Manzanillo, Col, 1 de diciembre de 2016.

Versión Estenográfica de la Conferencia "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Retos y Alcances", 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: Damos y caballeros, damos paso a la siguiente Conferencia, relativa a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Retos y Alcances.

Cedo el uso de la voz al coordinador de Protección de Datos personales del INAI, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Luis Gustavo Parra Noriega.

Adelante, por favor.

Moderador, Mtro. Luis Gustavo Parra Noriega: Muchas gracias.

Buenas tardes a todos.

Sean bienvenidos a esta Conferencia Magistral, en el marco del Cuadragésimo Sexto Foro de Autoridades de Privacidad Asia-Pacífico.

En esta ocasión tenemos el honor de contar con la presencia del doctor José Luis Piñar Mañas, quien impartirá la Conferencia sobre Los Retos y Alcances de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Gracias, José Luis, por estar aquí.

Sin embargo, antes de cederle la palabra al doctor Piñar, le pediría si me regala un minuto o dos minutos para mencionar que precisamente la importancia –como ya lo comentaba la doctora Ximena Puente el día de ayer– sobre la aprobación del Proyecto de Dictamen de la Ley General de Protección de Datos Personales, ya que con ésta se abrirá

paso a la expedición del primer ordenamiento mexicano que a nivel nacional fija las bases para el ejercicio efectivo y la tutela del Derecho de Protección de Datos Personales en Posesión de Entes Públicos, de los tres órdenes de gobierno y de partidos políticos.

El dictamen prevé, entre otras cosas, los estándares mínimos e imprescindibles que van a permitir homologar, uniformar el derecho a la protección de datos personales en posesión de sujetos obligados del sector público.

También esta Ley distribuye competencias entre el INAI, los órganos garantes estatales, lo cual va permitir la cooperación, la coordinación entre los tres órdenes de gobierno, para precisamente el cumplimiento de los objetivos previstos en la Ley.

Destacaría que por primera vez en la Historia de México se van a definir las bases para elaborar y ejecutar un Programa Nacional de Protección de Datos Personales, como una política pública de la materia.

Lo anterior significa precisamente que cualquier persona esté segura, al menos, de que la Ley exige que sus datos personales sean utilizados y cuidados bajo las mismas reglas, en cualquier parte del país.

Que se solicita también a cualquiera autoridad el acceso, la rectificación, la cancelación y la oposición de sus datos personales, de la misma forma.

Denunciar ante los órganos garantes o el INAI, según corresponda, el uso indebido de sus datos personales.

También confiar en que sus datos personales serán obtenidos mediante el consentimiento; claro que conforme las reglas establecidas en la Ley, con sus excepciones y sus modalidades.

Los mecanismos que existan cuando sea vulnerado o restringido el derecho de protección de datos personales.

Con esta minuta que ayer se aprobó en la Comisión de Transparencia y Anticorrupción de la Cámara de Diputados, pasa ahora su discusión al Pleno.

Por cierto, esta minuta fue aprobada mayoritariamente por 16 votos a favor y cuatro en contra; va pasar al Pleno para su discusión y aprobación.

Esperemos en este mismo periodo ordinario de sesiones, que termina el 15 de diciembre, y esperemos que tengamos esta promulgación muy pronto de la Ley General, que precisamente va sentar las bases para construir un sólido sistema de protección de datos personales en México, orientado a un efecto ejercicio y respeto de este derecho fundamental.

Habiendo dicho lo anterior, José Luis, y disculpa que haya tomado estos breves momentos, quisiera hacer una presentación de la biografía de nuestro conferencista el día de hoy, a quien agradecemos su presencia y como amigo que es de este Instituto, siempre es muy generoso con su presencia aquí, en nuestro país.

Él es Doctor en Derecho por la Universidad Complutense de Madrid; Abogado Consultor Internacional en Materia de Protección de Datos Personales; es catedrático de derecho administrativo de la Universidad CEU, San Pablo, en Madrid, España.

Y es director del master universitario internacional en protección de datos personales, y transparencia y acceso a la información en la misma universidad.

Fue director de la Agencia de Protección de Datos Personales Española, de 2002 a 2007, vicepresidente del Grupo Europeo Autoridades de Protección de Datos, de 2004 a 2007 y presidente fundador de la Red Iberoamericana de Protección de Datos Personales, de 2003 al 2007.

Es poseedor de la Cruz de Honor de San Raimundo de Peñafort, donde las máximas condecoraciones que otorga el Gobierno español a juristas.

Y ha colaborado en la redacción de diversas propuestas normativas, como el reglamento de desarrollo de la Ley Orgánica de Protección de Datos de España, la Ley Española de Transparencia, Acceso a la Información y Buen Gobierno, y el Reglamento de la Ley Federal, aquí en México, de protección de datos.

Es miembro de la Red Académica internacional de protección de datos, miembro de honor de la Asociación de Profesionales de Privacidad en España, y de la IAPP a nivel internacional.

Y, bueno, es, como todos lo sabemos, conferenciante en diversos países, en Europa, en todos los continentes de este planeta y fue profesor adjunto en la Universidad de Georgetown, de 2005 a 2007, y profesor también en diversas universidades de Europa y Latinoamérica.

Cedo la palabra al doctor Piña, y muchas gracias, José Luis.

Sr. José Luis Piñar Mañas: Buenos días a todos, casi buenas tardes.

Ante todo, quería agradecer al INAI y a los organizadores por haberme permitido la ocasión de compartir con todos ustedes unas reflexiones sobre la Ley General de Protección de Datos en este importantísimo Foro de Autoridades de Protección de Datos de Asia-Pacífico.

Quiero agradecer muy especialmente a la presidenta del INAI, la doctora Ximena Puente; al comisionado Francisco Acuña, y al doctor Luis Gustavo Parra, la invitación.

Que debo decir es muy generosa, y que me genera sentirme casi, llevando a cabo una osadía, porque qué hago yo hablando en México sobre la Ley General de Protección de Datos, que ayer mismo se dictaminó, como acaba de decir el doctor Luis Gustavo Parra.

Pero, en fin, voy a intentar en los próximos minutos compartir con ustedes algunas reflexiones, partiendo de la base de que gran parte de lo que voy a exponer, a transmitir lo sabemos, lo saben ustedes, ya se ha dicho de alguna manera en este foro.

Voy a intentar no repetir, voy a intentar aportar algo, pero no va ser fácil porque, como digo, no pocas de las consideraciones que tenía preparadas, que tengo preparadas para compartir con ustedes, ya se han expuesto, pero intentaremos aportar algo nuevo.

Lo que vamos hacer, si me permiten, el cómo voy a sistematizar mi intervención, va ser del siguiente modo: Primero voy hablar de en dónde estamos en materia de protección de datos, qué lugar ocupa la protección de datos, cuál es la relación entre derecho, innovación y ética; haré referencias a la expresión: “La ley también existe”, por lo que luego les comentaré; y luego ya me centraré en la Ley General.

Pero para intentar aportar algo nuevo, lo que he hecho ha sido llevar a cabo un análisis comparativo entre el Reglamento General de Protección de Datos, que se ha aprobado en abril de este año en la Unión Europea, y la Ley General de Protección de datos, para ver o para concluir en el sentido de que seguramente estamos en el camino de un modelo global de protección de datos, en el que los nuevos textos normativos que se están aprobando coinciden en no pocas cosas y, sobre todo, que esto es lo que me interesa resaltar, coinciden en un modelo que quizá será o está empezando a ser el modelo global de protección de datos de carácter personal, algo que es importantísimo, porque como veremos y todos sabemos, cuando hablamos de protección de datos tenemos que dejar aparcadas las fronteras.

Es un derecho que no sabe de fronteras, es un derecho cuyas violaciones no saben de fronteras; es un derecho, además algo muy importante, cuya violación pasa desapercibida, no nos enteramos de cuándo alguien está violando nuestro derecho a la protección de datos y no sabemos tampoco desde dónde está violando nuestro derecho a la protección de datos.

¿Dónde estamos? Esto es algo que ya sabemos, todo lo que hay en esa lámina ya lo sabemos, a algo de ello también ha hecho referencia antes el doctor Puccinelli.

Estamos en una nueva época, en una nueva etapa, los jóvenes mucho más. Nosotros todavía quizá vivimos con internet, ellos viven en internet, internet es su ámbito vital.

Estamos en un momento en que los parámetros en los que el ser humano se ha desenvuelto tradicionalmente, que son tiempo y espacio, están saltando por los aires.

La memoria era algo que nos acompañaba, el círculo vital era algo que nos acompañaba, ahora ni tiempo ni espacio son lo que antes era, porque podemos relacionarnos con personas que están en el otro extremo del mundo y les sentimos más cercano que al vecino que tenemos en la puerta de al lado.

En efecto, en un mundo sin fronteras mucha gente se siente más como perteneciente a una red social, que como perteneciente a un país, se siente más de Facebook que mexicano o español, y se siente mucho más cercano respecto de las personas que comparten con él su círculo en Facebook que con quienes conviven con él en su país.

Fíjense que esto también es muy interesante, porque hay millones de personas que voluntariamente se someten a un marco normativo, que es el que rige, el que establece esa red social, Facebook, y lo hacen voluntariamente antes que a sus propias normas de su país; es decir, una entidad privada ha creado un marco normativo que se aplica a más millones de personas, a un número más elevado de personas, que puede aplicarse cualquier ordenamiento jurídico de cualquier país.

Esto, junto a situaciones como la videovigilancia, redes sociales, las aplicaciones, Big Data, pero también nanotecnologías, los drones, la posibilidad de leer el pensamiento, que ya empieza a ser una realidad, y la física cuántica y la protección de datos.

Con los Qubit ya se puede almacenar muchísima más información de la que uno puede imaginar y se puede hacer muchísimo más rápidamente de lo que uno puede imaginar, y se va a generar un cambio radical en la ciencia y en la técnica que va a afectar a nuestras personas de la mano de la física cuántica.

Están ya, y no es ciencia ficción, están ya empezando a darse los primeros pasos hacia la tele transportación.

Hace unos años no podíamos ni imaginar lo que está ocurriendo ahora en materia de nuevas tecnologías. Utilizo la expresión de nuevas tecnologías siendo consciente de que no es correcta, pero todos sabemos a qué nos referimos.

No tenemos ni idea de qué es lo que va a ocurrir dentro de unos años, pero lo grave es que poco a poco el propio ser humano se está convirtiendo en una base de datos, somos una base de datos andante.

Y les pongo un simple ejemplo, no hace mucho se planteó la posibilidad de que en Barcelona, en una discoteca; estaba yo en la Agencia de Protección de Datos; quizá alguien de ustedes que me conoce ya me ha oído exponer esta anécdota o esta circunstancia, una, como digo, discoteca en Barcelona ideó el que los clientes VIPs pudiesen contar con un dispositivo subcutáneo, implantado subcutáneamente, una especie de telepeaje para que pudiesen entrar en discotecas sin guardar fila, y además también podían consumir sin tener que pagar.

Tan solo había un lector a distancia que captaba cuando entraba, salía el cliente y qué es lo que consumía, como el telepeaje en algunas vías de comunicación. Eso es ético del conocimiento.

El garante italiano prohibió esa circunstancia, pese que contaba con el consentimiento del afectado.

¿Por qué? ¿Por qué decía que eso convertía a los clientes en una base de datos? Y eso iba contra la dignidad de la persona.

También antes había señalado la importancia que tiene la protección de datos en relación con la dignidad de la persona. No se puede cosificar a las personas.

Y con estos avances empezamos a cosificar a las personas, no ya con el internet de las cosas, que también sino con estos distintivos ya saben que empieza a hablarse de los smartphones, de los móviles que tenemos implantados en la piel.

Vamos a ir con nuestro smartmovil implantado en la piel, y nuestra piel va ser el producto que va llevar a cabo el tratamiento de la

información, la propia piel. Esto convierte, como digo, al ser humano en una mera base de datos, y esto pone en riesgo su dignidad, y esto es algo con lo que el legislador no puede estar de acuerdo.

Y es algo que exige contar con leyes de protección de datos, leyes de protección de datos que no tienen nada fácil, porque se mueve el mundo con una serie de retos que tiene que afrontar.

La protección de datos y la permanencia no es una contradicción ni un reto, no son derechos contrapuestos. Más bien de lo contrario, son complementarios, pero tienen que convivir.

Protección de datos y seguridad nacional, protección de datos y mercado, los intereses de las multinacionales en cuanto al tratamiento de la información en un mundo global. Se ha dicho que la información lo es y mucho más.

Y sería muy interesante exponer, ya lo ha hecho también el doctor Puccinelli, la evolución jurídica de la protección de datos, ¿por qué estamos donde estamos y qué evolución se ha producido para llegar a donde estamos?

Y una de las fases de la evolución de la protección de datos es sin duda alguna aquella que considera al dato personal como una simple mercancía, como una mercancía que se maneja, que se compra, que se vende en un mundo global, y que es muy importante para el mercado.

Y por supuesto el gran reto de la protección de datos es el de la privacidad en un mundo global. La privacidad en un mundo que no conoce de fronteras, en un mundo en el que las leyes continúan siendo leyes territoriales acostumbradas a aplicarse a un determinado territorio.

Los juristas estamos habituados a ello, queremos saber dónde se aplica una ley, a quién se aplica una ley, y esto se compadece mal con la realidad de la protección de datos y con la realidad del tratamiento de la información en el mundo actual.

Donde a veces la ficción va más allá o, mejor dicho, se queda corta en relación con la realidad. Fíjense en este relato, este trozo, este texto, es de un año en una obra de arte, el comic V de Vendetta, está la película, no sé si han tenido ocasión de leerlo, merece la pena. Es, en mi opinión, una verdadera obra de arte.

¿Y saben ustedes de qué va? De un gran control por parte de un poder dictatorial que se ubica en un Londres de finales del siglo XX, y en un momento determinado se comete un atentado, y el poder público, el gobierno quiere distraer la atención de sus ciudadanos para que no estén atentos a ese atentado que se ha cometido.

Entonces lo que hace el gobierno, el poder dictatorial es esto: Para conmemorar la más violenta de las noches, el gobierno de su majestad se complace en devolverles a ustedes, sus leales súbditos, el derecho a la privacidad.

Durante tres días, sólo tres días sus movimientos no serán vigilados, sus conversaciones no serán escuchadas, y el “haz lo que quieras” será la única ley. Buenas noches y que Dios les bendiga.

Esto es ciencia ficción, pero esto puede darse en la realidad. El que todos estamos vigilados es algo real.

No estoy desvelando ningún secreto ni estoy diciendo nada nuevo, pero esto ya se había planteado.

Qué relación también debe darse no sólo entre el derecho y la protección de datos, entre las normas jurídicas y a través de la partida, sino también entre la ética; entre la ética y el avance tecnológico, entre el derecho y la innovación.

Porque también tenemos que ser conscientes, no podemos poner puertas al campo. El derecho no puede pretender parar los avances de la técnica, porque la técnica o la innovación si no se desarrolla en un país porque hay obstáculos jurídicos, se va a ir a otro donde no los haya.

Esto está ocurriendo ya con la investigación biomédica, allá donde hay problemas con el uso de células madre el investigador se va a otro

país donde no lo haya. Y qué más da llevar a cabo la investigación en un país que en otro, siempre que haya medios.

El derecho no puede poner puertas al campo, pero el derecho tampoco puede renunciar a fijar una serie de principios, de criterios, de reglas éticas.

Esto es lo que estamos intentando hacer en la cátedra Google, constituida en la Universidad, en mi Universidad San Pablo CEU, sobre privacidad, sociedad e innovación. Ese es el gran reto, el saber cómo debe relacionarse el derecho, la innovación, en la sociedad, que no es nada fácil.

En este sentido tenemos que tener muy en cuenta que la Ley también existe.

¿Por qué les pongo esta imagen? Fíjense, hace unos meses tuve ocasión de participar en el Campus Party en Guadalajara, acá, en Jalisco; saben que el Campus Party es un encuentro de miles de jóvenes que duermen allá, que están allá, todos genios, además es verdad que inventan cosas, drones, nuevas aplicaciones, nuevos sistemas, también la impresión tridimensional y están no encerrados, pero sí reunidos dos, tres días.

Y me pidieron los organizadores que diez una charla sobre protección de datos y digo “qué hago yo hablando de protección de datos a unos jóvenes a los que esto sinceramente ni les va ni les viene”, pero literalmente ni les va ni les viene lo de la privacidad, están ahí a lo suyo, a los drones, a la impresión tridimensional, a las nuevas aplicaciones y no les entra en la cabeza lo de la Ley de Protección de Datos.

Entonces utilicé este recurso, digo “no, les voy a decir que la Ley también existe, aunque sea recurriendo a Serrat y a Mario Benedetti”.

Pero sí que les dije una cosa y ahí sí que quizá salieron más impactados, dije: “Imaginen ustedes que este encuentro, el Campus Party, en lugar de ser un encuentro de genios de la informática y de la innovación tecnológica, lo es de diseñadores de vehículos, de carros,

de coches” y que alguien les dijese “tengo que ver una conferencia para hablarles de la seguridad”.

Y les tengo que recordar, ayer también decía algo el doctor Cannataci, les tengo que recordar que si ustedes van a diseñar un vehículo tienen que poner el cinturón de seguridad, tienen que poner el reposacabezas, el air bag; todos me dirían “pero usted cree que somos tontos o qué, ya sabemos que tenemos que hacer eso, por supuesto que sabemos que tenemos que implantar esas medidas de seguridad en el vehículo. No venga a recordárnoslos como si fuésemos tontos”.

Bueno, algo así tendríamos que conseguir con la protección de datos, que nos dijesen “no vengan ustedes a recordarme que tengo que tener en cuenta la protección de datos cuando diseño una aplicación, cuando diseño una red social, cuando diseño un programa o cuando diseño cualquier producto que tenga que ver con el tratamiento de datos de carácter personal” y, sin embargo, hay que recordarlo, hay que recordar una y otra vez que la Ley también existe en materia de protección de datos.

Es una Ley además transversal, que afecta a todo y a todos.

Fíjense, cuando dejé la Agencia de Protección en el año 2007, en España tenemos un régimen de incompatibilidades muy riguroso, durante dos años después de dejar un cargo público nadie que haya ocupado ese cargo público puede dedicarse a ninguna actividad que tenga que ver directa o indirectamente con aquella que era objeto de su desempeño público.

Cuando yo volví a mi universidad o quise volver a mi universidad, a la San Pablo CEU, la llamada Oficina de Conflicto de Intereses me dijo “oiga, usted no puede volver a la universidad”. Le pregunté: “¿Por qué no?”, me dijo: “Porque en la Universidad hemos visto que tiene escritos en la Agencia de Protección de Datos”.

Les dije: “Claro que sí”; luego, ha tenido relación con la agencia “por supuesto que sí”. Me dijeron: “Pero es que no podría ir a ningún sitio, porque todas las empresas, todas las entidades públicas, privadas tienen que cumplir con la Ley de Protección Datos, todas”.

No es que ya está trabajando en el Sector Financiero, en el Banco de España o en el Sector Seguros, que tiene un ámbito más reducido; es que la protección de datos abarcar a todos, con lo cual me he encontrado en la tesitura de no poder trabajar en ningún sitio durante dos años.

Menos mal que me lo resolvieron y cayeron en la cuenta de que eso era absurdo y pude regresar a mi Universidad.

Es una Ley transversal. Fíjense, paradójicamente, siendo como es una Ley transversal que afecta a todos, la gente sigue sin conocerla; sigue sin tener en la cabeza la legislación de protección de datos, cuando lo que hay que hacer es normalizar, lo que yo llamo normalizar la cultura de la protección de datos.

En una publicación que pueden ustedes localizar en internet, en la página web de la agencia, que es un libro que se editó de los 20 años de la Agencia Española de Protección Datos, me pidieron una colaboración y la titulé “Normalizar la Cultura de la Protección de Datos”.

Eso es lo que intenté durante el tiempo que estuve en la agencia: Normalizarlo. Incluir el chip de la protección de datos en la cabeza de todos.

Que no se considere como algo excepcional, que sólo tiene que ver con los expertos en privacidad, con los técnicos informáticos o con los ingenieros de telecomunicaciones y no con los demás; tiene que ver con todos.

Pese a ese carácter transversal de la Ley, ésta sigue siendo poco conocida.

Esto nos lleva, por tanto, a resaltar el derecho a la protección de datos y qué modelo a elegir.

No podemos en absoluto renunciar al modelo que se basa en el reconocimiento del derecho a la protección de datos, como un verdadero derecho fundamental.

Así se dice en la Constitución mexicana, se ha resaltado aquí en la inauguración; así se dice también en la Carta de los Derechos Fundamentales, se ha resaltado en la mesa anterior.

No podemos entender que la protección de datos es un principio, es un *desiderátum*, es algo que tiene que ver con otro derecho; es un derecho fundamental por sí mismo, es autónomo.

Además, fíjense, es un derecho que no equivale ni es el mismo que el derecho a la privacidad.

Hace muchos años que privacidad y protección de datos se desvincularon; son primas hermanas, pero no son lo mismo.

La protección de datos hace ya mucho que se emancipó de la privacidad.

No sólo hay que proteger los datos privados o íntimos; hay que proteger todos los datos, todos los datos personales, sean éstos íntimos o no lo sean.

Todavía sigue estando generalizada la cuestión, la duda, la equivocación de que la protección de datos sólo se refiere a los datos personales íntimos o privados.

No, todos nosotros sabemos, todos ustedes saben que esto no es así y tenemos que resaltarlo una y otra vez.

La protección de datos afecta a todos los datos y se traduce en ese poder de disposición sobre los propios datos de carácter personal.

Es la “Shell Determination” a que antes hacía referencia y que ya en los años setenta, antes de la Sentencia del Tribunal Federal Alemán, que puso sobre la mesa Westin.

Westin era un científico, un investigador americano fallecido hace unos años, hace pocos años, que tenía la idea acerca de que la idea clave era la autodeterminación, la “Shell Determination”. La

autodeterminación en el sentido de que nosotros somos propietarios de nuestros datos.

Por cierto, Westin tiene una frase preciosa. Él dice que “los Estados totalitarios quieren un ciudadano de cristal y una administración opaca y los Estados democráticos quieren un ciudadano opaco y una administración de cristal”, y es así.

Las dictaduras quieren un ciudadano de cristal y una administración opaca.

Las democracias, por el contrario, quieren o deben querer un ciudadano opaco y una administración de cristal.

Un modelo basado en la partición de datos global, que va poco a poco tomando principios, tomando criterios de los distintos modelos que están conviviendo.

Se ha dicho en más de una ocasión, en este mismo foro, que México ocupa un lugar privilegiado en materia de protección de datos, privilegiado y al mismo tiempo en la encrucijada, en la encrucijada porque está a caballo entre el modelo APEC, el modelo de Estados Unidos, el modelo latinoamericano y el modelo europeo. Privilegiado en ese sentido y en la encrucijada porque tiene que convivir con muchos modelos.

Fíjense que la legislación mexicana ha sido capaz de diseñar un modelo mexicano que ha tomado criterios, elementos, características de los distintos modelos con los que tiene que convivir.

Esta legislación mexicana, que ya se pone de manifiesto en la Ley Federal de Protección de Datos en Posesión de los Particulares, es una legislación que responde a la inmensa mayoría de estos principios, que son los principios, los que tienen ustedes, que se están ya implantando a nivel casi mundial y que se recogen, como veremos de inmediato, en el Reglamento General de Protección de Datos que se acaba de aprobar en la Unión Europea, en abril de este año.

Los he puesto en inglés, pero única y especialmente porque no hay quien traduzca el primero de los principio, no tenía sentido poner "*accountability*" y luego los demás en español.

¿Qué es *accountability*?

Responsabilidad, compromiso responsable, responsabilidad proactiva. Ya veremos cómo se traduce.

El tema es que a través del principio de accountability se deja en manos de los responsables, encargados, que ellos sean los que decidan qué medidas técnicas o administrativas, de todo tipo, no sólo de seguridad, tienen que adaptar, tienen que implantar para garantizar el derecho a la protección de datos. Ahora lo veremos.

Privacidad desde el diseño, suena muy bien, *privacy from desing,* es algo sencillísimo, es algo muy simple, es tan simple –como antes les señalaba– como que cuando se vaya a diseñar un producto o aplicación que implique tratamiento de información se tenga en cuenta la privacidad.

A nadie –como antes les decía– se le ocurre el diseñar un vehículo sin tener en cuanto la seguridad, desde el diseño, en el diseño forma parte de la seguridad; a nadie se le ocurre diseñar un proyecto de un edificio sin el sistema de prevención de incendios.

Pero no hay que decírselo al arquitecto, él ya lo sabe, es *security by desing* en los vehículos, en los edificios, bueno, pues *privacy from desing,* es algo tan sencillo como esto.

Si usted va diseñar un producto o un sistema o programa, tenga en cuenta la privacidad, igual que *privacy by defolt*, si hay varias posibilidades, usted elija la más respetuosa, el ejemplo, ya es lugar común decirlo, y disculpen porque lo repita de nuevo, porque seguramente lo han oído montones de veces, es en las redes sociales, pues haga el perfil del usuario privado por defecto en lugar de público por defecto, y si el usuario lo quiere hacer público, que lo haga; no que sea público por defecto y que tenga que cambiar la configuración de seguridad para hacerlo privado, porque la privacidad por defecto exige que por defecto el perfil sea privado y no público.

El principio, la obligación, estamos hablando de principios, derechos, deberes de la notificación de violaciones de seguridad. Luego me referiré a ello.

Y luego a otros derechos, nuevos derechos, el derecho al olvido, el derecho a la portabilidad. Todo esto junto con el bagaje que ya tenemos desde los años sesentas o setentas del siglo pasado, va configurando un nuevo derecho a la protección de datos.

Una protección además que es muy semejante en muchos países, de muy distintas latitudes.

Esto nos lleva ya a la Ley General de Protección de Datos, que fue ayer dictaminada y al Reglamento Europeo de Protección de Datos; Ley General, que se publicó en la Gaceta de la Cámara de Diputados de 3 de mayo de 2016, pero que ayer fue dictaminada y Reglamento General de Protección de Datos, que se publicó en el Diario Oficial de 4 de mayo de 2016. Fíjense, importante que van muy parejos.

El Reglamento ya está aprobado, no así, como saben o es evidente, la Ley General.

El Reglamento consta de 99 artículos, la Ley General de 168 artículos. No voy a entrar ahí evidentemente, pero sí que interesa resaltar que el contenido del Reglamento y el de la Ley General son semejantes; hay diferencias, pero responden a un mismo patrón, con las peculiaridades de la Ley General evidentemente y las peculiaridades del Reglamento.

Se habla de los principios, de los derechos del interesado, de la figura de responsabilidad y el encargado, de las figuras internacionales, de los actores de control, etcétera.

Lo mismo que ocurre con la Ley General, los principios y deberes, derechos, responsable y encargado, comunicaciones de datos y transferencias, acciones preventivas, responsables en materia de datos, organismos garantes, procedimientos, facultades de verificación, medidas de apremio y responsabilidad.

El esquema es muy semejante desde el objeto y principios hasta las autoridades y régimen sancionador, pasando por autorregulación, transferencias internacionales, responsable y encargado, derechos de los ciudadanos, derechos de los titulares.

Por tanto, el esquema es muy semejante, y no sólo el esquema y el hilo conductor, sino a veces también los contenidos.

Del mismo modo, el Reglamento, esto es un poco complicado, pero el Reglamento entró en vigor en mayo de este año, pero no es plenamente aplicable hasta el 25 de mayo del 2018.

Para entenderlo, es una especie como de transitorio, de demora en la aplicación hasta mayo de 2018. ¿Para qué? Para que los estados miembros de la Unión Europea vayan adaptándose a la nueva norma, un Reglamento como la Ley General, que en parte es directamente aplicable a todos los estados miembros.

En este sentido, la Directiva 45/46 tenía que ser traspuesta por los estados miembros, la directiva generaba o regulaba una serie de principios, un marco mucho más general, que tenía que ser traspuesto por los estados miembros a su ordenamiento interno.

El Reglamento no, el Reglamento es directamente aplicable, es obligatorio en todos los estados miembros, de modo además también que, pese a que no sea aplicable hasta mayo de 2018, en virtud del principio de lealtad comunitaria, no se pueden tomar medidas que puedan afectar a la eficacia del propio Reglamento desde mayo del 2018.

También, en cuanto al Reglamento, se plantea lo mismo que se está planteando acá en México con la Ley General, que es la relación entre el Reglamento y las leyes nacionales de protección de datos, aquí entre la Ley General y las leyes de los distintos estados.

También hay que determinar cuáles son los efectos del Reglamento sobre las legislaciones nacionales, no las deroga.

En España, por ejemplo, la Ley Orgánica de Protección de Datos no queda derogada, quedará desplazada, en su caso, pero no queda derogada.

Y lo que sí es verdad es que hay que adaptarla y, en ese sentido, en España, por ejemplo, el gobierno ha encargado, a través del Ministerio de Justicia, a la Comisión General de Codificación, y en particular a la sección de Derecho Público, que tengo el honor de presidir, nos ha encargado que elaboremos, junto con la Agencia Española de Protección de Datos, porque es impensable hacerlo sin la Agencia, junto con la Agencia se ha constituido una comisión mixta, que, como digo, yo coordino, Comisión de Codificación y Agencia de Protección de Datos, para elaborar una propuesta normativa, que tendremos que presentar al gobierno en el primer trimestre del año que viene.

¿Por qué? Porque una vez que se apruebe este proyecto de norma, tendrá que pasar al gobierno, dictaminarse por el Consejo, etcétera, de ahí al Congreso, como aquí también, y esto tiene que estar aprobado para mayo de 2018 y ya no hay tiempo, no hay tiempo, hay muy poco tiempo.

Por lo tanto, para marzo del año que viene, como muy tarde, tenemos que tener ya una propuesta y estamos trabajando en ello, estamos ya trabajando en la Ley de Adaptación en España al Reglamento General de Protección de Datos.

La Ley General se mueve en un estadio muy semejante. Como saben ustedes perfectamente, mucho mejor que yo, en el artículo 1º se dice que la Ley es de directa aplicación y observancia directa en el orden federal, igual que exige el Reglamento General de Protección de Datos en Europa, que es de directa aplicación, con un alcance más general que la Ley.

Se dice que entra en vigor al día siguiente, en Europa el Reglamento entra en vigor al día siguiente, pero no es aplicable hasta mayo de 2018, igual que aquí se establece que hay un plazo de seis meses para adaptar las normas.

Y si no se adaptan esas normas, como si no se aprueban leyes en Europa, será directamente aplicable el reglamento, que lo es. Y aquí también será la Ley General la que se aplicará.

Con lo cual fíjense que el escenario es muy semejante, es muy fácil comprender tanto desde fuera, desde la Unión Europea lo que puede ocurrir con la Ley General, como quizá aquí lo que está ocurriendo o va ocurrir en la Unión Europea.

Y ambos, la Ley y el reglamento responden a lo que yo creo que, como antes señalaba, es un modelo más global de protección de datos.

Un modelo en el que, y este es irrenunciable totalmente, la protección de datos es un derecho fundamental, es un derecho autónomo. Lo dice claramente el artículo primero de la ley remitiéndose a los artículos seis y 16 constitucionales, y dice claramente el artículo primero del Reglamento Federal de Protección de Datos de la Unión Europea, remitiéndose al artículo ocho de la carta europea de derechos fundamentales.

Luego tanto una norma como otra se remiten a una norma superior, la constitución en México, la carta de derechos fundamentales, que reconocen expresamente el derecho fundamental a la protección de datos.

Y dos principios que recogen tanto uno como otro son muy semejantes, si los ven ahí: Legitud, no los voy a leer, ahí están. Tanto uno como en otro son muy semejantes.

Fíjense que me atrevería a decir; atrevería a decir no, afirmo que es más clara en cuanto a la definición de los principios la Ley General que el reglamento. El reglamento yo no sé por qué, sinceramente, se ha complicado tanto a la hora de definir los principios.

Tampoco son tan complicados, es habilitación, finalidad, calidad, seguridad. Sin embargo el reglamento, comprendan ustedes que el reglamento es fruto de la negociación entre 28 países.

El reglamento de protección de datos es la norma en toda la historia del derecho de la Unión Europea, que más enmiendas ha recibido en su elaboración.

Es la norma que más presiones de lobbies externos ha recibido en toda la historia de la Unión Europea. Ni el derecho a la competencia, ni derecho a protección de los consumidores ni nada.

La que más presiones ha recibido en cuanto a lobbies de todo tipo y condición, privados y públicos.

Y esto ha generado una norma que está bien, está muy bien, es un gran paso en el ámbito de la protección al derecho de la Unión Europea, pero que tiene sus problemas.

Es como cuando ya a mi madre ya algo mayor le pregunto que qué tal está, y me dice: Estoy bien, sin entrar a detalles. Aquí el reglamento igual, está bien, sin entrar en detalles.

Lo mismo ocurre, el reglamento está muy bien. Pero amigo, cuando entramos en los detalles ya el tema ya empieza un achaque por aquí, un achaque por allá, la cadera, el corazón y tal. Algo falla.

Y por eso es también por lo que los principios no están tan claramente definidos, en mi opinión, porque aquí se trataba que los países fuesen imponiendo un poco su criterio. Y en el reglamento es verdad, se nota una influencia de España, de Bélgica, de Francia, de Italia, de Reino Unido.

Hay cosas que son claramente españolas, el tema de los derechos de los menores, el tema del régimen sancionador es claramente español.

Hay otras que son claramente de otros países, el modelo anglosajón, la accountability claramente; hay otros que son claramente alemanas, el delegado de protección de datos. Se ha tenido que configurar una norma que ha tenido que contentar a todos, y de ahí es que quizá los principios no encajen o no sean tan claros.

Hay uno que está al final entre paréntesis, porque no está en la relación de principios de los primeros artículos de la Ley del reglamento, que es el del control independiente.

¿Pero qué responde? Que respeta tanto la Unión Europea como a México.

Y fíjense que esto es muy importante. El principio de control independiente, la existencia de autoridades de protección de datos independientes forma parte del contenido esencial del derecho a la protección de datos de carácter personal, aquí en México y en la Unión Europea.

Quizá con más claridad en la Unión Europea, porque el artículo ocho de la Carta Europea de Derechos Fundamentales dice expresamente que una autoridad independiente de control será la que tutele el derecho a la protección de datos. Es el único derecho fundamental en el que en cuya derogación se hacer referencia a una autoridad independiente de control, que no son los jueces, que también velan por el derecho a la protección de datos.

De modo y manera que si no existe esa autoridad independiente, se entiende que el derecho a la protección de datos no está protegido adecuadamente y el núcleo esencial del derecho sufre, se atenta contra el núcleo esencial si no existe esa autoridad independiente.

Bien, ese principio, por tanto, que llega de una autoridad independiente también se recoge, aunque no se numera en la Ley y se numera y se recoge también, aunque no se numera en el Reglamento; con lo cual, en cuanto a los principios, ambos textos son muy parejos.

Y ambos textos, y más, el cambio es más notable en Europa que en México, sobre todo en Europa, en Europa se pasa de lo que llamo de la gestión de los datos al gobierno responsable de la información personal.

¿Qué quiero decir con gestión de los datos? Hasta ahora en Europa, no tanto en México, porque en México ya desde la Ley Federal de Protección de Datos en Posesión de los Particulares se asumió el criterio de la accountability, de la responsabilidad, pero en Europa no.

En Europa, con la Directiva 9646 y con las Leyes de Trasposición, los modelos eran más de cumplimiento formal por parte de los responsables encargados, instrucción de los ficheros, medidas de seguridad tasadas en nuevas normas, obligaciones que había que cumplir.

Ahora no, ahora de esa gestión de datos se pasa a un gobierno responsable de información personal.

Los responsables y los encargados tienen que ellos asumir la responsabilidad de ese gobierno responsable de información; de información personal, evidentemente, en el que los titulares de los datos salen fortalecidos, salen reforzados. Y en el Reglamento Europeo, especialmente.

¿Por qué? Y sinceramente dudo, se los digo sinceramente que se trate de una opción totalmente correcta o totalmente acertada, mejor dicho, por parte del Reglamento Europeo.

En el ámbito europeo se ha optado claramente por el consentimiento explícito, no ha lugar al consentimiento tácito ni al presunto; es más, en esos considerados, en el 32 del Reglamento se dice expresamente que el silencio no equivale al consentimiento, que silencio no tiene que ver con consentimiento.

Algo distinto a lo que ocurre en la Ley, el consentimiento debe ser previo, pero puede ser expreso o tácito. Y algo que es lo que ocurre hoy en la Ley Española, el consentimiento puede ser, debe ser inequívoco, previo, pero puede ser tácito también, presunto o tácito, expreso, presunto o tácito.

Se ha acabado con este modelo, se va a acabar con este modelo en la Unión Europea desde el 27 de mayo del 2018. Yo tengo mis dudas.

Y les pongo también el ejemplo: ¿Qué es lo que está ocurriendo con la exigencia de consentimiento previo en relación con el uso de las cookies?

Pues que se están diseñando mecanismos para hacer ver que es expreso el consentimiento o que no lo es.

Si usted sigue navegando se entiende que ha autorizado el uso de las cookies, porque exigir consentimiento previo y expreso para decir las cookies no tiene sentido, con todos mis respetos. No tiene sentido porque es poner puertas al campo.

Yo como usuario quiero saber, quiero mejor o prefiero saber qué van a hacer con mi información, quiero poder revocar el consentimiento, quiero tener información, quiero saber qué es lo que se está manejando, pero pedir el consentimiento expreso paso a paso puede bloquear el uso de internet. Y no es necesariamente una mayor garantía.

Si algo fuere, el Reglamento ha optado por el procedimiento explícito y recoge una serie de nuevos derechos, entre otros, antes de que se me olvide, que no se recoge en la Ley General, siendo ésa la cancelación, pero no el derecho al olvido; en la Ley General Mexicana no se recoge, como saben ustedes, sí en el Reglamento, como derecho de supresión.

No podemos entrar en ello, pero no tengo muy claro que la relación que tiene el artículo 17 del Reglamento sea todo lo correcto que debería ser, pero ahí está, el derecho al olvido se ha recogido, y de hecho la portabilidad que se recoge en la Ley, artículo 57; y en el Reglamento, artículo 20.

Y fíjense que también aquí, en mi opinión, la regulación de la Ley General es más acertada que la relación del Reglamento; porque el Reglamento al final lo que viene a decir es que existe el derecho a la portabilidad respecto de los datos personales que el afectado ha aportado. Sólo eso.

Y la Ley General es mucho más amplia, incluso tiene también algunas cuestiones más concretas, no sólo en cuanto a los datos personales, sino más en cuanto a la información y cita incluso la posibilidad del paso de un proveedor de servicios de correo electrónico –no lo dije expresamente, pero se deduce– a otro, que nos podemos llevar toda

la información de nuestro prestador de servicio de correo electrónico al nuevo.

Sin embargo, el Reglamento Europeo, si se interpreta restrictivamente, puede plantear problemas porque se refiere solo a la portabilidad e los datos personales aportados por el interesado, no a toda la información que tenemos en nuestro correo electrónico.

Muy rápidamente, para ir ya terminando, todo lo que tienen ustedes en esa pantalla tiene que ver con esa nueva aproximación, basada en la responsabilidad del afectado; perdón, del responsable; responsabilidad del responsable, del encargado, la accountability.

Por eso el riesgo pasa a ocupar un papel principal en la protección de datos, porque el responsable y el encargado tienen que valorar el riesgo, asumir que el tratamiento puede generar riesgos y en función del riesgo que se genere tomar las medidas que sean necesarias, adecuadas, pertinentes, para intentar garantizar que el tratamiento de los datos sea, a su vez, correcto y adecuado respecto a la Ley o al Reglamento.

La perspectiva del riesgo pasa a ser esencial, lo que se traduce en la responsabilidad proactiva, muy bien definida en los artículos 29 y 30 de la Ley y también en el artículo 24 del Reglamento Europeo, en esos principios que ya hemos hablado desde el diseño perfecto y, muy importante, la evaluación de impacto a la privacidad.

Pasan a ser puntos esenciales, tanto en la Ley como en el Reglamento, basado una vez más en el riesgo; no podemos entrar en ello, pero tanto la Ley General como el Reglamento se detienen en la evaluación de impacto a la protección de datos, cuando se pueda prever que se va generar un riesgo en el tratamiento de la información.

Una figura esencial en el Reglamento Europeo es el Delegado de Protección de Datos, al que también se ha hecho referencia, pero quizá más de pasada y de forma potestativa en la Ley, sin perjuicio de que también se cita a los Comités y Unidades de Transparencia, que son algo distinto a los delegados.

El Delegado de Protección de Datos es una figura nueva en el Reglamento Europeo que viene de Alemania, que van a tener que nombrar a todos los responsables públicos, no así todos los privados; sí los privados cuando lleven a cabo tratamientos a gran escala de datos especialmente protegidos, sensibles o aquéllos que impliquen un seguimiento o control de las personas, y que pasa a ser una figura central, nuclear.

Porque es quien va ser interlocutor de las autoridades de protección de datos; tiene que ser absolutamente independiente; no puede recibir mandato alguno; no puede ser despedido por el desempeño de sus funciones en cuanto a Delegado de Protección de Datos.

Se obliga –fíjense– el propio Reglamento Europeo obliga a los responsables públicos o privados a dotar de medios suficientes, económicos y de recursos al Delegado de Protección de Datos; quiere que ser una figura central.

Igualmente, se ponen un enorme hincapié en la inseguridad.

Fíjense, en mi opinión los criterios de proporcionalidad o calidad, finalidad y seguridad, en mi opinión son los centrales, los nucleares.

De nada sirve contar con el consentimiento expreso, previo, justificado, acreditado con evidencias, garantizar el precedente de finalidad, garantizar el precedente de proporcionalidad, de calidad, si no hay medidas de seguridad.

¿Por qué? Porque si no hay medidas de seguridad se pierde el control sobre los propios datos.

Si yo no sé qué medidas de seguridad me está implantando un responsable, aunque no tenga por qué saberlas. Si dudo de que tratamiento de mis datos sea seguro, eso implica que no voy a saber qué va ocurrir con mis datos, porque si resulta que cedo mis datos a una empresa que me ha informado aviso de privacidad, magnífico, el mejor posible de todos los avisos de privacidad; los datos que recaba son los adecuados, pertinentes, no excesivos.

Pero resulta que no tienes medidas de seguridad, eso para qué me sirve; si resulta que cualquiera va poder acceder a esos datos y los va a utilizar para algo totalmente distinto de lo que ni me han informado ni sé qué va a ocurrir con ellos.

La seguridad es el punto central, en mi opinión, cada vez más el punto central en la protección de datos, porque es lo que realmente garantiza el resto de los principios y el resto de los derechos.

Se regula el responsable encargado, así como el subencargado, tanto en el Reglamento como en la Ley, mecanismos de autorregulación, certificación. Muy importante y muy interesante la regulación de las mejores prácticas en la Ley General de Protección de Datos, y por supuesto las experiencias internacionales.

Y, para terminar, se hace referencia al sistema institucional y de autoridades, tanto de los organismos independientes, organismos garantes en la Ley General, el INAI y otros organismos garantes.

Las autoridades de control independientes en la Unión Europea.

Aquí se ha hecho referencia antes, por Julián Prieto, lo ha explicado en su interesantísima exposición, hay que tener en cuenta que las cosas van a cambiar en la Unión Europea.

Como consecuencia de lo que antes les decía, la inexistencia de fronteras en el tratamiento de los datos, y a eso es cuando me refiero cuando o se refiere el Reglamento cuando habla de la autoridad principal y autoridad interesada.

En estos momentos en Europa, cuando una multinacional, porque esto está pasando en multinaciones, lleva a cabo un tratamiento en algún país, la autoridad competente para conocer de la reclamación contra ese tratamiento presuntamente ilícito para conocer y para resolver es aquella donde se lleva a cabo el tratamiento.

Si una multinacional, con sede en Finlandia, en Holanda, lleva a cabo un tratamiento de España, un tratamiento, pero ordenado desde Finlandia o desde Holanda que afecta a naciones de la Unión

Europea, pero afecta en particular a un español, esta persona denuncia ante la agencia española y la agencia española resuelve.

Esto que había o qué está generando. Es verdad, que las multinacionales se encuentran con resoluciones de la agencia española, de la francesa, de la danesa que pueden ser contradictorias y que pueden atender a criterios distintos de interpretación.

Esto se intenta resolver diciendo lo siguiente: Cuando estemos ante un tratamiento internacional, que afecte a ciudadanos de más de un país, por tanto tenga trascendencia más que local, no es sólo local, la denuncia se presenta ante la autoridad del ciudadano afectado, pero quien va resolver va ser la autoridad donde esté radicada la oficina principal, la estación principal del responsable.

No quiero, empecemos en Ikea o Phillips, pues si es Phillips yo denuncio en España y resuelve la autoridad holandesa; denuncio en España y resuelve la autoridad sueca.

Tienen que estar de acuerdo ambas autoridades y tener un mecanismo de cooperación, tienen que estar de acuerdo, y si no están de acuerdo entra el Comité Europeo. Es muy complicado, pero estas son las reglas esenciales.

Y al final decide la autoridad principal, salvo que la resolución sea desestimatoria o no se admita, es decir, no le den la razón al ciudadano.

En cuyo caso la resolución la adopta la autoridad de origen, la interesada.

¿Por qué?

Para dar pie a la posibilidad de recurrir ante los tribunales de tu país; si a mí me dicen que Ikea ha tratado bien mis datos, pese a que yo considere que no lo ha hecho, desestima mi petición, quien resuelve no es la autoridad sueca sino la española, para poder yo recurrir ante la otra instancia.

La paradoja se produce: Resulta que la autoridad española es la que toma la decisión, pero es una decisión que le viene dada de la sueca, aplicando el reglamento y la legislación sueca, que es adoptada por alguna autoridad española, y recurrir al tribunal español, que va tener que juzgar en base a la aplicación del derecho sueco. Es un lío, es muy complicado.

Y las autoridades, me consta, y Julián nos lo podrá decir con más seguridad, están ahora colaborando, trabajando, para intentar poner orden en esta situación enormemente complicada, que afecta al procedimiento y que afecta incluso al control jurisdiccional de las decisiones de la administración.

Asimismo, también hay órganos conjuntos o modelos de cooperación del Sistema Nacional de Transparencia o el Comité Europeo de Protección de Datos, que es el antiguo artículo 29, el antiguo grupo del artículo 29, que ahora se llamará Comité Europeo; sale fortalecido, tiene personalidad jurídica.

La Secretaría corresponde al Supervisor Europeo de Protección de Datos y tiene más funciones de las que antes tenía el artículo 29.

Por último, el modelo sancionador, hay un modelo sancionador muy definido, tanto en la Ley General como en Reglamento.

Se definen los procedimientos, fíjense, es quizá la parte más extensa de la Ley General, pero ¿por qué? Porque la Ley General se aplica directamente en el ámbito federal, por eso requiere también de una relación más detallada de los procedimientos, igual que hay una regulación de los procedimientos y de las sanciones en el Reglamento.

En este sentido, se ha llamado la atención acerca de que el Reglamento Europeo incumpla o podría incumplir los principios de tipificación de infracciones y sanciones previstos en las normas constitucionales. En la justicia española, por ejemplo, artículos 24 y 25, existe la tipificación de infracciones y sanciones cuando hablamos del hecho sancionador.

Fíjense ustedes, según el Reglamento, antes lo apuntaba también Julián, en España la agencia puede imponer multas de hasta 600 mil

euros, son las multas más elevadas que puede poner una autoridad en Europa, salvo error mío.

Ahora, sin embargo, según el Reglamento, te pueden imponer multas de uno a 20 millones de euros o al 4 por ciento del volumen total anual global de facturación de una empresa.

Yo hice el otro día el cálculo de Google y Facebook y me salían unas cantidades absolutamente astronómicas.

Pero el tema no es que se pueda imponer esa sanción, sino que el Reglamento no define sectores, no escalona las sanciones, dice: Para un tipo de sanciones, de uno a 20 millones de euros, de uno a 10 millones y para otro de uno a 20 millones de euros.

Fíjense ustedes la discrecionalidad tan exagerada de que disponen o que van a disponer las autoridades, eso puede ir en contra, salvo que se resuelvan las leyes nacionales del principio de tipificación de infracciones y sanciones.

Los grandes retos, y con esto acabo, son desarrollar la Ley o desarrollar el Reglamento. En ambos modelos hay que unificar la normativa sobre la protección de datos, pero fíjense que esto no va a ser fácil en Europa.

De hecho, hace unos meses tuve una reunión en París, estuvimos debatiendo el Reglamento, había autoridades de protección y de datos y las autoridades de protección de datos, cuando expusieron qué se está haciendo en cada país en relación al Reglamento, lo primero que dijeron fue “estamos ya empezando a relatar la adecuación de Reglamento”, con lo cual va a haber también disparidad en los distintos estados de la Unión Europea.

Aquí en México se puede, salvo que se opte por la elaboración de normas muy semejantes entre sí.

Creo que aquí los institutos tienen mucho que ver, aparte de los legisladores, evidentemente los estados, pero tienen mucho que ver para potenciar una normatividad que sea homogénea.

No una Ley General, no una ley marco, o quizá sí, unas guías, unas directrices, porque va a verse envuelto en una gran incertidumbre en cuanto a la legislación que sea de aplicación, porque además no sólo tenemos que contar con la legislación de protección de datos, sino también con leyes sectoriales, leyes que conviven.

En México, la Ley Federal de Protección de Datos Personales en Posesión de Particulares, las leyes de transparencia, leyes sectoriales. En España también, en la Unión Europea y otras directivas que tienen que convivir.

Luego, no va a ser fácil conseguir la unificación, hay que también concienciar y capacitar, y aquí verán que hago un poco de publicidad, voy a aprovechar en esta lámina.

Concienciar y capacitar, esto es esencial, creo que si hay algo que trae bueno, que hay mucho, la Ley General y el Reglamento, es que ha puesto de nuevo la agenda de la protección de datos; mejor dicho, la protección de datos en la agenda de todos.

Ahora, hay mucha gente hablando de la Ley General, en Europa y en el mundo hay mucha gente hablando del Reglamento de Protección de Datos, mucha gente.

Ya sólo la aprobación de la Ley General y la aprobación del Reglamento ha hecho que se hable de protección de datos, que se conciencie a la gente de la importancia de protección de datos, pero hay que capacitar, hay que generar profesionales, porque esto es complicado.

Si me permiten hacer referencia a ese máster que antes se citaba que estamos impartiendo en la universidad en colaboración entre otras, con INFUEN, hemos tenido alumnos del INFOEM, INAI, de INFODF, en estos momentos del instituto de Colima, indirectamente de Chihuahua, también de Perú, de Colombia, de Brasil.

Es un master semipresencial que además sí que puede y sí que tiene efectos de cara a la certificación o acreditación para delegado de protección de datos.

Y terminaría con estas frases. Quienes de ustedes estuvieron en Uruguay en la conferencia, de Autoridades de Protección de Datos de Uruguay, recordarán que la clausuró Mujica, y si recuerdan los que ahí estuvieron, él dijo: Me dicen que estándares de privacidad, pero si privacidad sólo tienen los malos, los demás no tenemos privacidad.

Saben qué es lo que dijo Scott Mackinlay, dijo dos cosas, no sé cuál de las dos más graves, que todos conocemos ya. Primero: Tenemos cero privacidad, desengañémonos, tenemos cero privacidad.

Y poco después unos años después le escuché yo, fue en el 2002, creo en el 2003 en Washington, él mismo dijo en un evento, sino me equivoco de la IAPP, dijo: Hace años dije, desengáñense, tienen cero privacidad. No, me corrijo, sí tenemos privacidad, pero tenemos la privacidad que los demás consienten que tengamos. Yo no sé qué es peor, si una cosa o si la otra.

Y luego recuerdo que una vez iba a un encuentro, precisamente del INAI, y el taxista dijo: Ah, sí, el INAI, protección de datos. Y le dije: Y usted, en lo personal, cree en privacidad. Y me dijo el taxista literalmente: ¿Privacidad? Pero si eso no existe. Dijo convencido.

Nos rodea un mundo complejo, muy complejo, tenemos que intentar generar certidumbres. Me gusta mucho esa frase de *Gamborí*n con la que termino siempre o casi siempre mis intervenciones: “Nos movemos en trizas de certeza en un mar de incertidumbres”.

Es verdad, tenemos que intentar generar islas ce certeza en un mundo como el de la protección de datos que es incierto por naturaleza. Cada uno debemos intentar generar, hacer surgir islas de certeza.

Y luego la otra se nos haría, discúlpenme, por eso pongo Benito Juárez en grande y Piñar en pequeño. Sería, Benito Juárez estropeado por José Luis Piñar.

Desde la primera vez que vine, me acuerdo, a México, cuando el INAI estaba en Insurgentes en un piso, no en la sede que tienen ahora, la primera de todas, estaba María Marván de comisionada, vine aquí a hablar y tuve que conocerla, se me ocurrió esta frase: “El respeto al dato ajeno es la paz”. Creo que esto es muy importante.

¿Por qué?

Porque aquí está resumido todo lo que es la protección de datos. Primero, hay que respetar los datos; segundo, los datos por definición siempre son ajenos, salvo los nuestros propios.

Tenemos que superar ya esa idea de que si yo hago una base de datos los datos son míos. Los datos siempre son del titular, los datos siempre son ajenos, y si no respetamos esto nos llevará a una situación de paz idílica que ojalá se consiga.

Nada más por mí parte, muchas gracias por su atención y quedo a su disposición.

Moderador: Muchas gracias por la excelente conferencia al doctor Piñar, y vamos a dar paso a algunas preguntas que nos ha hecho llegar el público.

Tenemos como 10 minutos, entonces haré las cuatro preguntas que tengo aquí, y ya si nos va ayudando a contestar el doctor en el orden que él considere.

¿Por medio de un tratamiento internacional existente, en caso dé, o en proyecto, se ha considerado regular en especial las redes sociales y noticiarios como CNN o buscadores como Facebook, Twitter, no sólo pensando en la jurisdicción?

También piden al doctor detallar más algunas de las implicaciones del principio de legitimación y qué elementos involucra.

Después, para los jóvenes europeos de 18 a 24 años es relevante el tema de la privacidad. ¿Cuáles son los mecanismos que considera usan para ello?

Y, por último: ¿Debería desaparecer el principio del consentimiento?

De ser el caso, ¿a dónde poner el acento en las Leyes de Datos?

Esas son las cuatro preguntas que le vamos a agradecer al doctor Piñar nos ayude a contestar en ese lapso de los últimos 10 minutos, por favor.

Sr. José Luis Piñar Mañas: Perfecto. Las respondo en orden.

En cuanto al Tratado Internacional, desconozco este Tratado Internacional por la que parece, según la pregunta, se pretenderían regular las redes sociales y noticieros, como sería Facebook y Twitter.

Desconozco la existencia de este Tratado Internacional, incluso del proyecto.

Lo que sí, es que esto me da pie para indicar que quizá en un mundo global lo que sería necesario es contar con un tratado internacional que fijase las reglas del juego aplicables a nivel lo más amplio posible mejor en materia de protección de datos. Claro, esto es complicado.

Entiendo que debe ser un tratado incluso aprobado en el seno de Naciones Unidas sería lo mejor, pero esto nos llevaría a todo el mecanismo no siempre fácil de ratificación de los tratados y de sometimiento voluntario de los Estados al tratado.

Porque claro, no podemos olvidar ni ignorar que determinados países en los que parece ser, y hay también evidencias, que se llevan a cabo un número muy importante de tratamientos que afectan a terceros en otros países que no son del todo lícitos, quizá no serían propensos a ratificar ese tratado internacional, con lo cual a lo mejor nos encontraremos con un tratado ineficaz y al final ratificarían los países que ya cuentan con una legislación de protección de datos y que no necesitan de ese tratado para colaborar.

Pero en cualquier caso, yo creo que un tratado internacional sería un paso muy importante para conseguir de una vez por todas una regulación homogénea a nivel mundial en materia de protección de datos porque, repito, estamos ante un derecho que no conoce para nada de fronteras y cada quien en un menor nivel de aplicación territorial.

El territorio y la protección de datos creo que están más separados, están más desvinculados, cuando la Ley y el territorio siguen estando totalmente vinculados.

En cuanto a la legitimación, si el tema es, y ésta encaja con el consentimiento, con lo cual puedo a lo mejor responder ambas preguntas al mismo tiempo.

Primero, yo creo que no hay que acabar con el consentimiento ni mucho menos, y si se ha dilucidado algo semejante de mis palabras, lo quiero corregir. Para nada hay que acabar con el consentimiento, el consentimiento sigue siendo uno de los títulos habilitantes que legitiman el tratamiento más importante, sino el que más.

Lo que yo quiero resaltar es que el consentimiento no es la Panacea.

Es muy fácil conseguir un consentimiento exprés; de hecho, debo decir que no he podido exponerlo porque no he tenido tiempo, pero el Reglamento General de Protección de Datos tiene una regulación mucho más detallada del consentimiento enlazado con la información para garantizar que el afectado está más y mejor informado antes de dar su consentimiento.

Por ejemplo, dice, es un pequeño detalle: “Cuando el consentimiento se tenga que obtener en el marco de un contrato que se refiera a otros asuntos distintos del tratamiento de datos, en el que el tratamiento de datos sea algo accidenta, pero necesario, no se puede incorporar la cláusula informativa como una cláusula más dentro del articulado o del clausulado del contrato, sino que se tiene que diferenciar, separar, hacerlo, claro, legible y fácilmente comprensible”, o sea, no valdría el consentimiento otorgado porque la cláusula vigésima octava, que es la que va después de la 27 y va a anterior a la 29 y nada más, con la misma letra y el mismo texto, es la del consentimiento de protección de datos y sí te ha pasado.

Tiene que resaltarse. Por tanto, el consentimiento es muy útil y es uno de los tipos de legitimación.

Pero, ojo, que el consentimiento expreso –repito– no es la panacea. Yo prefiero hablar de un consentimiento válido, válidamente otorgado, que puede ser tácito o presunto, por qué no, en mi opinión.

¿Por qué?

Primero, ha venido funcionando bien en España y está funcionando en México. En España el conocimiento puede ser tácito y no ha generado grandes problemas.

Cuando se pone el conocimiento expreso se buscan subterfugios para superarlo, para hacer ver que es expreso el consentimiento, cuando en realidad no lo es.

Por eso yo creo que, en mi opinión, hay que poner más énfasis en otros principios: Finalidad, calidad, seguridad y siempre con la posibilidad de revocar el consentimiento.

En cuanto la legitimación el tema es que quien trata datos que son siempre por definición datos ajenos, tiene que tener un título que le legitime para ello. Ese título puede ser el consentimiento, hace legítimo el tratamiento de unos datos, o bien otro título –como sé– que lo establezca una Ley, que sea necesario por un contrato, etcétera, de las cosas que ya conocemos.

Por último, la última pregunta, el tema de los jóvenes europeos, la privacidad para los jóvenes europeos de 16 a 24 años.

Cada vez para los jóvenes tiene más importancia la privacidad, aunque no lo parezca. Yo hace unos años dirigí un proyecto de investigación que era Redes Sociales y Privacidad del Menor, y para él aparte de que hicimos público el texto, un libro, también llevamos a cabo un estudio de campo con más de tres mil niños en España, de entre 14 y 16 años, preguntándoles acerca de su percepción de la privacidad.

Fíjense que más de un 70 por ciento nos dijeron que para ellos la privacidad es importante y un porcentaje casi igual nos dijeron que ellos habían cambiado la configuración de la privacidad en su desarrollo. Es decir, esto es importante.

Los jóvenes ya conviven con las redes sociales y ellos empiezan a convivir con la privacidad.

¿Por qué? Porque entre ellos también, primero que ya saben mucho más que nosotros de estas cosas; sí sabe más que yo, ni nieto de tres años, así como los jóvenes de 18 y 24 años.

Pero ellos que es ya empiezan a conocer amigos y gente que ha tenido experiencias negativas en las redes sociales, por el mal uso de los datos y eso entre ellos enseguida se sabe.

Por tanto, es importante, pero para mí lo esencial y veo aquí, además, a bastantes alumnos de universidad, es la formación y capacitación preuniversitaria, antes de la universidad y en la universidad.

En este sentido, me parece muy interesante que en la Ley General se diga que las autoridades deberán promover que en los planes de estudios, que en las universidades se incorpore, se incluye la protección de datos como materia a estudiar.

Yo creo que a través de la concientización, capacitación, vendrá la asunción, como normal, de lo que no debe ser más que normal, que es el respeto a la privacidad.

Moderador: Excelente.

Muchas gracias al doctor José Luis Piñar.

Vamos a reconocerlo con fuerte aplauso.

Teníamos preparadas algunas notas de resumen, pero por el tiempo creo que está muy claro y agradecemos al doctor lo que nos ha compartido.

Quiero agradecer este esfuerzo, además, de análisis de nuestra casi ya nueva Ley General y su comparativo con el Reglamento Europeo, el cual realmente yo rescataría lo que él menciona del modelo mexicano, que creo que estamos generando y esa es la apuesta precisamente de los Comisionados del Pleno del INAI, de ir

modelando una apuesta porque el derecho de protección de datos personales en México tenga su propia identidad, su propia naturaleza y, al mismo tiempo, avancemos a esa cultura de protección de datos personales verdaderamente en nuestro país, con la participación ahora de un Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, que se sumaría ya de una manera conjunta para verdaderamente que todas las autoridades garantes de los estados, precisamente en mayor medida coadyuven justamente en esta tarea.

Y todos coordinados, todos trabajando por esta educación, como decías, digital, de nuestros niños, nuestros jóvenes y que precisamente todos los ciudadanos, esos porcentajes que mencionabas se vayan tomando en consideración para que en todo lo posible, también está muy claro, nos podamos sentir menos inseguros en nuestra información personal.

Muchas gracias a todos y recibe, José Luis, un reconocimiento de parte del Pleno del Instituto y sigamos con el programa.

Les pedimos que no se vayan porque vamos inmediatamente a proceder con la siguiente conferencia.

Muchas gracias.

Presentador: Se dará un breve receso para dar paso a la última conferencia.

-----o0o-----