en seis meses, como máximo.

En este caso, en el procedimiento sancionador se lleva a cabo por los instructores que determinan y llevan a cabo la calificación jurídica de los hechos como características y además han introducido últimamente, están las posibilidades al inicio de reconocer la responsabilidad por parte del inspeccionado, por parte del

denunciando y una posibilidad de pago inmediato de la sanción que podía ser objeto, lo cual conlleva una reducción de la sanción y que nos está dando también ciertos resultados.

Todavía no hay datos definitivos, pero la agencia está contenta porque ha evitado continuar con procedimientos y gasta recursos, porque en este caso se han acogido a esta posibilidad de pago fraccionado.

La finalidad de este procedimiento acaba con una resolución, que puede ser concretando que no hay vulneración de la normativa de producción de datos o que hay una vulneración y se acaba imponiendo una sanción.

Ahí, hablando del apercibimiento, porque una de las opciones que tiene la agencia para aquellos casos en los que la infracción fuera grave o leve, nunca muy leve, nunca muy grave y se dieran determinadas circunstancias, lo que puede es emitir un apercibimiento al denunciado para que lleve a cabo las medidas correctoras y acomode el tratamiento de datos a lo que exige la normativa a los principios de protección de datos.

De no ser llevado a cabo, evidentemente acaba constituyendo en infracción. Pero esa posibilidad, que está establecida desde el año 2011, también ha facilitado que muchos procedimientos finalicen ahí y se acojan, muchos de los denunciados se puedan acoger a esta vía, como veremos posteriormente en la recaudación que vamos haciendo.

En el caso de administraciones públicas el procedimiento es el mismo, sólo que en el caso de haber una infracción se declara la infracción y se impone una multa; se le pide que adopten las medidas correctoras oportunas a la administración, pero la agencia no va sancionar económicamente a un ministerio ni a la presidencia del gobierno ni a un ayuntamiento ni a una alcaldía; le va obligar a que ponga aquellas medidas correctoras, para que el tratamiento de los datos se acomode a la normativa.

Y, eso, sí le acaba enviando una copia al defensor del pueblo de esa decisión, para que la tenga en cuenta; pero ahí acaba nuestra labor.

Frente a la potestad sancionadora y también en ámbito del cumplimiento de la Ley, la agencia dedica a las personas que antes señalábamos, orientándose a la tutela de derechos; la tutela de derechos, que la tenemos que resolver en e plazo de seis meses y que conforman todas aquellas actuaciones necesarias, para ver si el acceso ya sido correctamente denegado o la cancelación o la oposición o la rectificación.

En este caso la resolución consiste simplemente en estimar o no estimar este derecho y en caso de que sea estimado y que no se cumpla por parte de los responsables en el plazo de 10 días, conlleva un procedimiento sancionador y una infracción, en este caso grave.

En quiebre de seguridad también tenía un apartado, porque la quiebra de seguridad la recoge nuestra normativa hasta el momento exclusivamente la Ley General de Telecomunicaciones.

Cuando entre en aplicación, en mayo del 2018, el nuevo Reglamento General de Protección de Datos, tendremos esa misma figura en el ámbito de la protección de datos.

En el ámbito de telecomunicaciones lo que los operadores de redes o de servicios de comunicaciones públicas nos tienen que notificar, son aquellas violaciones de seguridad que pongan de manifiesto la quiebra, la pérdida o el acceso inconsentido a los datos de carácter personal, como consecuencia de las comunicaciones a través de servicios públicos de comunicaciones.

No tenemos capacidad, en este caso, sancionadora, pero sí podemos recordar o reiterar a los operadores la adopción de aquellas medidas de seguridad necesarias, para que se subsane la violación o se subsane la quiebra que se haya podido detectar y se pongan todas aquellas medidas correctoras.

No hay –como ya digo– en este caso ninguna opción de sanción.

¿Qué tenemos en infracciones?

Aquí quisiera señalar, de manera breve, que tenemos tres tipos de infracciones: Leves, graves y muy graves, que van con unas

sanciones de 900 euros a 40 mil euros para las leves, de 40 mil uno a 300 mil euros para las graves y de 300 mil uno a 600 mil euros para las infracciones muy graves.

La Ley se acompaña de un conjunto de criterios o de características para graduar la sanción dentro de ese abanico, como si el gasto continuado, el beneficio que haya podido tener el infractor.

De su actuación infractora, los daños y prejuicios causados a los interesados, si han puesto o no, o aplicado procedimientos para corregir las causas que dieron lugar a la infracción. Y todo eso se va tener en cuenta a la hora de graduar la sanción a imponer.

Pero como nos vamos acercando al límite de tiempo, solamente yo quisiera señalar lo del apercibimiento, el apercibimiento que se introduce en la Ley en el año 2011 y que se introduce de una manera excepcional, como de manera excepcional cuando se atiende a la naturaleza de los hechos, siempre que la infracción no sea muy grave, que sea grave o leve, y siempre que se den una serie de circunstancias atenuantes, por decirlo así.

En ese caso, la agencia, desde el año 2011 ha aplicado la figura del apercibimiento en muchos casos, evitando en este caso la sanción económica a muchas empresas.

Tenemos también la posibilidad, durante el procedimiento sancionador, de inmovilizar los ficheros, es una posibilidad que desde que yo estoy en la agencia la he visto utilizarse una sola vez, es bastante efectiva, y en este caso lo que permite es inmovilizar aquellos ficheros, cuando como consecuencia de una infracción muy grave, en la tramitación de un expediente o de un procedimiento por infracción muy grave, lo que se pone de manifiesto es que el tratamiento de los datos personales lo que puede acarrear son un alto riesgo a los derechos y libertades fundamentales de los interesados.

Se puede requerir, en este caso, a la entidad involucrada, y en el caso de no llevarse a cabo el cese, la tramitación de los datos personales, se puede dictar una resolución inmovilizando los ficheros.

Pero como ya digo yo, lo he visto, desde que estoy prestando servicios a la agencia, en una sola ocasión.

Ya para acabar, esta es nuestra línea de denuncias. Los que están en las barras gris son los procedimientos sancionadores, las actuaciones de inspección, y en la línea azul son las tutelas de derechos.

Antes se ha comentado que hemos ido creciendo, efectivamente, menos este año, 2015, que hemos detectado un descenso de 10 mil a 8 mil denuncias. Es un número de denuncias, que por decirlo de alguna manera, está colapsando los recursos que tiene la agencia.

Entonces, encontrar, como antes se ha dicho, soluciones alternativas de resolución de conflictos, como pudiera ser el acudir a aquellas vías en las que queden satisfechos, tanto los afectados como los interesados, puede ser bastante interesante, y en los que la agencia está muy interesada en estas posibilidades.

Quizá el nuevo Reglamento Europeo de Protección de Datos, a través de los códigos de conducta nos permita, y a través de los delegados de protección de datos nos permita esta posibilidad.

Por último, yo quería señalarle que este es el volumen de recaudación que la agencia tiene en los últimos años, y en consecuencia, entre otros, de la entrada en vigor de la figura del apercibimiento, entre otras cosas, evidentemente no exclusivamente ellas, hemos pasado de una imposición de sanciones por 20 millones de euros en el año 2012 a 12 millones de euros el año pasado.

Con lo que se puede demostrar que el nivel de cumplimiento es mayor. También es consecuencia, en el año 2015, del número, el descenso de denuncias que se nos han planteado ante la agencia. Ese es el volumen.

Desde luego las actividades donde más sanciones se imponen son las telecomunicaciones, con un 51 por ciento. Es el sector que más infracciones acaban siendo detectadas y donde imponen mayores sanciones.

En esta última diapositiva lo que quisiera recalcar, y se puso ayer de manifiesto, es la importancia de la cooperación internacional para la aplicación efectiva de la Ley.

Y dentro de, bueno, esta relación del grupo de trabajo, el artículo 29 o la Red Iberoamericana de Protección de Datos; ayer se mencionaba que el Reglamento General de Protección de Datos establece, en su artículo 50, la posibilidad de adopción de medidas, tanto por la Comisión Europea como por los estados miembros, para llevar a cabo acciones de cooperaciones entre los estados de la Unión Europea y terceros estados para la aplicación de la ley, especialmente en la posibilidad de revisión de reclamaciones, asistencia de información, que tiene que ser o ha de ser una de las vías en las que podamos hacer o poder aplicar la ley en un ámbito tan globalizado en el que las tecnologías lo invaden y no hay fronteras para ello.

No sé si me he pasado mucho, pidiéndole disculpas al moderador.

Muchas gracias, muy amables.

Moderador: Agradecemos la participación de Julián Prieto Hergueta.

A continuación, es licenciado en derecho por la Universidad Autónoma de México, tiene diversos posgrados y es doctor en derecho con el reconocimiento Summa Cum Laude por la Universidad Panamericana de la Ciudad de México, la máxima distinción que entrega la Universidad.

Ha sido catedrático en diversas universidades impartiendo clases de derecho; se ha desempeñado en diversos cargos público, tanto administrativos como de elección popular, entre los que destacan la Presidencia del Honorable Tribunal de Arbitraje del Estado de Morelos; Secretario General de Gobierno del Estado de Morelos; Delegado del Departamento del Instituto Federal en Azcapotzalco; Presidente Municipal Constitucional de Cuernavaca, Morelos; Presidente de la Comisión de Hacienda de la Asamblea Legislativa del Distrito Federal; Diputado Federal; Senador de la República, y actualmente se desempeña como Magistrado del otrora Tribunal Federal de Justicia Fiscal y Administrativa, el ahora Tribunal Federal de Justicia Administrativa.

Con ustedes el doctor David Jiménez González.

Dr. David José del Carmen Jiménez González: Muchas gracias.

Me da mucho gusto saludarlos a todos ustedes, agradecer la hospitalidad de esta magnífica ciudad que es Manzanillo, de nuestro estado de Colima, que realmente es una de las bellezas que tenemos dentro de este marco que conforma nuestro país.

Yo quiero agradecer a mis compañeros Andrés Miranda Guerrero, Oscar Puccinelli, a Richard Benham y a Julián Prieto, la participación que me dan en esta oportunidad.

No era yo el indicado el que venía a hablar sobre estos temas tan importantes, era el señor Presidente del Tribunal, Presidente de la Junta de Gobierno, el doctor Manuel Hallivis Pelayo, pero hace treinta y tantas horas me comunicaron que si podría venir en su representación y del Tribunal a discernir, a platicar, a dialogar con ustedes sobre estos temas tan importantes. Por supuesto que acepté y por eso estoy aquí.

Yo quisiera hacer algunas reflexiones, si ustedes me lo permiten. Fíjense que en el año 2000, efectivamente, participé en el Senado de la República, y del 2000 al 2006, que terminó nuestro periodo en las dos legislaturas que conformaban el Senado en aquel entonces, nos dimos a la tarea de ir pensando en una Ley Federa que permitiera proteger los datos personales en posición de particulares o de las propias dependencias gubernamentales.

Y, a decir verdad, no pudimos hacerlo, terminó nuestra gestión en el Senado y no salió la Ley sino hasta el año siguiente, hasta enero de 2007. Ya para ese entonces su servidor ya estaba designado por el Presidente de la República y por el Senado como Magistrado del Tribunal Fiscal Federal de Justicia Administrativa.

Y ahí nos permitió ver un panorama muy amplio, ya concretamente desde el punto de vista jurisdiccional, de qué es lo que acontece cuando se suscitan controversias entre los particulares y las autoridades, y desde luego no escapaba dentro de esta área del

Tribunal Federal de Justicia Fiscal y Administrativa en aquel entonces lo que nosotros venimos en este momento a escuchar, a plantear y a exponer de nuestras experiencias respecto a la protección de los datos personales.

¿Qué es lo que hemos nosotros podido observar? Si bien es cierto que en nuestros países, en donde queremos que verdaderamente los sistemas democráticos funcionen, que nuestro sistema normativo funcione, en donde las conductas irregulares o ilícitas se sancione, en donde este tipo de conductas no queden impunes para evitar que se repitan las conductas que tanto daño no solamente han hecho desde el punto de vista económico a nuestros Estados, y me refiero a países. O ya dentro de nuestro propio país, me refiero a nuestras entidades o a nuestras municipalidades.

De tal manera que aquí vemos que el marco normativo no solamente lo vamos a referir a una sola Ley. La Ley tiene que estar armonizada con el resto de las leyes.

La Ley de Protección de Datos Personales tiene que ir forzosamente vinculada con otra Ley, que es el acceso a la información.

Del acceso a la información fundamentalmente va orientada para que los ciudadanos, la sociedad en general sepa y conozca fundamentalmente quiénes son aquellos que en un momento dado pueden estar detentando el poder público, pueda estar detentando el poder económico, o tengan una fuerza de carácter político o social que redunde dentro de la misma vida de la sociedad.

Por eso es tan importante que vayamos analizando cada uno de los preceptos que cada dispositivo normativo establece para que no encuentren en su momento una contradicción o una oposición.

Los datos, por ejemplo, que el INAI tiene respecto de los servidores públicos, aunque el servidor público sea muy importante tienen forzosamente que darse a conocer.

No los podemos considerar como confidenciales, sino que debemos al contrario darle, como dice nuestro artículo sexto constitucional, la máxima publicidad.

¿Para qué?

Para que el pueblo esté perfectamente enterado de quién es quien ocupa un determinado cargo público y cómo este se desempeña en él y cuál ha sido su trayectoria.

Lamentablemente en los últimos meses hemos conocido los mexicanos de casos sumamente dolorosos que han pasado en diferentes partes del país, en diferentes entidades. No quisiéramos que eso pasara.

Y a veces eso pasa, y México no es la exclusividad, lo podemos ver en el resto del mundo, no solamente de América Latina o algunos países africanos o del Medio Oriente, sino también en Europa y en los Estados Unidos, en Canadá o en los países más avanzados, en suma, del mundo.

¿Entonces qué es muy importante que tengamos acceso a esa información?

Sí, a esa información que nos permita tener el objetivo primordial para conocer a una persona que con esos datos la hacen identificable, la hacen distinta a los demás.

¿Por qué?

Porque hemos venido cayendo en una serie de actitudes, de conductas o de acciones que sin darnos cuenta han venido a repercutir no solamente económicamente a un particular, sino a las mismas sociedades.

Por eso el acceso a la información, protegiendo los datos personales por supuesto, nos van a permitir tener una magnífica orientación.

El artículo seis de nuestra constitución, y el artículo 73 como el sexto, fueron modificados y reformados por el Congreso de la Unión.

¿Y por qué fueron modificados?

Primero, para darle competencia al congreso para legislar sobre estas materias.

Segundo, en el artículo 16 se agrega un segundo párrafo para dar la protección a, desde luego, los particulares cuando vean vulnerados algunos de sus datos que se consideran personales y que puedan afectar su propia persona, su ente como individuo.

Y por eso se habla, y se ha venido comentando aquí en estas mesas lo que es el arco. Que es el acceso, la corrección, la rectificación y la oposición que tienen los particulares para oponerse a la publicación o a la eliminación que consideran que vulneran su personalidad.

De tal suerte que hemos nosotros venido avanzando en eso. Y al ir avanzando en esto, lo que nos ha permitido es que lleguemos a transparentar cada vez más algo que es muy importante, la actividad que realizan cierto de personas encargadas o al frente, tanto de instituciones públicas como de instituciones privadas o instituciones morales.

En el tema que nos ocupa podíamos irnos a ciertos casos particulares que hemos visto dentro del propio Tribunal y otros que han salido de la esfera del mismo.

Pero que esto es muy importante, porque de estas actividades de las leyes que hemos mencionado, pueden derivar conductas sumamente delicadas, que se encuentran perfectamente tipificadas dentro de otro tipo de ordenamientos jurídicos, como puede ser el Código Penal.

Y ustedes se preguntarían: ¿Cuáles conductas o qué irregularidades podríamos encontrar en ellas?

Pues se puede presentar el fraude, se puede presentar el abuso de confianza, se puede presentar la asociación delictuosa, etcétera.

Con los adelantos tecnológicos hoy, por ejemplo, ¿qué es lo que nos hemos percatado y aquí en estas mesas se ha dicho ya?

La evolución de las telecomunicaciones, la evolución tecnológica ha permitido que fácilmente tengamos acceso a una serie de información

que nos interesa, para bien para muchos, y otros para usarse de una manera incorrecta.

Entonces, ¿qué es lo que nosotros estamos viendo?

Que hoy día, y ustedes lo pueden consultar, inclusive en aquellos países que vienen de Asia, de América Latina, de Europa y de los Estados Unidos, lo que viene siendo el robo de identidad o usurpación de identidad.

Por eso es tan importante que la protección de estos datos personales, cuando son clasificados como tales, confidenciales, tengan que ser salvaguardados.

Pero aquellos en donde se hace necesario que la sociedad conozca el desempeño, las actividades, la eficiencia y los resultados de lo que ha pasado en el desempeño también de ese tipo de actividades, fundamentalmente de personas morales.

¿Por qué? En este tipo de usurpación de identidad lo que hemos estado viendo cuando se dan falsificaciones de firmas, por ejemplo, al de los notarios, los notarios públicos, en donde tiran instrumentos que permiten, a su vez, con esos poderes, llevar a cabo la ilicitud de otros instrumentos notariales.

¿Y ahí qué es lo que estamos viendo? Que muchas veces por ignorancia o por no haber conocido esa información oportuna, y no es porque estemos afectando datos personales de determinada persona o determinado individuo, vengan a ser violatorio de garantías constitucionales.

Yo creo que sí es muy importante que tengamos en cuenta qué es lo que nosotros debemos entender como una verdadera reserva como dato confidencial y cuáles deben ser totalmente publicadas.

En el Tribunal Contencioso Administrativo de los Estados, como sucede en el nuestro, en el federal, verán ustedes que se publican unos en el Diario Jurisdiccional que tienen a su alcance los tribunales; otros, nosotros, por medio del boletín electrónico, en donde tenemos que dar a conocer, ¿qué? Quién es el actor, el número del expediente,

quién es el magistrado ponente que está llevando el asunto y contra qué autoridad se está impugnando uno de sus actos.

Muchas de las gentes pensaron que el poner eso en el boletín electrónico y salir a la publicidad para que surta efecto la notificación, por ejemplo, podría violentar sus derechos respecto a la protección de datos personales.

Y entonces acudieron a lo que el propio artículo 16, en su fracción II, Constitucional establece, ¿qué es lo que el titular de ese tipo de derechos puede tener? Primero, el acceso, la rectificación, la corrección o la oposición.

Un caso emblemático en el Tribunal, en la Sala Superior, en donde una persona impugnó, pero no lo impugnó más que por la vía de la oposición, circunstancia que por cierto –si mal no recuerdo– todavía no la tenemos perfectamente reglamentada, pero que podemos aplicarla forzosamente.

¿Por qué? Porque ya se encuentra en los convenios y tratados internacionales y también se ha hecho exploración doctrinaría sobre esta situación de la oposición a lo que tiene el particular derecho a que se manejen sus datos personales.

Un minuto más. Creo que al final del camino a todos nos interesa que nuestros datos personales, los confidenciales tengan verdadera salvaguarda; es decir que estén garantizados, y lo están.

Porque aún las instituciones, cuando emitan un acto, en el cual la estén lesionando, el particular puede acudir a uno de nuestros maravillosos medios de impugnación, que es el Juicio de Amparo.

De tal manera que aquí lo que tenemos que hacer es coordinar y saber perfectamente bien, dentro de equis número de leyes, cuáles son aquellos datos que deben de ser totalmente protegidos y cuáles deben ser difundidos.

De ahí la importancia en que podamos armonizar nuestro ordenamiento jurídico y podamos llegar a que cuando se viole cualquier tipo de disposiciones de esta naturaleza, que no quede

flotando la sanción o la recomendación, sino que fundamentalmente tenga una sanción.

Muchas gracias por su atención.

Moderador: Muchas gracias, doctor magistrado del Tribunal Federal de Justicia Administrativa de nuestro país.

Es investigador y catedrático de la Universidad Nacional de Rosario, en la Pontificia Universidad Católica Argentina.

Además, es profesor honorario de las siguientes universidades peruanas: Universidad Privada Antenor Borrego, Nacional de San Agustín de Arequipa, Nacional de Piura en Nacional de Huanuco.

También es Juez de la Sala Segunda de la Cámara de Apelación en lo Civil y Comercial en Rosario, y ha participado en alrededor de 300 cursos de posgrado, congresos y jornadas en Argentina y en el exterior, sobre protección de datos personales y acceso a la información pública.

Es Doctor en Derecho Constitucional por la Universidad Nacional de Buenos Aires; además, ya recibido el título de Doctor Honoris Causa por la Universidad Privada Antonio Guillermo Urrelo y por la Universidad Nacional de Cajamarca.

Él es Oscar Raúl Puccinelli. Por eso les decía que son grandes especialistas y eso que leí una tercera parte del currículum.

Adelante, Oscar.

Sr. Oscar Raúl Puccinelli: Muchísimas gracias por la presentación.

Yo agradezco enormemente, por supuesto, al INAI y a los amigos de México que siempre han sido y son tan generosos conmigo.

La verdad es que es un honor para mí, además de esta en este foro, en este evento tan importante, donde se están tratando temas tan trascendentes.

Yo voy a tratar de ir muy rápido en una primera parte. Les pido que básicamente sigan las imágenes, no hagan esfuerzo en ver los textos porque la idea era es ser gráficos.

Fundamentalmente voy intentar hacer una primera explicación, en especial porque hay alumnos y hay mucha gente que nos sigue por streaming.

Básicamente explicaré lo que es el derecho a la protección de datos y algunas de las dificultades que presenta en la práctica; especialmente cómo se ha llegado hasta hoy.

Lo primero que queremos destacar –ya se ha dicho– estamos entre autoridades que algunas de ellas tienen las dos funciones: Las funciones de controlar el acceso a información pública, hacer efectivo el derecho al acceso a la información pública y también la de proteger los datos personales.

Algunas han llegado a los datos personales desde el acceso y otras hemos llegado de la protección de datos al acceso a la información pública pública, como puede ser España, como es Argentina, que acaba de editar, después de muchos años, su Ley de Acceso a Información Pública, su primera Ley.

Lo primero que tenemos que destacar es que estamos en el ámbito del derecho a la información; el derecho a la protección de datos está en el campo del derecho a la información, y en el derecho a la información vemos –como dije antes– estas dos vertientes: El derecho de acceso a la información pública, el derecho a la protección de datos, que son característicamente disfrontales.

Es decir, uno está gobernado por el principio de máxima publicidad y el otro precisamente por el de minimización, el de básicamente la restricción máxima posible a la publicidad de los datos.

Ponemos al Dios Jano, como ejemplo, el Dios Jano era un dios de los romanos que miraba hacia, era el dios de los principios y el dios de los finales también, porque por eso también incluso enero se llama de esta manera Janeiro, enero es precisamente, marca el fin de un año y el comienzo de otro.

Esto es bien importante, cuando hablamos de autoridad de control; a mi modo de ver las autoridades de control deben ser colegiadas, y precisamente, cuando se tratan estos dos temas, porque quienes vienen por el lado de acceso a la información están más impregnados, en principio mayor publicidad y ahí la discusión se traba entre estas dos vertientes y se logra un resultado mucho más equilibrado.

Por supuesto que la archivística, los archivos en la antigüedad eran muy primitivos, no voy hacer una evolución ahora, sinceramente tenemos que recordar que este problema, la protección de datos no empezaría en aquel tiempo, pero simplemente los archivos son tan antiguos como la humanidad misma.

El problema empieza con la prensa escrita, y acá otro problema que se presenta, en colisión en este momento, muy fuerte, es con la libertad de expresión; es decir, nosotros tenemos tres derechos muy importantes cuando hablamos de protección de datos, que son el derecho de acceso, el derecho, por supuesto, a la protección y la libertad de prensa, que juega un papel preponderante, especialmente a partir del periodismo, que esto es lo que conocemos, ahí están las gacetas donde empiezan las noticias escritas.

Ahí hay dos monedas que precisamente se llaman gacetas, el nombre de periódico se asimila con el de gaceta porque precisamente era lo que costaban los primeros periódicos.

Entre 1700 y 1800 aparece la libertad de prensa como un baluarte en la defensa de los derechos personales, incluso fue altamente defendida por los jurados norteamericanos frente a las persecuciones que hubo por parte de la corona respecto de, bueno, la sublevación y sobre todo la falta de pago de impuestos en ese momento. Eso daba origen a la Declaración de Virginia, da origen, por supuesto, a las enmiendas de la constitución americana.

Y llegamos a 1890, aparece el periodismo amarillo. Ya el periodismo no se dedica sólo a atacar al Gobierno o a cuestionar al Gobierno, sino que se mete en la vida privada de las personas.

El periodismo amarillo, que se llamó así porque *yellow* en inglés no significa sólo amarillo sino también cruel y cobarde. Por eso es que nosotros lo conocemos de esa manera.

Y aparece el primer antecedente importante del derecho a la privacidad, ahí tenemos a Warren y a Brandeis, Brandeis fue un gran exponente, no solamente de protección de la intimidad, sino también de acceso a la información pública. Ahí algunas frases que vamos a pasar.

Pero básicamente fíjense en lo importante, que el individuo debe tener una protección completa en su persona y en su propiedad, es un viejo principio, pero de tiempo en tiempo ha sido necesario redefinir y actualizar la exacta naturaleza y extensión de la protección. Es lo que hacemos permanentemente en protección de datos.

Cuando hablamos de los derechos estamos actualizando permanentemente esa protección.

Los cambios políticos exigen ese crecimiento y ahí se refería básicamente a estos avances que había en materia de prensa, los grandes avances tecnológicos, el telégrafo, el teléfono, obviamente la fotografía instantánea.

Fíjense que en ese momento en juez Culli, toma la idea del juez Culli del derecho a ser dejados solos, que es el nacimiento del derecho a la protección de datos, el nacimiento del derecho a la privacidad, el nacimiento del derecho al olvido que tanto estamos hablando.

El mismo mil ocho, 90 (sic), aparecen los tratamientos automatizados de información personal, las tarjetas hollerith, que de alguna manera ya ven ustedes, primero la tarjeta perforadora que establece los campos y después a través de un criterio de búsqueda, esa máquina que está a la derecha empieza a seleccionar, como hace hoy un buscaron en internet, empieza a seleccionar el criterio que queremos. Eso fue muy útil en censos y elecciones en Estados Unidos, pero luego va dar origen a lo que vamos a ver después.

Y aquí aparece el primer antecedente constitucional de derecho a acceso a la información personal en la Convención de Weimar en

1919, el funcionario, fíjense en el último párrafo, el artículo 129. “Tendrá derecho de examinar su expediente personal”. Es el derecho de acceso a la información personal. ¿Para qué? Para controlar esa información personal.

Vienen los regímenes autoritarios europeos, obviamente etapa negra de la humanidad, y aparecen las tarjetas Hollerith de nuevo en el censo alemán de 1933, que va a dar origen a la desaparición de millones de personas al holocausto que ya conocemos y que no merece más explicación.

Siguen usando esta tarjeta en censo y elecciones entre 1930 y 1940 en Estados Unidos y también va a dar origen a un problema, que fue el de la orden ejecutiva que fue dictada en 1942, 1943, que finalmente da origen a la relocalización de los individuos con ascendencia japonesa lejos de la costa oeste de Estados Unidos.

Está la Relocation Center, que en esa decisión aquí la seguridad nacional es el otro componente que siempre va a aparecer. Fue convalidada en Kurimatsu, versus Estados Unidos, por la Corte Norteamericana.

Aparecen las computadoras, en 1945 la primera computadora. Fíjense qué antigüedad, todas con clavijas, nada que ver con las actuales, pero en ese momento ya se preveía que la técnica iba a estar al servicio de los estados y obviamente no se pensaba que iba a estar en poder de los particulares.

En el contexto de este autoritarismo aparece la creación de algunas agencias, incluso de investigación, y específicamente aparece el Gran Hermano de Orwell 1948, que va a predecir o de alguna manera va a hacer esta suerte de exorcismo literario tratando de advertir a la humanidad respecto de lo que podía pasar en cuanto a la técnica en poder de un estado autoritario de los que gobernaban en ese entonces.

Lo que vemos en la imagen de en medio es una telepantalla que era capaz de emitir y recibir pensamientos, lo mismo que ocurre hoy con las Smart TV. Por supuesto que no recibe nuestro pensamiento, pero ya hubo un antecedente en Corea en 2013 donde se reconoció que se

había espiado a un ciudadano del Reino Unido a través de su Smart TV por los criterios de navegación.

En 1957 aparece la carrera espacial, Rusia gana esa carrera espacial.

Estados Unidos, a través de la directiva de Eisenhower, de 1958, crea la Advanced Research Projects Agency, que va a dar lugar a ARPANET. Y ahí ya entramos con internet, con la primera, aquella primitiva internet, que no se llamaba así, que empieza con esas cuatro universidades y que se extiende luego a Estados Unidos.

Y ahí aparece, bueno, un homenaje a Ray Tomlinson que murió este año, el e-mail, en 1971, y en 1978 aparece el Spam. Esto es, ya existía en aquella configuración de aquella primitiva ARPANET.

Y aparecen las primeras normas de protección de datos, tanto en Estados, la privacidad; como en Europa, las leyes y constituciones europeas, Alemania, 1970; 1977, la Ley General. Bueno, obviamente las normativas comunitarias de la OCDE, el Convenio 108.

Estas primeras normativas eran por supuesto pioneras, pero no tienen mucho que ver con la configuración actual.

Nace el internet de 1982 a 1983 y ahí empieza a cambiar el mundo, ahí empiezan a cambiar las amenazas.

Aparece el derecho a la autodeterminación informativa por el Tribunal Constitucional en Alemania en 1983, cuestionando una Ley de Censo de Población, por esas informaciones que separadas no decían nada, no eran invasivas, conjugadas sí lo podían hacer y por eso lo declara y lo reconoce desde el principio de dignidad humana.

Esto es muy importante, porque el principio de dignidad humana es el que nos va a dar la llave para construir muchos de los derechos que están en construcción hoy en materia de protección de datos.

Las computadoras personales en 1984. Y aquí viene una cuestión, Orwell había predicho otra cosa distinta, entonces empezamos a aparecer los particulares, ya no es el Estado el que empieza a generar información, sino los particulares.

El hombre se evoluciona hasta meterse en la computadora, su vida empieza a pasar por una computadora y aparece un señor, Maslow, que creo una pirámide en 1943, la pirámide de las necesidades, donde al revés que en la Pirámide de Kelsen lo más importante está abajo, las necesidades fisiológicas, pero ya en este año que veníamos diciendo, 1984, empieza a aparecer la necesidad más básica, que empieza a ser internet.

Luego de esto, sí, está reconfigurada esta pirámide, aparecen otras generaciones de protección de datos: la directiva, de 1995 a 1946; empiezan las autoridades de protección a tener una mayor preponderancia, el supervisor de datos europeos y muchas directivas. No hay tiempo para el marco de privacidad de APEC, simplemente hacer un repaso de aquellas.

Y aparece otra estrella en el firmamento, el derecho a la protección de datos personales como un derecho autónomo.

En la carta obviamente de derechos fundamentales de la Unión Europea, que recientemente en 2009 entiendo que entró a regir; en 2000 fue aprobada.

Y de hecho esto ya lo cataloga como un derecho fundamental, y al ser un derecho fundamental medial es muy importante, porque a través de él se puede proteger cualquier derecho, no hay derecho que quede exento de la protección cuando protegemos un dato.

Hay muchos ejemplos de jurisprudencia, voy a mencionar sólo uno de mí país, que es el caso Urteaga, donde un hermano de un desaparecido pidió información y la corte, se le había negado, le reconoció el derecho pese a que no se trataba de un dato relativo a él. Pero sí dijo: Aquí está implicada la intimidad personal, la dignidad de esta persona, el derecho al duelo, el derecho a enterrar a los muertos, derechos que no podríamos ni imaginar que son alcanzables por el derecho a la protección de datos y están ahí.

En el 2001 empieza la otra interferencia, los ataques, la seguridad nacional, los ataques de la Ley patriótica, y acá empieza otro de los

problemas de la aplicación de la Ley o de las normas de protección de datos.

Aparecen obviamente estas personas que empiezan a hacernos conocer estas realidades ocultas, y se convierte la web 1.0 en la 2.0. Aquí ya empieza la participación de todos nosotros en la web, empezamos a cargar información, y creo que es el problema más grave que tenemos hoy.

El problema de la falta de conciencia de mucha gente cuando carga información personal, la web se hace más participativa y aparecen los Smartphone.

Y ahí ya el hombre que estaba sentado en la computadora empieza a tener el internet consigo todo el tiempo, y acá tenemos lo que nos pasa cuando perdemos el celular.

Alguien lo decía, en algunas de las previas, de las posiciones previas perdemos esto y perdemos la vida, ¿Hay algo más íntimo que el celular? Creo que no.

¿Cuántos pasaríamos el examen si este celular fuera conocido por todo el mundo? No lo sé.

Y entonces se reconfigura la pirámide y demás, ya no es internet sino Wi-Fi, necesitamos internet inalámbrico. Y con esto empieza a reconfigurarse toda la geografía, porque el hombre a través que necesita Wi-Fi también necesita batería.

El otro problema que tenemos es que ya por debajo de Wi-Fi, por debajo de internet está la necesidad de batería. Todos llevamos dos, tres, cuatro baterías porque necesitamos eso primordialmente, sin eso no hay nada.

Y el problema con internet e internet 2.0, es que esta participación tanto de la prensa como de nosotros requiere que tengamos más responsabilidades.

Y aquí tenemos una noticia de hace no mucho tiempo, donde Mónica Lewinsky pedía que internet fuera más compasivo. Y de hecho el caso

Costeja en definitiva termina pidiendo más compasividad por parte de internet.

Luego seguiremos o seguimos en internet 3.0, un internet más responsable, y empiezan los problemas, Big Data, Data Cloud, internet de las cosas, internet de todas las cosas. Ya en 2020 se cree que cualquier objeto que conecten a internet va ser completamente obsoleto.

Podemos mencionar millones de aplicaciones y de nuevos artefactos que están conectados a internet y que suben permanentemente información personal. Muchos de esos relacionados con nuestra salud.

Nosotros utilizamos muchos implementos en donde estamos subiendo datos de salud y cualquiera lo puede tener.

Las ciudades se van modificando y aparecen las ciudades inteligentes, y ahí hay tres ejemplos: A la izquierda puse en la antigüedad, obviamente, a Machu Picchu, a la derecha Monte Albán por un honor a Perú y a México, y en el medio a Deming, New Mexico. Es una ciudad inteligente que está en este momento en ejecución, donde debajo de esa ciudad están todos los laboratorios donde se está estudiando cómo configurar nuevas ciudades a través de las tecnologías.

Por supuesto entramos en las normas de la cuarta generación, resolución de Madrid, el convenio de Europa de acceso a documentos públicos, el reglamento especialmente nuevo de protección de datos, sobre el cual me voy a referir a algo.

Por supuesto la OEA dicta su principio de protección de privacidad y datos personales. En este caso tomó un criterio diferente, sobre acceso a la información pública dictó una Ley modelo, pero aquí para acercarse más al modelo americano opta por una declaración de principios.

Bueno, el Reglamento no lo vamos a tratar, pero lo importante es que básicamente hay unas nuevas perspectivas que nos van a poner de frente a lo que va a venir después, que es la evolución posterior a 4.0.

Con eso termino la presentación y ahora les voy a hablar, para cerrar, de algunas cuestiones que se pidieron específicamente.

En este contexto el derecho a la protección de datos requiere del máximo de esfuerzo y ese esfuerzo no puede ser sólo de la Auditoría de la Protección de Datos, es responsabilidad de todos; y también responsabilidad del Poder Judicial.

Ya que hablamos, me toca a mí estar en este momento en el Poder Judicial hace unos años.

El Poder Judicial en América Latina ha tenido un buen desempeño que ha reemplazado en muchos casos a agencias de protección que no han tenido capacidad o creativa.

Y de hecho hay una figura que es el habeas data, que funciona muy bien en Argentina, funciona muy bien en Uruguay y varias constituciones; el 50 por ciento de las constituciones latinoamericanas la han incorporado. Esa figura es muy eficiente, ayuda mucho porque el juez inmediatamente toma medida de protección que puede incluir el bloqueo de los datos.

Por supuesto, en este balance el derecho a la información es crucial la función, por supuesto de verificación y sanción, que es el tema de este panel, el problema es para llevarlas a cabo, el problema de la globalización. Ya hemos visto un poco de esto, la idea era plantearlo de una manera gráfica.

¿Cómo hacemos para superar la fragmentación de normas? Y en esto el Reglamento yo creo está atendiendo acercarse al modelo norteamericano, es un esfuerzo que ya venía haciéndose previamente con la Resolución de Madrid, que básicamente trata de acercarse al otro modelo.

Esto fue destacado en la Cumbre del G8 de 2011, obviamente estaba en el proyecto de Obama de 2012, de la Consumer Privacy Act; y, de hecho, está tratado en el Convenio del Protocolo 108 sobre autoridades de protección y transferencias internacionales.

El gran problema de acá es cómo se llega a también infracciones que no están dentro del contexto del país donde vivimos o donde está la persona afectada.

Y en esto también el Reglamento Europeo hace hincapié en el sistema de ventanilla única, en el sistema de coordinación que ya viene haciendo a partir de esa coordinación con el supervisor europeo las distintas agencias de los distintos países.

Por supuesto todo esto trae algunas dificultades que tienen que ser superadas.

Desde luego también el problema que se marcó antes por mi compañero español, que es el tema de que las autoridades de control han sido, lo conversábamos con José Luis Pineda también, cómo quedan superadas las agencias por la cantidad de reclamos.

Y aquí éste es uno de los grandes desafíos, cómo hacer para que esto pueda mejorar.

Algunos plantean esto que se mencionó antes del *diselectic to be affecting*, pero si estamos en el marco de un derecho fundamental, la protección de datos, como lo menciona Antonio Raigada, es muy difícil poder aplicar este principio, hay que atender a todas las reclamaciones.

Desde luego esta selección podría aplicarse de una manera, dando prioridades a los temas más importantes, pero sin dejar de atender a cada uno de esos reclamos.

Para terminar, porque ya me han avisado que terminó mi tiempo, acá tendríamos que ir, como tantas veces se ha dicho, hacia una regulación internacional, pero para que esa regulación internacional global pueda tener efectividad, obviamente que se requieren sociedades democráticas que estén en capacidad de aplicar estos principios, porque mientras no estemos en un mundo globalizado que tenga sociedad democrática, va a ser muy difícil que esto pueda llegar a buen puerto.

Termino simplemente con esto, le agradezco la atención y quedo a las preguntas que puedan tener.

Muchas gracias.

Moderador: Agradecemos de antemano su excelente participación, del doctor Oscar Raúl Puccinelli.

Es actualmente el presidente del Centro Nacional de Administración Cibernética en el Reino Unido y es fundador del Fondo Cibernético, una beneficencia que ayuda a las víctimas del cibercrimen.

Es profesor de gestión de la ciberseguridad y de estudios sobre políticas en diferentes universidades del Reino Unido, y trabaja como asesor para gobiernos y bancos centrales, así como para agencias de procuración de justicia.

Con ustedes Richard Benham, del Reino Unido.

Sr. Richard Benham (Interpretación del inglés al español): Buenos días.

Esto va ser en inglés, así que para cambiar un poco; solamente para hacerlo un poco más interesante.

Muy bien. Tengo algunos mensajes que quiero pasarles, antes de ir a mi presentación directamente.

Primero que nada, me gustaría agradecerles por invitarme a su tan maravilloso país aquí, en México. Verdaderamente han sido muy hospitalarios y verdaderamente he disfrutado mi estadía aquí.

Muchas gracias por ello.

También tengo un mensaje por parte de la Secretaría para las Cibers Seguridad del Reino Unido y de nuestro Jefe de Policía.

Cuando les dije que iba venir a hablar aquí con ustedes, ellos me pidieron que les mandara sus mejores deseos a todos ustedes, en

nombre del Reino Unido. Ese fue un mensaje de apoyo para ustedes, de parte de ellos.

Ciertamente, creo en la colaboración y en la necesidad de platicar, para poder contrarrestar algunos de los problemas que tenemos con estas tecnologías digitales emergentes que tenemos.

Mi presentación va ser un poco diferente a las previas, aunque algunos de los mensajes claves van a ser iguales.

Tengo antecedentes y voy a explicarles rápidamente de dónde vengo.

Yo, como tal, no me involucro con datos; tengo antecedentes que incluyen de manera efectiva los datos.

De hecho, estaba en lo que era la Banca y en aseguradoras, y cuando empecé en la industria bancaria no era como tal digital, era por papel, se basaba en documentos, todo se hacía de manera manual; los procesos eran lentos y era mucho más seguro, en ciertos sentidos.

Lo que he notado, por lo menos en mi corta carrera, es que la Banca como tal, como industria, ha cambiado y ha cambiado de ser de papel y de proceso a hacerse más digital, y algunos de los beneficios de este cambio han sido inmensos, pero también ha traído a la par muchos retos.

La razón por la que acabo de mencionarles mis antecedentes ese porque pasé 11 años en la aplicación de la Ley. De manera que tuve un comienzo de mi carrera muy interesante: Yo pensaba que iba ser gerente de Banco, que iba hacer mucho dinero en el Banco, pero luego me volví, en cierta forma, un policía, por falta de una mejor palabra para describir mi puesto y me involucré en diferentes cuestiones.

Era responsable en el Reino Unido para introducir una advertencia europea de arresto y también un centro de protección en línea y hubo unas cuestiones muy interesantes que surgieron, a medida que trabajé en la agencia policiaca.

Esto a la parte me ha dado una visión del mundo en el que vivimos, no solamente desde el punto de vista digital, sino también los elementos humanos y el cómo nos afecta a todos como seres humanos.

Desde este punto me he especializado, en cierta forma, en esta área: En el cómo este mundo digital nos afecta no solamente como individuos, sino como negocios.

Solamente quería hablar con ustedes algunas de las cosas que he descubierto a lo largo de algunos años y algunas de las maneras interesantes en las cuales creo que podemos hacernos más seguros.

Así que regresemos a esa palabra “ciber”, cibernético, porque soy un profesor en cuanto al manejo de la ciber seguridad y la pregunta que siempre se me hace es: ¿Qué significa la palabra “ciber”?

Siempre trato de describir, veo que la mejor manera de describirlo es describiéndolo regresando un poco a una palabra que ya lleva mucho tiempo disponible, que es la cibernética, y es ciertamente cuando el hombre se une con la máquina.

A mis estudiantes les gusta esta definición, porque todos han visto la televisión, han visto las películas de “Terminator” y entendemos que es aquí cuando la ciencia se vuelve interesante, cuando el humano empieza a interactuar con la tecnología.

Pero para mí es, de hecho, mi preocupación principal, porque es aquí donde se presentan los problemas.

Siempre que hago una investigación y, sí, ciertamente hago muchas investigaciones para muchas organizaciones muy grandes, así como gobiernos, encontramos que los problemas se presentan más cuando los humanos se involucran.

La tecnología por lo general se resuelve a sí misma, pero siempre hay alguna parte humana involucrada en los problemas.

Es por eso que la palabra “cibernética”, esta palabra que tiene que ver con que le hombre se encuentra con la máquina, por eso es tan importante.

Hace algunos años dije: “Bueno, voy a escribir una teoría, porque me moví al área académica y todo profesor nuevo tiene que tener una teoría”.

En aquel momento escribí mi teoría y pensaba que era muy obvia: “Si tienes un ciberataque va afectar tus procesos a la sociedad, se va diseminar”.

Y lo que me di cuenta es que la ciberseguridad, hace cinco o seis años, era más que nada una ciencia técnica o de tecnologías de la información, y desde aquel momento se ha vuelto más una ciencia humana.

Una de las cosas que he subrayado o que subrayé en aquel momento es que a medida que este efecto empieza a diseminarse de cualquier acto criminal, hay que manejar muy bien este efecto ondulante, pero no solamente desde el punto tecnológico sino de procesos y de las personas, y una vez que lo entiendes puedes evitar que se vuelva a dar y esto es algo muy importante.

Una de las cosas que he descubierto en muchas de las compañías con las que he trabajado y ayudado, es que no hacemos las cosas de manera apropiada, queremos ahorrarnos pasos.

Y la necesidad de tener un buen proceso, todas estas cosas que se han discutido en los últimos dos días son vitales.

Ciertamente estoy muy consciente del tiempo que tenemos, yo les recomendaría que pusieran tantos criterios y seguridad como sea posible, ciertamente en el Reino Unido estamos tratando de hacerlo, GDPR va hacer algo muy importante para nosotros. Esto lo voy a manejar en un minuto, muy rápidamente se los comentaré.

Ustedes saben que hay un robot que siempre sale en la pantalla, ¿cuáles son mis retos más grandes? Bueno, qué pasa cuando nos involucramos con escuelas, con negocios y con gobiernos, que hay que asegurarnos que la ciberseguridad sea también emocionante, porque tan pronto mencionas el tema las personas como que se aburren, dicen: “Ay, sí”, pero no te escuchan.

Y en particular con los niños. Una de las preguntas que me hacen, ¿tienen ustedes hijos? Si tienen hijos saben a qué me refiero. Muy bien, tengo dos adolescentes yo, adolescentes, y no me escuchan, incluso a pesar de que los haya entrado, tienen su propio curso en casa, del que soy encargado, pero no escuchan, ¿por qué? porque todo lo sacan del teléfono y siguen usando el teléfono, pero dejan de pensar.

Y una de las buenas preguntas, y aun así discuto mucho con mis hijos, incluso el día de hoy les digo que la nube no es como tal, los datos no están ahí en el cielo y discuten conmigo, me dicen: “Sí está”. Porque es todo lo que ellos conocen.

Y existe una gran cantidad de educación que necesita hacerse, no solamente con los niños, sino con los adultos, y en particular las personas encargadas de compañías, en la cual tienen que entender, de una bonita manera, qué significa esta nube. Y este es uno de mis retos.

Este robot de aquí lo introducimos como una especie de manera de captar el interés de las personas y parece que funciona, y funciona ahora tan bien que ahora las personas me mandan fotografías de este robot, ¿por qué? porque, disculpen, así lo dejamos con los negocios, así que ya hemos hecho versiones, incluso a gran escala de este robot para que se queden con él y se los recuerde.

Se toman fotografías a lo largo del día y a lo largo de la noche de esta ciberpersona o este robot en diferentes personas. Entonces, lo tienen en diferentes eventos y me mandan las personas con el robot.

Hemos desarrollado; de hecho, ya una competencia nacional, que nos ha ayudado a diseminar la necesidad que tenemos de que las personas tengan un mejor conocimiento digital, y ha funcionado.

Uno de los sectores que más me apasionan, y ustedes probablemente ya lo vieron en mi introducción, hice una caridad, una organización caritativa en el Reino Unido, porque nos preocupaba que la mayoría de las personas, a pesar que tienen cierta concientización o algo de inteligencia en el teléfono, hay otras partes de la sociedad que no, por

ejemplo, tenemos a personas mayores, personas con discapacidad y también tenemos grupos de personas que han sido víctimas de crímenes cibernéticos.

De manera que nosotros hicimos una organización caritativa para lidiar con estos problemas. Yo creo que en cualquier sociedad necesita haber alguna manera para que esas personas que no tienen acceso a las buenas prácticas lo tengan. Esto no se trata como tal de las compañías, se trata de cuidar su población también. Ciertamente trato de alentar a todos porque así lo hagan.

Entonces ¿por qué importa toda esta ciberseguridad?

Muy bien, yo también cumplo otro trabajo –por cierto, tengo muchos trabajos– pero también tengo una infraestructura crítica nacional, yo vivo en un centro en Inglaterra muy conocido, una de las tareas de mi centro es la de defender la nación contra ataques de otras naciones o estados. Y lo que hemos visto es que cada vez más las naciones tratan de atacar a otras mediante cibercrímenes.

Hemos visto que en el Medio Oriente tenemos una especie de guerra cibernética que se ha dado entre las naciones y creo que hay muchas cosas en el futuro en esta área.

Es una manera fácil de destruir una nación y es por eso que importa tanto.

Pero regresando al tema en cuestión, para los negocios y las organizaciones también hemos encontrado en el Reino Unido que muchas personas se están robando nuestro diseño, nuestra propiedad intelectual y esta manera cibernética es una manera muy fácil de tener una ganancia competitiva, entonces a veces no se trata de destruir, sino de robar ideas y replicarlas. Así que verdaderamente importa, en términos de poder, proteger la economía.

Y verdaderamente, de nuevo regresando al tema, cuando trabajo con negocios pequeños y medianos muchas de nuestras víctimas sufren por facturas falsas.

El número de facturas, incluso a mi negocio las que entran, tenemos al menos una factura falsa que llega al día, alguien trata de robarnos dinero utilizando nuestras debilidades.

Y de nuevo, me gustaría ver mejores regulaciones en este campo, tenemos que hacer que la profesión sea más confiable y que se tenga este tipo de protección digital y creo que el GDPR va a ser el punto focal para nosotros en el Reino Unido, para cambiar la manera en que nos conducimos.

Así que, primero, importa mucho en negocios, también importa mucho como nación y también importa a nivel individual también. Todos ustedes tienen teléfonos móviles, los puedo ver aquí, y todos somos muy dependientes.

Muchos de los conferencistas esta semana han hablado acerca del hecho de que tenemos teléfonos móviles, tenemos más información que está más cercana a nosotros, más cercano nuestro celular que nuestra pareja.

En el Reino Unido tenemos 54 por ciento, esto representa que la mitad de todos los crímenes reportados fueron relacionados a una cuestión cibernética.

Ahora, cuando decimos cibernética, puede ser incluso fraudes, y nos está presentando un verdadero problema en el Reino Unido.

Para ponerlo simple, debido a que no tenemos oficinas de policía y no tenemos a las personas que se han capaces para lidiar con estos temas cibernéticos, pensamos que la manera para enfrentarlos a futuro es aumentar las multas, el hacer que más personas sean arrestadas y también el hacer que sean más responsables las organizaciones que permitieron que sucediera.

Son fáciles las palabras para decirlo, pero el costo de tener una investigación para un solo ciberataque para un individuo es muy costoso en relación, por ejemplo, a la cantidad que robaron.

De manera que la policía está tratando de sofisticarse y encontrar otras maneras para poder rastrear a los cibercriminales en el mundo.

Es por eso que la colaboración internacional es tan importante para poder encontrar a estas bandas y destruirlas, y verdaderamente es la colaboración la que es la clave.

Solía trabajar para EUROPOL, que obviamente se encarga del territorio europeo, y tiene una muy buena colaboración en términos de poder compartir la inteligencia.

El sistema de la banca no está tan dispuesto a compartir información y una de las mayores barreras que tenemos en el momento es que las personas no quieren ser posibles víctimas de un crimen o de fraude, y creo que con el tiempo se va a forzar a muchas personas que liberen la información, pero creo que a largo plazo esa es la manera como debemos de conducirnos.

Y otra cosa que hemos aprendido en el Reino Unido, y ésta es verdaderamente la elección a aprender, es que no podemos tener una policía para todos, la solución no va a ser simplemente seguir haciendo leyes, seguir yendo tras los criminales y seguir castigándolos, no, tenemos que también ocuparnos de la protección, la prevención para la sociedad.

En otras palabras, estamos tratando de crear un ambiente en los cuales los ciudadanos tengan mayor conciencia, queremos educar a los ciudadanos desde abajo hacia arriba.

La palabra de autoprotección es muy clave aquí, porque no cuesta mucho si se hace de la manera correcta, así que quiero mencionarles rápidamente: Nosotros tuvimos un ataque muy grande en el Reino Unido hace dos semanas con el Banco Tesco.

Para los que no lo saben, es un súper mercado que tiene una filial, una bancaria, y la razón por la que causó problemas es que probablemente fue un trabajo hecho desde dentro, como así le llaman, utilizaron la vulnerabilidad humana para poder entrar al bando y extraer el dinero y hacer un ataque.

Y aún estamos esperando para hacer el reporta al respecto, porque va cambiar la manera como el sector bancario hace sus regulaciones y

sus leyes, y probablemente fuerce a que nuestro gobierno también cambie sus leyes. Y probablemente me lo voy a salgar, porque ya les hablé de las facturas falsas.

Desde el punto de vista personal, solamente para terminar mi presentación de nuevo, en mi caridad “Organización Caritativa” vemos a muchas víctimas de los crímenes cibernéticos, si es un crimen real y está a la alza.

Y lo que verdaderamente me preocupa es cuando me encuentro a víctimas que han sido abusadas en línea o aquellas a las que les han hecho bullying, en particular a aquellos niños pequeños. Este verdaderamente es un problema.

Y soy un creyente muy apasionado en tener restricción en el acceso de los niños. En términos de privacidad creo que los niños no deberían tener mucha privacidad, hay un equilibrio ahí que se tiene que buscar.

Esto puede ser controvertido, pero yo creo que hay que proteger a los niños por lo menos hasta cierta edad del internet. Esa es mi visión.

Pero aquí el problema más grande que tenemos al momento es el robo de identidad, los cibercriminales no tienen reglas, son muy sofisticados y están detrás de tu identidad porque pueden sacar dinero de eso, ya sea por vender tu identidad o por usarla de manera fraudulenta para entrar a algo a lo que tú tengas acceso y que sea de valor.

Así que en el Reino Unido tenemos tres iniciativas, en el momento nosotros lanzamos un curso para crear concientización en el público, y este actualmente se está llevando a lo largo de todo el Reino Unido, y también trabajos en conjunto con una compañía, CPP, que también tiene oficinas en México, y nosotros tratamos de tener teléfonos móviles que te dé una alerta si alguien lo ha utilizado en la web y poder rastrearlo.

Uno de mis compañeros ya lo había mencionado, nosotros tenemos siete pasos para tener buenas prácticas, y si no hacen nada más en el trabajo o con su familia. Siempre y cuando sigan estos siete pasos van a tener un poco más de seguridad.

Creo que ya se me acabó todo el tiempo.

Muchas gracias.

Moderador: Muchas gracias a Richard Benham por esa manera tan fácil y con un lenguaje muy ciudadano de decirnos todo lo complicado que es la tecnología, y sobre todo en materia de seguridad.

Las conclusiones de este panel, si me lo permiten mis compañeros panelistas, son las siguientes: En este panel se hizo referencia a la importancia de la aplicación de la Ley, considerando que ningún derecho es absoluto, todos tienen límites, y es importante distinguirlos.

Se subrayó la importancia de contar con leyes que sean aplicables, se hizo referencia en el caso español a los pilares de la Agencia Española de Protección de Datos, sus competencias en materia de protección de datos, su facultad de investigación o inspección, de sanción, y la posibilidad de cooperar con otras autoridades internacionales.

Se hizo referencia a las actuaciones preventivas, como las recomendaciones; se habló sobre la potestad sancionatoria de la agencia española, de la protección de datos, describiéndose las actuaciones previas, el procedimiento sancionador que puede concluir con la determinación de una vulneración.

Se describió el procedimiento en administraciones públicas, en el que se imponen medidas correctivas; se refirió al procedimiento de tutela de derechos, a las infracciones, los montos de las sanciones económicas, la figura del apercibimiento, así como de la innovación de ficheros como consecuencia de una infracción muy grave.

Las áreas con mayor importe global de sanciones destacando el sector telecomunicaciones; por último se subrayó la importancia de la cooperación internacional para la aplicación de la ley.

Y en mis notas tengo también incluso hasta con fines recaudatorios la agencia, recaudan muy bien. Mencionabas que 12 millones de euros el año pasado.

Se habló de la importancia que el marco normativo de datos personales esté armonizado con diversas leyes, así la Ley en materia de los datos personales tiene que estar vinculada con la normatividad en materia de acceso a la información, con la finalidad de evitar contradicciones.

Se mencionó el fundamento constitucional del derecho a la protección de datos personales en México, citando el artículo 16 en el que se prevén los derechos de acceso, ratificación, cancelación y oposición.

Se comentó la repercusión de ciertas conductas que pueden derivar en delitos como fraude, asociación delictuosa o robo de entidad, la evolución de la tecnología ha facilitado el acceso a la información, lo cual tiene consecuencias positivas, pero al mismo tiempo puede dar lugar a conductas delictivas, como el robo de identidad y de ahí la importancia del derecho a la protección de los datos personales.

Se habló también que estén garantizados los datos personales de los sujetos obligados, sobre todo lo decía muy acertadamente el magistrado, cuáles datos deben ser protegidos y cuáles no.

Asimismo, se mencionaron los principios de máxima publicidad y la minimización como principios característicos del derecho de acceso a la información y de protección de datos personales.

Consideró la conveniencia de que las instituciones garantes sean colegiadas.

Asimismo, se hizo un repaso del desarrollo cronológico de la privacidad, mencionando la definición que Samuel Warren y Louis Brandeis dieron al término “privacidad” como el derecho a ser dejado solo.

¿Cuál es el cimiento del derecho a la privacidad?

Se hizo referencia a la Constitución de Weimar, las tarjetas Hollerith e IBM en el censo, a la aparición de las computadoras en el año 1945, la aparición del email y el spam, la aparición de la primera normativa de protección de datos, el nacimiento de internet, la sentencia del

Tribunal Constitucional Alemán sobre la Ley de Censo, la aparición de la tercera generación de datos en el año 2000, la aparición de la Carta de los Derechos Fundamentales de la Unión Europea.

Se hizo referencia a las implicaciones del mundo digital en los negocios, destacando la importancia de los procedimientos de la ciberseguridad, se destacó la importancia de que la ciberseguridad sea accesible a todos los sectores de la población, incluyendo a los niños, considerando su cercanía con la tecnología.

Subrayó la importancia de mantener protección digital en diversos documentos para impedir la afectación a los negocios.

Estas serían las conclusiones que ponemos a su consideración, van a estar disponibles en la página web del INAI.

No me resta más que agradecerles a los panelistas sus valiosas intervenciones, colaboraciones y apuntes que compartieron con nosotros.

A Julián Prieto, el licenciado Julián Prieto Hergueta, de España; al doctor David Jiménez González, magistrado de aquí, del Tribunal Mexicano; Oscar Raúl Puccinelli, de Argentina; Richard Benham, del Reino Unido.

Creo que hemos recibido una gran información de cada uno de ellos, cosa que les agradecemos y los dejamos con un fuerte aplauso.

Y, por supuesto, también finalmente, en nombre del INAI y de todos los organismos que hicieron posible este Foro, les agradecemos la presencia a todos ustedes, que gentilmente nos acompañaron esta mañana, a los compañeros del organismo garante de la República Mexicana, que aquí se encuentran también acompañándonos y a todos, a todas las organizaciones que aquí están representadas.

Muchas gracias a todos.

Vamos a proceder a entregar los reconocimientos a los panelistas y unos regalos, unos obsequios que hace el INAI.

Julián Prieto Hergueta.

David José del Carmen Jiménez González, magistrado.

Oscar Puccinelli, catedrático de la Universidad Nacional del Rosario, Argentina.

Richard Benham, del National Cyber Management Centre, Reino Unido.

Con eso terminamos. Muchas gracias a todos.

-----o0o-----