

Ciudad de México, 26 de enero de 2018.

Versión estenográfica de la Conferencia Magistral: “La Protección de Datos Personales en Internet”, impartida por Miguel Recio Gayo, dentro del Seminario Internacional de Protección de Datos Personales, celebrado en el Centro Cultural San Ángel.

Presentador: Les hacemos una cordial invitación para que pasen a ocupar sus lugares.

Se informa a los asistentes que el recinto cuenta con la señalización, equipo y salidas de emergencia exigidas por Protección Civil para llevar a cabo evacuaciones ante cualquier tipo de eventualidad.

Solicitamos al público asistente, sea tan amable de apagar sus celulares y aparatos localizadores, o bien, ponerlos en modo vibrador.

El Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal les da la más cordial bienvenida al segundo día de actividades del Seminario Internacional de Protección de Datos Personales 2018.

Damos la bienvenida a este seminario al Magistrado Presidente del Tribunal Electoral de la Ciudad de México, licenciado Armando Hernández Cruz.

Esta mañana daremos inicio con la Conferencia Magistral: “La Protección de Datos Personales en Internet” que imparte Miguel Recio Gayo, para ello invitamos al Comisionado ciudadano del InfoDF Luis Fernando Sánchez Nava, haga uso de la palabra y es quien va a moderar esta conferencia.

Lic. Luis Fernando Sánchez Nava: Muy buen día a todos. Vamos a continuar con los trabajos de este seminario que ha estado muy nutrido, ha estado muy interesante y ahora nos acompaña Miguel Recio Gayo, quien aparte de ser conferencista de honor, digamos, para el Instituto, es un gran amigo, a quien le tenemos mucho aprecio.

Damos la bienvenida a las autoridades del Tribunal Electoral, al Magistrado Armando, bienvenido, a los Comisionados, a los

especialistas internacionales y a todos los servidores públicos que hoy nos acompañan.

Primero les presentaré a nuestro ponente, es doctorante en protección de datos personales por la Universidad de San Pablo, CEU de Madrid, maestro internacional universitario en protección de datos, transparencia y acceso a la información por la misma universidad.

Maestro en derecho de la propiedad intelectual por la Universidad George Washington University. Actualmente se desempeña como consultor en materia de protección de datos y privacidad.

Es profesor de la maestría internacional universitario y protección de datos, transparencia y acceso a la información por la Universidad de San Pablo, CEU de Madrid.

Es autor de diversas publicaciones en materia de protección de datos personales y derecho digital, entre ellas el ensayo 25 del InfoDF, la protección de datos en el ámbito de las telecomunicaciones a internet. De esta edición quiero destacar rápidamente las siguientes ideas:

El derecho a la protección de datos personales se concreta para el titular de los datos personales en el poder de decidir y controlar si un tercero puede transmitir a utilizar sus datos, que van desde el teléfono o domicilio hasta su religión, es decir, es el poder de control, la persona física, titular de los datos sobre quién, cómo y para qué se usan sus datos personales.

A diario en la Ciudad de México las personas proporcionan al menos 35 veces sus datos personales sin tener conciencia de que deben estar protegidos y no deberán ser utilizados con fines distintos por los cuales fueron entregados.

El internet es uno de los servicios de telecomunicaciones que proporciona a los usuarios importantes beneficios sociales y económicos, ya que a través de internet es posible acceder a multitud de servicios y aplicaciones, tales como el correo electrónico, las redes sociales, las páginas y sitios web, de manera que se pueda hacer uso del mismo como usuarios de dichos servicios, también como

profesionistas que, por ejemplo, tienen páginas o sitios web de comercio electrónico.

Con estas reflexiones que les invito a leer de manera completa el ensayo 25 del InfoDF, escrito por nuestro distinguido conferencista y que pueden descargar en el portal del InfoDF.

Sin más le doy la palabra, la bienvenida a Miguel Recio.

Dr. Miguel Recio Gayo: Muchas gracias, Comisionado, por su amable presentación, muchas gracias al InfoDF por la invitación a poder estar aquí en el día de hoy con todos ustedes. Es para mí un verdadero honor.

Y vamos a hablar de un tema que creo que es interesante y que nos afecta absolutamente a todos, a todas y a todos en este sentido. Y creo que en este auditorio en el día de hoy nos puede, incluso, llegar a efectuar en un doble sentido como usuarios de internet, pero si me lo permiten, de su lado, seguramente también ustedes como sujetos obligados son también responsables del tratamiento, con lo cual también están tratando datos personales a través de internet, cualquiera de sus instituciones que tenga una página web y que trate datos personales a través de un formulario, pues estaríamos dentro de la protección de datos personales en internet.

Lo que voy a hacer es darles una exposición en general, voy a intentar ajustarme al tiempo, dando posteriormente lugar a un posible debate o aceptar algunas preguntas, si me lo permiten. La Protección de Datos Personales en Internet, le podríamos haber puesto cualquier otro título, cómo navegar en internet sin sufrir un naufragio o cualquier otro que se les pueda ocurrir, porque creo que ayer, les felicito también por el evento en el sentido de que es muy ameno y estamos tratando temas que son muy, muy complicados y que son muy, muy serios y el poder combinar esa amenidad de los temas que se tratan con ese rigor, es muy de agradecer.

Con lo cual, si me lo permiten, bueno, es viernes, sé que todavía incluso es un poquito temprano, no se preocupen, no les voy a hacer preguntas complicadas, me las iré respondiendo yo a mí mismo. Sí me

van a permitir que les haga algunas preguntas, pero son en general, es para que podamos reflexionar.

Obviamente, el próximo domingo es justo el día que se celebra el Día de la Protección de Datos Personales en Internet y qué bueno que estamos en México y podemos hablar de la protección de datos personales en internet.

Imagínense con nuestros vecinos de allá arriba o con sus vecinos de, bueno, son vecinos de todos nosotros, hoy no estaríamos hablando de la protección de datos personales en internet, no hay un derecho humano a la protección de datos personales en Estados Unidos, sí lo hay en la Unión Europea, sí lo hay en México, sí lo hay en países de Latinoamérica, pero todavía hay algunos lugares en los que no hay ese derecho fundamental, desde un punto de vista europeo o derecho humano, desde el punto de vista mexicano a la protección de datos personales en internet.

Creo que eso nos puede permitir, pues responder a la primera de las preguntas, ¿qué es el derecho a la protección de datos personales? Pues es un derecho humano, es un derecho fundamental, como tal, que está reconocido en la Constitución Federal, obviamente, en los artículos 6 para sector público y 16 para sector privado.

Incluso, si me lo permiten de manera rápida, podríamos distinguir protección de datos personales de privacidad como tal, tenemos dos derechos humanos o dos derechos fundamentales: a la protección de datos personales como tal en los artículos 6 y 16 y luego hay un derecho a la privacidad en el Artículo 16, que es diferente, es la privacidad de las comunicaciones electrónicas, es proteger la correspondencia, es proteger, pues el contenido de esas comunicaciones.

Estos derechos aterrizan también en la Constitución Política de la Ciudad de México, el Artículo 7 incluye el derecho a la privacidad y el derecho a la protección de datos personales, con lo cual podemos ver cómo se encuentran los dos también en dicha Constitución y eso, si me lo permiten, les obliga a ustedes también como sujetos obligados, obviamente, hasta ahí llega el que podamos ir aterrizando el derecho a la protección de datos personales como tal.

Incluso, es muy llamativo cómo está establecido en la Constitución y creo que es importante que lo tengamos en cuenta, digo, la Constitución de la Ciudad de México, se protegerá la información relativa a la privacidad y a la protección de datos personales dentro de los límites establecidos por la Constitución Política de los Estados Unidos Mexicanos y de la ley.

Eso es algo importantísimo, ¿qué nos está diciendo? Que el derecho a la protección de datos personales, aunque sea un derecho humano no es ilimitado, tiene también sus límites establecidos en otras leyes, tiene también esos límites, esas fronteras, por ejemplo, en materia de transparencia o en materia de otros derechos humanos en los que podamos estar pensando.

Obviamente este derecho ha ido evolucionando en diferentes lugares alrededor del mundo, diríamos obviamente que la Unión Europea ha sido la que de alguna manera comenzó con este derecho a la protección de datos personales como tal en el marco del Consejo de Europa donde, pues como perfectamente saben ustedes, el año pasado México ha sido invitado a poder acceder al Convenio 108 del Consejo de Europa y que tendrá importantes implicaciones para el país en materia de protección de datos personales, es más, es un paso más en esos compromisos internacionales que tiene México en materia de protección de datos personales y que incluso podríamos considerar como un avance más, incluso, para llegar al nivel adecuado de protección de datos que confiere la Unión Europea, en su caso.

Conozco cuáles son mis derechos en protección de datos personales y cómo ejercerlos, pues obviamente esto es algo de lo que también podemos pensar, justo en estos días, ya que tengo un derecho a acceso de rectificación, de cancelación, de oposición, incluso, si vamos viendo van surgiendo nuevos derechos, o por ejemplo, ahora en la Unión Europea más que los derechos ARCO deberíamos poner ya abiertamente una manta con todos los derechos que tenemos, portabilidad, limitación del tratamiento, bloqueo, decisiones individuales automatizadas y perfilado, que ya lo teníamos de alguna manera, pero que se suma a esos derechos ARCO que ya conocíamos.

Y obviamente, cómo ejercerlos, esto también implica que tenemos obligaciones, desde el punto de vista del usuario, les dije: “No les voy a hacer preguntas complicadas”, pero obviamente se me ocurriría preguntar quién no ha utilizado alguna vez de manera irresponsable internet. Bueno, si quieren le damos la vuelta, quién lo ha utilizado de manera irresponsable, empiezo yo mismo, me autodeclaro culpable.

Todos alguna vez hemos dado más datos personales de los que podría hacer falta para obtener un servicio, todos o casi todos alguna vez hemos podido no entender y directamente dar algo a cambio de algo que se nos ofrecía como gratis, que posteriormente veremos.

Incluso, alguien alguna vez ha podido llegar a responder a un correo electrónico de los que tienen una intención de robar datos personales, de *phishing*, yo, por ejemplo, preparando esta presentación la semana pasada, les puedo reconocer que recibí un correo electrónico del Servicio de Administración Tributaria de México y estaba en España, obviamente rápidamente pude ver que no tenía los cuatro circulitos azules del SAT y entender que eso era un intento de *phishing*.

Esto también nos llevó a plantear que no estamos hablando sólo del derecho a la protección de datos personales en internet en México, sino que es una cuestión que supera cualquier frontera física en la que podamos pensar y que veremos que hay diferentes actores y diferentes implicaciones, incluso les diría: “Qué bueno que me tocó hablar de protección de datos personales en internet y no la protección de internet como tal”, eso se los dejo para mayo, en mayo que es el Día del Internet, ahí creo que tendrán oportunidad de hablar de ese tema.

Pero que está vinculado también, luego veremos que el gobierno de la privacidad, el gobierno de la protección de datos personales o esa privacidad, esa protección de datos personales es parte del gobierno de internet como tal, del funcionamiento de internet.

Es más, si me lo permiten, piensen que internet es un invento estadounidense que en materia de protección de datos personales está siendo fuertemente regulado por la Unión Europea y que utilizamos todos, o sea, incluso cuando ustedes están regulando en materia de protección de datos personales, están aplicando también

ese estándar de protección de datos personales a lo que está ocurriendo en internet, a esos tratamientos de datos personales.

¿Qué hago para proteger mis datos personales? Utilizo internet sin más y doy todos los datos que me piden siempre, establezco algún tipo de medidas que me permitan proteger mis datos personales, es más, piensen y recuerden siempre que tenemos una Ley de Protección de Datos Personales, pero que quien se protege realmente es al titular de los datos personales, cuando se están estableciendo mecanismos para esa protección de esos datos personales, realmente de lo que se trata es de proteger a la persona física como tal y obviamente me tengo que plantear si utiliza algún tipo de herramienta que pueda permitirme hacer un uso anónimo de internet, es otro de los grandes temas que se podría plantear, tengo derecho a hacer siempre un uso anónimo de internet o hay límites a ese uso anónimo de internet porque unas autoridades policiales o judiciales necesiten acceso a esa información, pues son otros de los límites que hay que considerar en ese caso.

Y, por último, el uso constante de mis acciones en internet, vuelvo a insistir en estos ejemplos, como hoy es viernes, a la mejor se acuerdan de mí el lunes, espero que no suban muchas fotos a Facebook de lo que hicieron en el antro esta noche o mañana.

Y no es sólo, soy consciente de mis acciones, siempre se ha hablado de que vamos dejando una huella, pero tenemos que empezar, creo, a ser conscientes de que esa huella también en muchas ocasiones es una evidencia de qué hemos hecho en internet e incluso, como les decía antes, el anonimato tiene límites y no me puedo escudar en ese anonimato, pues para cometer, por ejemplo, un delito y si estuviera haciendo uso de internet puedo estar dejando una prueba, una evidencia de qué es lo que hice en internet en ese caso.

A nivel internacional, simplemente me gustaría apuntarles rápidamente tres documentos de ámbito internacional, que pueden ser de interés porque reconocen el derecho a la protección de datos personales, además de la privacidad en internet.

El primero de ellos es una guía para usuarios, una guía, perdón, derecho derechos humanos para usuarios de internet elaborado en el

marco del Consejo de Europa, pues ahora que México accede al Convenio 108 del Consejo de Europa, quizá esta guía cobra todavía más interés. Otro de los documentos sería de políticas públicas en el ámbito de la OCDE.

Y, por último, la Carta de Derechos Humanos y Principios de Internet, si vamos simplemente al índice de los tres, como verán, en los tres encontramos la protección de datos personales y la privacidad y quizás enunciadas de diferente manera, pero lo importante es que ahí están, tanto el derecho humano o fundamental a la protección de datos personales, como el derecho humano a la privacidad, como les decía antes, el secreto de las comunicaciones electrónicas, por ejemplo.

Si lo aterrizo en el ámbito, perdón, simplemente, lo aterrizo en el ámbito de la Unión Europea, creo que sería interesante comentar aunque sea rápidamente, ayer nos hablaron del Reglamento General de Protección de Datos Personales, obviamente es una norma fundamental en cuanto al tratamiento de datos personales en la Unión Europea y que se aplica a internet, pero tengan también en consideración que más allá de ese Reglamento General de Protección de Datos Personales actualmente la Unión Europea está trabajando en un Reglamento de Protección de la Privacidad en las Comunicaciones Electrónicas.

Es decir, en la Unión Europea tenemos todavía durante unos meses la directiva del año 95, la 95 barra 46, pero hay otra directiva importante, que es la directiva 2002 barra 58, barras de protección de la privacidad en las comunicaciones electrónicas, que viene a completar ese marco de protección y que derivan a su vez o podremos enlazar con la Carta de Derechos Fundamentales de la Unión Europea Artículo 7, es el derecho a la vida privada o privacidad, en el mismo sentido que hay en México a ese derecho a la privacidad. Y el Artículo 8, que es específicamente el derecho a la protección de datos personales como tal.

Si continuamos, obviamente, cuando nos estamos planteando las cuestiones relacionadas con la protección de datos personales en internet, tenemos que tener en cuenta esa parte de derecho humano o derecho fundamental y que internet también es una plataforma para la

innovación y obviamente ahí tenemos o podemos encontrar una cuestión relativa a si vale cualquier innovación o sólo vale, como entiendo, la innovación que respeta los derechos humanos y los derechos fundamentales.

Obviamente, como les decía antes, si aplicamos de manera sin límites el derecho a la protección de datos personales de una manera absolutista, podemos estar perjudicando la innovación, la economía digital, internet es la plataforma clave para el desarrollo de la economía digital en ese sentido.

Pero obviamente esa innovación tiene que ser responsable, tiene que ser ética y tiene que cumplir con los derechos humanos y con los derechos fundamentales, en concreto, la protección de datos personales. Es posible encontrar ese equilibrio y es importante buscar siempre ese equilibrio.

Si me permiten hacer una, ir profundizando con una visión más europea de la materia, pues tengan en consideración que el grupo de trabajo del Artículo 29 que se creó en virtud del Artículo 29 de la directiva del año 95 y que con el Reglamento Europeo va a subsistir, pero que se enmarca ya en el Comité Europeo de Protección de Datos Personales con la participación del supervisor europeo de protección de datos personales, si ven la fecha del documento, en este documento del año 1999; es decir, estamos hablando de hace casi 20 años, el grupo de trabajo del Artículo 29 ya hacía referencia a que internet no es un vacío jurídico, esa declaración es importante y no es una declaración que va a quedar sin contenido.

Obviamente en la Unión Europea se ha trabajado desde hace años en aplicar las normas de protección de datos personales a internet, en este caso, y a todo tipo de tratamiento de datos personales que se lleve a cabo en internet.

Otro documento importante y de nuevo de hace 20 años, es este documento del grupo de trabajo del Artículo 29, esta recomendación y, además, por favor, pongan un poco en el título el mismo, el tratamiento invisible y automático de datos personales por software y hardware que obviamente podemos aplicar a internet, en este caso.

Y hemos dado una clave, lo fundamental que es informar al interesado el tratamiento de sus datos personales, informar a la persona física de que se van a tratar sus datos personales cuando estamos haciendo uso de internet.

Desde el momento mismo que abrimos el navegador y ya incluimos una dirección URL, ahí ya se está produciendo un tratamiento de datos personales, que incluso podemos no estar viendo, el grupo de trabajo del Artículo 29 en otros documentos se refiere a ese tratamiento incluso como el charloteo entre navegadores, cuando yo solicito ver una página web ya se está produciendo un intercambio de información, un envío de información al servidor correspondiente que puede llegar, incluso, datos personales relativos a mi persona como, por ejemplo, el lenguaje en el que se tiene que presentar el contenido correspondiente o que se está buscando ese contenido.

Si vamos a dimensionar a quién implica o a quiénes están involucrados en el derecho fundamental o derecho humano a la protección de datos personales. Una primera estadística que, aunque quizás no sea la más precisa, pero si buscamos en internet el número de usuario de internet, nos da que en México, ahí tienen la fuente, habría 85 millones de usuarios. Creo que está sobredimensionada, pero bueno, puede ser una referencia interesante para ver que México es uno de los países en América Latina que está incluso en el top ten de los países a nivel mundial en cuanto al uso de internet. Eso quiero decir que tiene implicaciones fuertes.

Obviamente esos 85 millones o 70 o 65, pues si lo comparamos con cifras, por ejemplo, de Facebook de 2 mil millones de usuarios, es poquito, pero es uno de los países alrededor del mundo que más usuarios de internet tiene y obviamente hablar de protección de datos personales en internet tiene importantes implicaciones en ese caso.

Yendo a las cifras del INEGI publicadas a través de internet, ayer el Comisionado Luis Sánchez Nava daba unas cifras que creo que están más actualizadas que las, son las últimas y no las que tiene publicadas INEGI en internet, pero si vemos ésta, vemos que en 2016 en México había 65 millones de usuarios de internet, si no recuerdo mal, ayer se dijo que son 70, es decir, entre 2016 y 2017 ha aumentado, se ha incrementado en 5 millones de usuarios. Pero

vamos a referirnos a ésta del año 2016, que creo que podemos extrapolar porque habrá una cierta continuidad en el crecimiento del número.

Bueno, 65 millones de usuarios, luego veremos en el caso específico de estos por grupos de edad, según el uso de internet, pues con el INEGI éstos serían los resultados relativos a 2016. Me imagino que en el mes de abril, es decir, dentro de tres meses el INEGI actualiza esta información a través de internet y van a estar disponible las cifras relativas a 2017.

Y ahora viene lo importante, si vemos esas tablas que les he presentado antes y las empezamos a analizar, pues veremos que en los usuarios menores de edad en México, sean 65 o 70 millones, representan casi el 30 por ciento de la población, es decir, son un grupo muy representativo de usuarios de internet, ahí tienen 29.4 de los usuarios de internet en México tienen entre seis y 17 años; obviamente, eso quiere decir que prestadores de servicios de la sociedad en información o cualquier tipo de prestador de servicios debe poner también atención a ese rango de usuarios de internet, incluso, pensemos en los 13 años, no voy a entrar ahora en cuestiones de la Unión Europea donde el Reglamento General de Protección de Datos, pues les está diciendo a los estados miembros que dejen que sean 13 o 16 años, decide tú en su caso, pero sí tendríamos que ver esa edad de seis a 17 años, en este caso.

Incluso, si me lo permiten, en México una anotación sería la normatividad de protección de datos personales no dice nada específicamente sobre a partir de qué edad puedes dar tu consentimiento, si fuésemos a España, actualmente son 14 años, con el Reglamento lo vamos a dejar en 13, pero en México no hay una o yo no he encontrado una edad concreta dentro de la normatividad.

En cuanto a los tratamientos de datos personales, lo que nos muestra, obviamente y obviamente sabíamos, esto quizás es obvio, que esos tratamientos de datos personales eran, tanto por parte del sector privado, redes sociales, servicios de nube, correo electrónico o cualquier servicio que puedan, en el que puedan prestar, como también por parte del sector público y en este caso, pues llamo la atención sobre ustedes mismos, cómo siendo ustedes parte de sujetos

obligados se lleva a cabo también un tratamiento de datos personales en internet.

Y lo último, obviamente, que año a año se va aumentando o va aumentando el número de transacciones electrónicas, pues por ejemplo, aquí en materia de comercio electrónico, pues aumentó de 2015 a 2016 un 6.2 por ciento y eso también es llamativo en cuanto, obviamente, qué tipo de transacciones se está haciendo y los tratamientos de datos personales a los que se pueda llevar a cabo, desde comprar un boleto hasta simplemente, pues consultar información en páginas web, puede ser, obviamente, ese tipo de tratamiento.

Muy rápidamente, algunas cuestiones sobre la protección de datos personales en internet, pues obviamente, tendríamos los identificadores únicos y de seguimiento, luego veremos un ejemplo, obviamente, cuando entramos en internet, pues si no estoy utilizando ningún tipo de herramienta o de navegación privada, como me ofrecen algunos buscadores, se puede estar haciendo ese seguimiento de la persona, incluso, cuando entro a comprar en un comercio electrónico, el responsable de esa página puede que esté rastreando todos mis movimientos a través de su página web.

Vuelvo a lo de antes, recomendación del grupo de trabajo al Artículo 29, los tratamientos invisibles en internet. Quizás no somos conscientes de que cuando entro a una página web, cada uno de mis seguimientos están siendo monitorizados por el sitio web de comercio electrónico para luego mejorar sus productos y/o servicios o incluso también para enviarme publicidad que pueda estar obviamente vinculada a mi perfil como tal, ese perfil que han ido construyendo con mis movimientos en internet.

Los tratamientos invisibles a los que me acabo de hacer referencia. La transparencia, luego veremos qué significa esta transparencia, no es transparencia en el sector público, es transparencia aplicada a cualquier responsable del tratamiento que está tratando datos personales en internet como tal.

Transparencia aplicada también a las empresas, y ahí si me lo permiten, pues de nuevo, Reglamento General de Protección de Datos

de la Unión Europea, un nuevo principio que no teníamos como tal hasta este Reglamento, la transparencia en cuanto a las condiciones en las que se está proporcionando la información a desinteresados. Lo que quiere la Unión Europea es que quien está tratando datos personales en internet, lo haga de manera transparente y dé la información de manera transparente.

Incluso, yo iría más allá, cuando utilizamos cualquier servicio de internet, es bueno también que sepamos qué va a hacer esa empresa con mis datos personales. Es decir, si los utiliza para llevar a cabo su negocio, podría haber empresas en internet que obviamente sus ingresos vienen dados por el licenciamiento de software y puede haber otras que realmente sus ingresos vienen dados por la publicidad y para poder conseguir esa publicidad necesita muchos más datos personales de los usuarios en cada caso.

La información, los avisos y políticas de privacidad. Quizás ya conocen el dato, en el caso de Estados Unidos, de que para poder leer todos los avisos y políticas de privacidad que se me presentan cuando navego por internet, necesitaría 73 días al año; o sea, ahí ya les pregunto, ¿tienen 73 días al año para leer todos los avisos y políticas de privacidad? Yo personalmente no, voy leyendo las que voy haciendo y poco más.

El consentimiento. El consentimiento como uno de los principios clave, que ya se ha hecho referencia también aquí el día de ayer, al interés legítimo, al consentimiento, pero el consentimiento como una cuestión a considerar, en cuanto, incluso, a si es el principio más adecuado o cómo aplicar el principio.

Las Naciones Unidas en un estudio en materia de protección de datos personales ha llegado a decir expresamente que puede ser un problema tanto para el usuario, porque al final no saber realmente qué está consintiendo o cómo está consintiendo, como para la propia empresa que trata datos personales porque puede ser difícil probar la obtención de ese consentimiento.

De nuevo cuña europea, por eso dice el Reglamento General de Protección de Datos Personales que ahora ya no vale el consentimiento tácito y que hay que buscar siempre algún tipo de

acción positiva o activa por parte del usuario para poder obtener ese consentimiento. Es un cambio importante.

El derecho a la supresión al olvido. Bueno, pues ahí simplemente lo dejo apuntado, el derecho al olvido pues creo que ya conocen suficientemente la materia y no obstante se volverá a dar este derecho al olvido con sucesivas cuestiones que se plantean en el Tribunal de Justicia de la Unión Europea, incluso, si se aplica a buscadores o a dominios fuera de la Unión Europea.

Los menores y otros grupos vulnerables. Obviamente, los menores pueden ser un grupo vulnerable porque pueden no tener ese conocimiento de los riesgos a los que se exponen y es necesario obviamente ayudarles.

Pero grupos vulnerables, hoy todos aquí somos todavía muy jóvenes, pero cuando pasen unos años, a lo mejor entramos en un grupo vulnerable, porque no comprendemos realmente esos avisos de privacidad o de determinada información, el perfilado, los datos masivos y la propiedad de los datos personales como tal y por último la seguridad.

No sé si gustan una galleta, perdón, ya sé que la hora es complicada, me referí antes a la cuestión de los identificadores únicos, siempre estamos pensando en las cookies, siempre hemos leído eso de las cookies, pero empezamos a olvidarnos de las cookies porque puede haber otros identificadores únicos que, incluso, permitan obtener más información que a través de una cookie.

Es más una cookie la puedo utilizar simplemente para cuestiones técnicas o administrativas que son necesarias para configurar la página web o por temas de seguridad, la puedo utilizar para hacer ese seguimiento o ese perfilado de la persona para enviarle publicidad, pero puede que, incluso, lleguemos a otros, y de hecho estamos ya ante otras técnicas de rastreo del usuario en internet, como pueden ser este *canvas fingerprinting* que simplemente abro mi navegador y cuando estoy abriendo el navegador ya se está produciendo ese intercambio de información, invisible para mí, pero que me está identificando de manera unívoca en ese caso.

Tres partes involucradas, aunque vean estas tres partes, yo les diría, y una cuarta son ustedes como sujetos obligados por lo que dije antes, cada vez que tratan datos personales en internet tienen que cumplir con esas obligaciones para hacer efectivo el derecho humano a la protección de datos personales en este caso.

Las autoridades garantes, obviamente, pues el InfoDF, por ejemplo, los usuarios y usuarias, que podemos ser tanto ustedes como yo y los proveedores de servicios. Si nos vamos centrando en cada una de ellas, pues tienen sus obligaciones también en esta materia.

Si me permiten, simplemente, en el caso de las autoridades garantes. Conocer las implicaciones interrelaciones que se plantean en este caso, la autoridad garante obviamente tiene que estar estrechamente vinculada al día a día, conocer esas tecnologías, conocer esos tratamientos de datos personales que se están llevando a cabo, ¿por qué? Porque van a ejercer sus funciones, en el caso de los responsables del tratamiento, y obviamente van a tener que conocer esa realidad.

La tecnología avanza mucho más rápido que la ley, incluso, la ley no puede regular absolutamente todo porque, incluso, podría tener efectos contraproducentes, pero sí es necesario conocer esas implicaciones y más allá del legislador, pues obviamente también la autoridad garante.

Promover códigos de conducta y certificaciones puede ser una buena práctica en un ámbito en el que obviamente todo evoluciona muy rápidamente.

Colaborar con todas las partes interesadas en cualquier tipo de acciones, pues obviamente las autoridades reguladoras y las autoridades garantes tienen que estar próximas o cercanas a que está haciendo la industria, conocer las buenas prácticas de la industria, pero también escuchar a los ciudadanos como tal, en el sentido de poderles dar consejo.

En ese sentido, el InfoDF da múltiples consejos muy prácticos, aplicables en el día a día de la navegación en internet para hacerlo de manera segura, en este caso.

Desarrollar y mantener esas acciones a lo largo del tiempo, no es sólo una acción de una vez o en un momento determinado, sino mantenerlas en el tiempo y obviamente también se tiene que plantear esa cooperación internacional entre autoridades de protección de datos personales que sí va ocurriendo cada vez más, por ejemplo, en el foro de la OCDE.

¿Qué están haciendo algunas autoridades de protección de datos fuera de México? Por ejemplo, el último en relación con internet sería que el Grupo de Trabajo al Artículo 29 sea dirigido a la ICANN, que es de alguna manera quien está gestionando el uso de internet; y los directorios WHOIS, son aquellos directorios en los que yo puedo consultar quién es la persona que ha registrado un nombre de dominio.

Lo que le está diciendo el Grupo de Trabajo del Artículo 29 al ICANN en esta carta, que me he permitido anonimizar, por si acaso un poquito, pero que la tienen disponible en internet, simplemente lo que le está diciendo es: “Oye, tienes que cumplir con el Reglamento General de Protección de Datos Personales y busca una base de legitimación del tratamiento para la publicación de los datos personales en los directorios WHOIS”, porque obviamente se están publicando actualmente pero podrían no estar haciéndose de manera adecuada en este sentido.

Si pensamos en nosotros mismos como usuarios o usuarias de internet, obviamente, lo primero es hacer un uso responsable. Ya les puse antes mi ejemplo, hacemos usos irresponsables dándonos cuenta o no porque damos más datos de los necesarios, obviamente, nos vamos poniendo en riesgos, si doy más datos de los necesarios pues a lo mejor luego posteriormente se utilizan con fines inadecuados.

Proteger nuestros datos, conocer el significado y el alcance del derecho como tal, ejercer nuestros derechos de manera responsable también y conocer, obviamente, qué es lo que hacen las autoridades garantes y quiénes son esas autoridades garantes.

En el caso de los proveedores de servicios, obviamente, pues considerar al principio de protección de datos personales desde el diseño y por defecto.

Aplicar ese principio de minimización de los datos personales. A mí me llama mucho la atención cuando, por ejemplo, entras en algún sitio de comercio electrónico, vas a comprar y te dice que quiere guardar el número de tu tarjeta de crédito para el futuro y yo le diría: “Permítame que le envíe, a lo mejor, una carta diciéndole que se hace usted totalmente responsable, que en el caso de sufrir un severo ataque en el que se lleve mis datos personales, pues me va a tener que indemnizar de alguna manera”.

Adoptar e implementar esas medidas técnicas y organizativas para cumplir con el principio de responsabilidad demostrada, el doctor Remolina que está aquí, creo que les hablará posteriormente de este principio también.

Proporcionar información de manera clara y transparente, y ahora veremos qué significa y actuar conforme al principio de responsabilidad.

En cuanto al valor económico de los datos personales, les he querido traer una referencia porque es la única que he encontrado por el momento de la Unión Europea. La Comisión Europea en ese documento, en ese documento que tienen aquí llegó a decir, el año pasado, si no recuerdo mal, sí, en 2017, que el valor económico de los datos personales de los europeos estaría cercano al trillón de euros anuales en el año 2020.

Simplemente quise tener la referencia porque esto me va a permitir introducirles algunas preguntas que son para reflexión y que creo que pueden ser interesantes.

¿Qué precio tienen los derechos humanos? Estamos hablando del derecho humano a la protección de datos personales, ¿pagarían ustedes porque protejan su derecho humano a la protección de datos personales? Por ejemplo, en Estados Unidos se plantea que el tema de la privacidad puede ser algo, casi llegar a ser un producto de lujo. Yo la verdad que con unos ojos europeos e, incluso, si quieren lo

ponemos desde un punto de vista mexicano o de otros países de Latinoamérica que han seguido esa aproximación europea. El derecho humano a la protección de datos personales no debería estar sujeto a precio ni a condiciones, si empezamos así, podemos ir por mal camino.

En cuanto al valor económico de los datos personales, cuando nos dicen que si no pagas algo en internet, la moneda eres tú, yo la verdad que le daría una vuelta a la pregunta y es, si me ofrecen algo gratis, ¿por qué tengo que pagar por algo gratis? Ni con mis datos ni con nada más o si no, oiga, dígame usted realmente cuál es la contraprestación de lo gratis para que vea si me interesa o no su servicio, o si me interesa o no descargar información.

A veces nos ofrecen informes buenísimos pero requieren tu correo electrónico y determinada información, ¿gratis?, ¿cuántos correos electrónicos con publicidad voy a recibir posteriormente a haber descargado esa información por lo que era gratis? Oiga si es gratis o quita usted el registro o me dices si te registras te voy a mantener informado de novedades y otras cuestiones.

Y como activos económicos el Supervisor Europeo de Protección de Datos Personales, que es una institución de la Unión Europea para los organismos e instituciones de la propia Unión Europea, como Comisión Europea, Parlamento Europeo y otros, se ha llegado a referir en cuestiones de Big Data a que los datos personales no pueden ser considerados un activo económico.

Incluso, si quieren volvemos al principio y debemos tener cuidado porque si sujetamos a precio el ejercicio de nuestro derecho humano a la protección de datos personales, podemos llegar a correr un gran riesgo en el sentido, obviamente, de que si pago o no por algo, a lo mejor puedo llegar acá, puedo acabar siendo discriminado porque me pongan en el lado de los usuarios que no pagan por el producto o servicio frente a los usuarios que sí pagan, que serían los Premium y que obviamente van a tener otra serie de beneficios en ese caso.

Aunque sé obviamente que estamos en un foro que está más dedicado al ámbito público, pero creo que debemos también pensar, por ejemplo, en esta cuestión que plantea el Supervisor Europeo de

Protección de Datos Personales, que la protección de datos personales está vinculada cada vez más, y lo vamos a ver en los próximos años y de hecho ya lo estamos viendo, a cuestiones de derecho de la competencia y de protección de los consumidores.

Es más, les dije: “Qué bueno que estamos hoy en México pudiendo celebrar el Día de la Protección de Datos Personales como derecho humano fundamental”, pero sí deberíamos quizá aprender de Estados Unidos esa aproximación al derecho a la protección de datos personales como una cuestión de los consumidores.

De hecho el papel de la Comisión Federal de Comercio es proteger a los consumidores en su privacidad, pero desde un punto de vista de derecho de los consumidores. Cada vez más se van viendo esas interrelaciones entre protección de datos personales y consumidores, en este caso, y es algo a considerar también porque obviamente tiene implicaciones para nosotros.

Aquí apuntaría, el derecho a la portabilidad, en concreto, en la Unión Europea surge como una cuestión de derecho de la competencia y es para que el usuario no quede vinculado simplemente a un prestador de servicios y se pueda ir, por ejemplo, a otra red social o se pueda ir, por ejemplo, a cualquier otro tipo de plataforma electrónica en ese sentido.

Y si me lo permiten, esta ya es la última, ¿cuáles serían las claves o para mí las posibles claves de la protección de datos personales en internet? Lo primero, el acceso, no el acceso a internet, el derecho de acceso a los datos personales, de hecho, simplemente si volvemos a la Carta de Derechos Fundamentales de la Unión Europea, al Artículo 8 que les cité al principio, si la leen o si tienen oportunidad, verán que cuando se refiere al derecho a la protección de datos personales habla de los derechos de acceso y de rectificación, no dice nada ni de cancelación ni de oposición, el acceso es realmente la clave.

Saber si alguien está tratando mis datos personales para posteriormente poder ejercer otros derechos en ese caso, lo que nos lleva al control, finalmente es el control de la persona, es nuestro control sobre nuestros datos personales, ahí es donde está la base del

derecho a la protección de datos personales, saber quién tiene mis datos personales para qué está tratando mis datos personales.

Y por último, la responsabilidad que creo que es una cuestión totalmente compartida, tanto de los responsables de tratamiento de ser realmente responsables, ese principio de accountability como de nosotros mismos, como usuarios de internet, en el sentido de ver qué medidas aplicamos para protegernos a nosotros mismos cuando tratan nuestros datos personales.

Y por mi parte, nada más, lo dejo aquí para que podamos tener alguna pregunta.

Muchas gracias.

Lic. Luis Fernando Sánchez Nava: Excelente presentación de Miguel, agradecemos su presencia, su acompañamiento con el InfoDF.

Y ya llegó aquí una pregunta por si va a haber más, yo quisiera adelantar, en lo personal, de las implicaciones ahora de la implementación del Reglamento Europeo que tiene para América Latina, porque pareciera que estamos aislados en el mundo y que allá se están tomando normas y acá no estamos haciendo nada.

Yo pudiera poner nada más como ejemplo el tema de los boletos de avión, tan sólo los boletos de avión de empresas aerolíneas mexicanas o de otra parte de América Latina, el tema del resguardo, sobre todo, que los boletos de avión, la mayor parte se compran vía internet y los ciudadanos europeos también tienen que exigir y reclamar que sus datos, que cuando contratan a una empresa o una aerolínea de América Latina tienen que estar resguardados.

No sé qué implicaciones podría, toda vez que va a entrar en el mes de mayo ya, de este año, ¿qué implicaciones tiene el Reglamento Europeo para América Latina?

Dr. Miguel Recio Gayo: Pues es una excelente pregunta y tiene todas las implicaciones posibles porque además el ejemplo es extraordinario.

El Artículo 3 del Reglamento General de Protección de Datos de la Unión Europea tiene una cláusula de extraterritorialidad, se va a aplicar no sólo a las empresas responsables o encargados establecidos dentro de la Unión Europea, sino también a otros responsables de tratamiento establecidos en cualquier lugar del mundo, que estén llevando, por un lado, a cabo un tratamiento de datos personales que implique una observancia habitual de la persona física, pero también aquellos responsables de tratamiento que dirijan sus productos o servicios a la Unión Europea.

Si pensamos en una aerolínea, pongamos, por ejemplo, mexicana que simplemente vende boletos de avión, que no está apuntando hacia la Unión Europea en el sentido de que no hay precios en euros, el idioma aunque sea español, la bandera del idioma es México, los servidores están en México, ahí no habría aplicación del Reglamento.

Quiere decir que un ciudadano europeo o un residente en Europa, que es el término exacto que utiliza el Reglamento, ha accedido a un sitio web de comercio electrónico fuera de la Unión Europea y se va a sujetar a la normatividad de protección de datos, si la hubiere de ese sitio web de comercio electrónico.

Por el contrario, si el sitio web de comercio electrónico que vende esos boletos de avión, es lo que suele ocurrir con las compañías aéreas, pues tuviese, por ejemplo, la bandera de España o de cualquier otro estado miembro de la Unión Europea, ofreciese el precio de los boletos en euros y dijese: "Yo no estoy en la Unión Europea, estoy fuera de la Unión Europea, pero estoy ofreciendo mis productos o servicios bajo estos términos" sí va a estar sujeto al Reglamento General de Protección a Datos Personales, va a tener que designar un representante en la Unión Europea, que será el punto de contacto para las autoridades de protección de datos personales para cumplir con el Reglamento como tal.

Sí que vamos viendo que cada vez se va produciendo más ese intento de aplicación de la normatividad europea, incluso, del estándar europeo de protección de datos personales.

El mismo hecho de que México acceda al Convenio 108 del Consejo Euro podría ser un primer acercamiento, así que por ejemplo este año la Comisionada Europea, aunque no sea América Latina, va a reconocer seguramente el nivel adecuado de Japón y quizá de Corea del Sur.

Y sí pensemos, obviamente, que en México realmente su ley del sector privado es de 2010, su ley de sector público en materia de protección de datos personales, aunque ya había algo en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, es mucho más reciente y sí obviamente, incluso, en la Ley General de Protección de Datos Personales, creo que se ve claramente esa influencia del Reglamento General de Protección de Datos Personales.

Está el punto de que ahí nos encontramos con el derecho a la portabilidad, la evaluación de impacto relativa a la protección de datos personales o incluso la figura del oficial de privacidad, en algunos puntos es determinado que, obviamente, quizá es seguir el Reglamento.

Lic. Luis Fernando Sánchez Nava: Han llegado algunas preguntas, si quieres te las paso, Miguel.

Dr. Miguel Recio Gayo: Una pregunta, que hable de autorregulación pura, ¿lo cree posible en México o su carácter extrajudicial no lo permite? Pues yo diría que México en la Ley Federal en posesión de los particulares y luego en posesión de los sujetos obligados ha implementado, y creo que podrá aprovechar mucho esa posibilidad de autorregulación.

Tenemos que entender la autorregulación como un paso más allá del cumplimiento, es decir, yo soy un responsable del tratamiento, que establezco medidas para cumplir y que ahora voy, además, a complementar con autorregulación.

Tener en consideración que ya está funcionando el registro, el registro, en el caso del INAI para los esquemas de autorregulación, que ahí obviamente esos lineamientos de esquemas de autorregulación

vinculante y creo que México sí ha sabido aprovechar esa oportunidad.

Incluso, lo hace en un doble sentido, quizás, por una parte siguiendo algunas previsiones de derecho de la Unión Europea en materia de protección de datos personales, pero también sin olvidar que es una economía de Asia a Pacífico y que dentro de Asia a Pacífico se impulsa la autorregulación como tal y creo que por ahí, obviamente, se podría aprovechar mucho y que se puede, obviamente, llegar a un buen nivel de cumplimiento.

Qué pasa en un país como México donde la impunidad y la torpeza del Sistema de Justicia son una constante, no resulta perverso defender sin matices los datos personales, que cuando estos datos son de criminales, así como existe el derecho al olvido, existe el derecho de memoria.

Obviamente, cuando estamos hablando de personas físicas pues aplica a toda persona física como tal y, obviamente, pues es una cuestión de protección de un derecho humano como cualquier otro derecho humano al que podemos estar haciendo referencia y obviamente lo que ahí tiene en consideración esos límites a los que me refería anteriormente, en situaciones en las que por ejemplo se puedan tratar de datos personales porque está previsto, obviamente, en un ley y no hace falta el consentimiento.

La siguiente pregunta es, ¿a qué se refiere lo relativo a la naturalidad de la red o de internet? Bueno, la naturalidad del arresto de internet, obviamente, aunque no es una cuestión específicamente de protección de datos personales, lo que quiere decir es no tratar la información que pueda transferirse a través de internet con diferentes criterios. No priorizar, por ejemplo, que una información se pueda transferir mucho más fácil que otra o, incluso, establecer impuestos para una determinada información o los temas de *zero rating* en internet que obviamente, pues tendríamos que ir viendo qué es lo que ocurre y no está resuelto todavía; o sea, sí se había alcanzado, por ejemplo, en Estados Unidos, un acuerdo para garantizar esa naturalidad.

Ahora está en peligro y habrá que ir viendo qué es lo que ocurre en ello, pero obviamente es facilitar que la información, incluso, que los datos personales se puedan mover fácilmente en internet con las garantías, obviamente, suficientes y evitar cualquier tipo de obstáculo que podría tener implicaciones para muchos derechos, en ese caso.

Lic. Luis Fernando Sánchez Nava: ¿Alguien quisiera hacer alguna pregunta de manera personal?, ¿no?

A mí se me hace una pregunta dice, ¿qué está haciendo el InfoDF para resguardar los datos personales acerca de las declaraciones patrimoniales que están en la página denominada Auxiliar Jurídico? Seguramente ya es un tema que haya que presentar una denuncia, pues el InfoDF va a actuar en consecuencia.

Acuérdense que las declaraciones patrimoniales, la fiscal y la de intereses, están establecidas en la ley y se tienen que establecer en los portales a través de versiones públicas.

Si no hay ninguna otra pregunta, agradecer a Miguel por su excelente exposición, que lo seguiremos invitando los próximos años, a lo mejor no nosotros, los próximos Comisionados y entregar un reconocimiento amplio por su participación.

---ooo0ooo---