Medidas de seguridad: Los datos especialmente protegidos

Mesa 7:

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

Los temas que serán abordados corresponden a las medidas de seguridad de los datos especialmente protegidos, a la protección de datos personales en los estados de la República Mexicana y a la presentación de los trabajos de la Red Iberoamericana de Protección de Datos Personales.

Presídium: María Marván Laborde, Comisionada Presidenta del Instituto Federal de Acceso a la Información Pública; Ricardo Sodi Cuellar, Director de la Facultad de Derecho de la Universidad Anáhuac; Luis Alberto Domínguez González, Consejero del Instituto de Transparencia y Acceso a la Información Pública del Estado de México; José Luis Piñar Mañas, Presidente de la Red Iberoamericana de Protección de Datos Personales; Rolando Barrera Zapata, Consejero Presidente del Instituto de Transparencia y Acceso a la Información Pública del Estado de México.

Ricardo Sodi Cuellar.

Es para la Facultad de Derecho de la Universidad Anáhuac, un verdadero privilegio ser sede alterna de este Encuentro Iberoamericano de Protección de Datos Personales, ya que ha sido preocupación de nuestra institución académica, crear espacios de reflexión y análisis de temas tan señalados y de tanta vanguardia, como lo es la protección de datos personales, el derecho a la información, el derecho a informar.

La Universidad Anáhuac y su Facultad de Derecho han establecido varias líneas en este sentido. En primer lugar dentro del programa curricular de nuestra Facultad de Derecho contamos con la materia de Derecho Informático, una novedad que nos pone a la vanguardia académica en este campo de derecho.

Asimismo, en nuestro Instituto de Investigaciones Jurídicas se ha creado una línea de investigación en torno al derecho informático, a la protección de datos personales y la regulación jurídica. De hecho hemos participado con universidades europeas y norteamericanas en el tema relacionado con la protección de datos personales, concretamente el doctor Emilio, de la Universidad Complutense de Madrid, el doctor José Antonio Núñez Ochoa, Director de nuestro Instituto de

Investigaciones Jurídicas han realizado y realizan varias investigaciones en torno a la protección de datos.

Por ello, la Universidad Anáhuac se congratula de tenerlos el día de hoy en sus instalaciones y la Facultad de Derecho considera esto como un día de gran trascendencia para su historia académica, toda vez que crear esos espacios de reflexión en torno a la protección de datos personales, en torno al derecho informático, al acceso a la información es una prioridad de nuestra formación académica.

Les agradezco mucho su presencia, sean ustedes muy cordialmente bienvenidos a la Facultad de Derecho de la Universidad Anáhuac. Espero que disfruten los trabajos de este Encuentro y que sean muy exitosos.

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

Como ha sido ya la mecánica de este evento, vamos a proceder a una Conferencia Magistral a cargo del doctor José Roldán y, posteriormente tendrán su intervención cada uno de los participantes de este panel, que en este momento solamente enumero, María José Blanco Antón, la doctora Marván Laborde, Abraham Sotelo Nava, Enrique Domville y Cédric Laurant.

Iniciamos entonces con esta conferencia magistral del doctor José Roldán de quien brevemente diré algo de su extenso currículum, es un académico reconocido, es licenciado en Derecho por la Universidad Autónoma de Puebla, maestro en Derecho Económico por la Universidad Autónoma Metropolitana, Unidad Xochimilco y, doctor en Derecho por la Universidad Nacional Autónoma de México; ha escrito diversos libros en materia administrativa y sobre otros temas que han sido de su interés y, actualmente es profesor de tiempo completo del Departamento de Derecho del ITAM, titular de la materia de Derecho Administrativo y se desempeñó además como director de la licenciatura en Derecho.

Conferencia Magistral: José Roldán Xopa

Agradezco su gentileza en haberme invitado a ésta que pretenciosamente se llama conferencia magistral; sin embargo, creo que es un buen momento para pensar y procuraré que podamos hacer un ejerció colectivo de pensamiento, tomando en cuenta el estado del arte de la cuestión en nuestro país.

Para nosotros, incluyéndome, resulta novedoso el que comencemos a hablar de un nuevo tema que anteriormente nos parecía hasta cierto punto lejano, pero que con la presentación que diversas iniciativas legislativas en el Congreso sobre la materia nos obliga a pensar mucho más detenidamente y por supuesto en la medida en que vamos entrando al problema vamos, por una parte, en un proceso de conocimiento, pero por otra parte también nos van suscitando diversas pregunta.

Primer punto de entrada, nos importa cada vez que regulamos algo nuevo que la regulación sea efectiva, esto es, que efectivamente, que realmente en la sociedad se provoquen las consecuencias que tiene la intención.

Puede haber muy buenas intenciones, pero si están mal instrumentadas entonces seguramente el resultado va a hacer ineficaz, no se va a lograr lo que se busca.

¿Cuáles serían las condiciones para llegar a tal objetivo? Yo creo que en primer término que la materia se encuentre bien definida. Esto es que se encuentre debidamente precisado qué es lo que se quiere, cuál es el bien que se está tutelando, y por otra parte, además, de la buena definición de la materia, que tengamos una buena organización institucional que instrumente el derecho, que proteja el derecho, que procure el cumplimiento de obligaciones, y por tanto también que tenga un buen sistema de cumplimiento de forzamiento de las conductas debidas.

El siguiente punto es: ¿Entonces de qué estamos hablando cuando oímos el término de datos especialmente protegidos o datos sensibles?

Procuraré hacerlo de una manera muy simple, si en términos generales el término que nos convoca a este seminario es el de la protección de los datos personales, cuando se habla de datos sensibles o datos especialmente protegidos.

Existe una previsión de qué es lo que se considera como datos sensibles. Y lo que dice el proyecto del artículo 19 para que todos podamos compartir esta información, dice: *Ningún titular estará obligado a proporcionar datos sensibles que le conciernen*; y posteriormente dice, *los datos sensibles únicamente podrán ser objeto de tratamiento cuando se cuente con la autorización vigente y por escrito del titular otorgada mediante su firma autógrafa, salvo lo dispuesto en equis artículo*.

Lo que nos está diciendo este artículo es que hay un conjunto de informaciones que está sujeto a una regulación especial.

¿A qué se refiere esto de los datos sensibles? En la Ley, en el Capítulo de Definiciones nos remite a datos tales como la salud, la raza, las preferencias sexuales que, por lo que ustedes pueden ver, presenta una calificación respecto de la valoración o de la posición social del individuo en una sociedad que pudiera dado el contexto de presentar alguna circunstancia particular.

¿Por qué pudiera ser sensible el dato?

La sola expresión de que se hable, por ejemplo, o que se refiera a preferencias sexuales o bien a la salud o a la raza, implica que tal información tiene determinada valoración en una sociedad.

Por tanto, el primer punto, creo, es que el dato sensible depende del contexto en el cual viva el individuo y, por tanto, los datos podrían ser relevantes y ameriten una determinada protección.

En este caso la protección se refiere a un elemento importante que es: No se puede dar a conocer ningún dato que pueda comprenderse dentro de esto, si no es con la autorización de la persona, de su titular, de a quién se refieren los datos.

Lo que podemos ver es una especie de soberanía del titular respecto de la información que le concierne, dependiendo del contexto en el cual se vaya desarrollando.

El primer problema es: ¿Cuáles son estos datos sensibles, cómo se determinan?

Hay un primer problema en la ley. La ley es enunciativa, dice: *Raza, preferencias sexuales, salud, otros y aquéllos que por disposiciones generales determine el órgano encargado de la regulación*.

Por tanto, aquí nos da una puerta, una abertura para que no sea un *númerus clausus*, sino que a través de una decisión administrativa de un órgano regulador se pueda extender el tipo de datos que pudieran ser protegibles. Esto nos plantea una serie de problemas.

Aquí viene entonces la cuestión de la técnica alrededor de la cual se va precisando qué es el dato sensible. Hay una definición legal y, por tanto, después habría una definición administrativa, lo cual crea una serie de problemas normativos.

Voy a entrar a alguna de estas definiciones.

La protección, en buena medida, está encomendada a un órgano regulador. La iniciativa es, hasta cierto punto, ambigua; a veces plantea que puede ser el IFAI o bien algún órgano regulador especializado en esto.

El problema de diseño institucional creo que tiene que entender dos cuestiones: Primero, que los sujetos regulados, si es que tomamos el modelo IFAI, no serían ya la clientela habitual del IFAI, que son entidades públicas, sino que

también serían entidades privadas, lo cual amplía no solamente la clientela, sino que además complica la ordenación, porque en la medida en que hay una relación o bien al interior de la administración o al interior de la organización estatal y al ampliarlo a los particulares, entonces, esto significa que hay una relación externa y, por tanto, la regulación jurídica también es diversa.

Porque las regulaciones jurídicas funcionan de manera distinta cuando el sujeto obligado es un sujeto público, porque hay un relación institucional especial, que no es una relación institucional en donde el sujeto obligado goce de derechos, pero en cambio sí lo es cuando el sujeto obligado, el sujeto regulado es un particular y, por tanto, su posición como gobernado, como administrado, activa una regulación especial y, por tanto, también los medios de defensa y las formas de actuación son distintas.

No operaría de la misma manera una norma general del IFAI que regule esta materia, frente a sujetos públicos que frente a sujetos privados. La exigencia frente a sujetos privados es mayor.

Por ejemplo, podría haber una oposición en el sentido de que la regulación de cuál puede ser el dato protegible debe ser hecho en ley y no por acción administrativa, lo cual evidentemente no podía ser oponible en el caso de instituciones públicas, porque la relación jurídica distinta. Y, por tanto, hay una diversidad de instrumentos y éstos operan de distinta manera si es frente a un particular o frente a una institución pública.

Allí hay que tener mucho cuidado en lo que podría expresarse como una simetría regulatoria.

El siguiente punto es la simetría regulatoria también puede estar complicada debido al tipo de derecho que se cree con la información.

Si un particular argumenta que respecto de la información tiene un derecho patrimonial, entonces el argumento de que se requiere una ley para que pueda consignarse qué dato es el protegible adquiere mucho mayor fuerza. Estoy simplemente señalando problemas.

La siguiente cuestión es el tratamiento, le hace la revelación de la información del dato sensible, está, como ustedes pueden ver establecido como una regla general, solamente con la autorización de su titular puede ser dado a conocer. Este es el principio, que me parece un buen principio, pero sin embargo, tenemos que pensar y preguntarnos respecto de si esto es absoluto.

El propio proyecto establece ya un indicio o un inicio de que esto puede ser relativo en el caso de revelación de datos médicos, esto es, si se requiere para una cuestión de salubridad general o bien de tratamiento específico en la persona puede accederse a esta información.

El ejemplo que me parece muy revelador es el siguiente: Supongamos que una persona llega a un hospital, a urgencias, está inconsciente y, por tanto, no está en condiciones de revelar la información necesaria para el médico, pero el médico requiere llevar a cabo una transfusión sanguínea; entonces, el conocimiento del dato, por ejemplo, de la religión puede ser relevante para el tratamiento, si un Testigo de Jehová, bueno, el médico tiene que enfrentarse al dilema de si opera con una transfusión sanguínea o bien busca otro tratamiento médico alternativo para poder salvar esta objeción, derivada de la religión.

Entonces, suena justificable que haya ahí una salvedad a la necesidad de una autorización previa.

Pero la ley dice que se requiere la firma autógrafa, lo cual plantea un problema de manejo de administración del tratamiento de los datos, a diferencia de lo que pasa con la consignación del tipo de datos que pueden ser regulados en una disposición administrativa, me parecer por ejemplo más razonable que los instrumentos, incluyendo los tecnológicos para poder salvar la autorización con métodos

alternativos a la firma autógrafa podrían ser más propios de una regulación por vía administrativa, tomando en cuenta los avances de la tecnología. Sin embargo, esta es una cuestión que tendría que darse en la discusión.

La pregunta y aquí confieso hasta cierto punto mi limitación de información, solamente en este caso se justificaría una salvedad al monopolio de la autorización autógrafa o pueden existir otras buenas razones para establecer, por ejemplo, que mediante autorización judicial o de alguna otra autoridad diversa a la judicial pueda tratarse, relevarse una información relativa a datos sensibles.

Yo me planteo, por ejemplo, el problema de la raza. En México a partir de la reforma al artículo 2 Constitucional, se establece la raza como un elemento importante para la determinación de determinadas situaciones jurídicas, la incorporación del derecho indígena, el reconocimiento de los pueblos indígenas implica que la raza es relevante para determinadas situaciones, ligadas a obligaciones, a derechos, a preferencias.

La definición de quién es un indígena es por sí misma muy problemática y además es costosa, puede ser algo así como la prueba del diablo. En México con los índices de mestizaje indígena es una cuestión problemática y cara y que en ocasiones no puede ser costeable cuando se va desahogando un procedimiento.

Entonces, ahí puede ser relevante la posibilidad de acceder a una información que puede estar en algún banco de datos público o privado que pueda resolver el problema.

El dato de ser indígena o de ser de otra raza no necesariamente importa o puede no ser viable a través de la autorización de su titular, es más, su titular puede oponerse a que se conozca esa información, pero esa información puede ser relevante para la determinación de una situación jurídica, por ejemplo, para el establecimiento de un agravante cuando se comete un delito.

Si esta información para no acudir a un peritaje médico que puede ser sumamente caro de DNA, por razón de economía de información puede solicitarse a través de algún medio a pesar o en contra de la no autorización del titular.

Nos van surgiendo una serie de problemas que creo que es importante que los vayamos pensando.

Y finalmente es: ¿Qué mecanismos son los que el proyecto de ley prevé para poder tener un adecuado cumplimiento de este tipo de cuestiones?

Partamos de lo siguiente, en la medida en que hay un ordenamiento que regula los datos personales, se lleva a cabo una operación en la cual se excluye del mero manejo de los particulares, y considerando que puede ser una situación de interés público, por tanto, se activa la posibilidad de intervención de órganos administrativos.

Y, además, que la infracción a los deberes tiene como consecuencia la imposición de multas o de sanciones públicas. Esto es, hay una exclusión del menor manejo de relaciones contractuales o defensa o extracontractuales de particulares.

Estamos frente a una cuestión de orden público, en donde la sola infracción, por sí misma, amerita una sanción. Pero la infracción a los deberes de cuidado de los datos personales también puede ocasionar daños particulares.

La pregunta aquí sería: ¿Cuál es la mejor forma o las formas de garantizar un adecuado cumplimiento de deberes?

La ley establece dos tipos de sanciones. Primero, una multa que evidentemente no va a beneficiar al particular. Ni un peso de la multa puede llegar a su bolsillo, pero por otra parte la posibilidad de indemnización si es que hay daño.

Me parecen buenas, me parecen razonables, en principio, estos dos instrumentos. Sin embargo, yo creo que puede quedarse corto. La revelación

de un dato sensible puede ocasionar daños, y por tanto genera la acción de daños y perjuicios. Pero no necesariamente puede generar daños. La revelación de un dato personal puede, inclusive, originar un beneficio a la persona, a su titular, puede darse ese caso. Pero no obstante se violó el deber de cuidado.

Si es así, y si no hay daño, ¿habría alguna acción que tiene el titular, aunque haya sido beneficiado o no haya sido dañado para exigir o pedir una indemnización por el incumplimiento del deber de cuidado de quien tenía ese dato privilegiado o no? Yo sería partidario de que podría intentarse una vía, porque de todas maneras hay una afectación a su decisión de que ese dato no se dé a conocer, independientemente si le origina daño o no.

El siguiente punto, y con eso concluyo, es cómo está diseñada la sanción administrativa. De acuerdo con el proyecto hay una sanción de 5 mil a 10 mil salarios mínimos. La única consideración que hago es que esto nos plantea siempre decisiones de costo-beneficio. Esto es cuánto va del dato personal, el dato sensible.

¿El dato sensible puede valer más de 10 mil salarios mínimos? Yo creo que sí, podría darse el caso de que valiera más. Si vale más entonces la sanción está mal diseñada, ¿por qué? Porque no es un adecuado instrumento para poder inhibir o para poder sancionar una práctica de este tipo.

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

Voy a darle la palabra a María José Blanco Antón, quien es licenciada en Ciencias Matemáticas por la Universidad Autónoma de Madrid, pertenece al Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado.

Se ha desempeñado en diferentes puestos en la Agencia Española de Protección de Datos, ocupando actualmente el de Subdirectora General del Registro General de Protección de Datos.

Ponente: María José Blanco Antón.

La seguridad de los datos y las categorías de datos especialmente protegidos, constituyen dos principios básicos de la regulación de la protección de datos personales, y en los tratamientos de estos tipos de datos la normativa exige una serie de garantías y obligaciones adicionales, a las que con carácter general establece en cualquier tratamiento de datos personales.

El tratamiento de datos especialmente protegidos es uno de los aspectos que plantea mayor complejidad en el análisis general de la regulación de la protección de datos, y esto se debe al hecho de que son tratamientos que conllevan recogidas conservación y uso de datos sensibles, esencialmente relacionados con la esfera más íntima de las personas.

La Directiva Europea de Protección de Datos define las categorías especiales de datos, incluyendo en éstas a aquellos datos personales que pueden revelar el origen racial o étnico de las personas, relativos a las opiniones políticas o con visiones religiosas y filosóficas, la pertenencia a los sindicatos, aquellos datos relativos a la salud o a la vida sexual de las personas y, por último, los relativos a las infracciones o condenas penales o administrativas.

En el tratamiento de estas categorías de datos pueden producirse conflictos entre la intimidad de las personas y, por ejemplo, su esencial derecho a la vida y a la salud, que exige la adaptación, por los ordenamientos jurídicos, de un conjunto de medidas específicas, que garantizando la protección al derecho a la intimidad, a la protección de datos, no dificulte o entorpezca la asistencia sanitaria o médica necesaria, para garantizar los derechos que antes comentaba, a la salud o a la vida de las personas.

La Directiva, cuando establece estas categorías especiales de datos, directamente dice que se prohibirá el tratamiento de estos datos, si bien

planten una serie de excepciones y situaciones, que deja pendiente de que cada Estado en su legislación nacional regule de una forma o de otra, siempre dentro del marco que define la Directiva.

En el ordenamiento jurídico español, la legislación española regula los datos especialmente protegidos en el artículo Siete de la Ley Orgánica de Protección de Datos de la Ley Orgánica de Protección de Datos de Carácter Personal, dentro del Título Segundo dedicado a los Principios de la Protección de Datos. Y define tres categorías de datos sensibles. En primer lugar, los relativos a la ideología, a filiación sindical, religión y creencias, para los que exige que únicamente pueda ser recogidos y tratados si existe el consentimiento expreso y por escrito de la persona, del titular de los datos.

Previamente la Constitución Española, en el artículo 16 fracción segunda recoge que *nadie puede ser obligado a declarar sobre su ideología, religión o creencias*.

La segunda categoría de datos especialmente protegidos que establece la LOPD son los relativos al origen racial, la salud y la vida sexual.

Para esta categoría de datos la legislación española exige el consentimiento expreso de los interesados o bien que exista una ley que por razones de interés general haga preciso el tratamiento de estos datos.

Para estas dos categorías de datos la LOPD realiza algunas precisiones, reconociendo la posibilidad de tratar estos tipos de datos en determinados supuestos, condicionados a ciertas finalidades y a las personas que realizan estos tratamientos de datos.

En cuanto a las finalidades, las finalidades que establece la ley son aquellas relacionadas con la prestación de la asistencia sanitaria o de un tratamiento médico o la gestión de servicios sanitarios o siempre que sea necesario para la prevención o diagnóstico médico.

En cuanto a las personas para las que la ley establece un tratamiento especial, son aquellas, los profesionales sanitarios que se encuentran sujetos al secreto profesional y otras personas que podrían estar sujetas a una obligación de secreto equivalente.

Para estos tipos de datos, además, establece una precisión; el artículo 7 de la LOPD estableciendo que quedan prohibidos los ficheros creados únicamente con esa finalidad exclusiva de almacenar datos que revelen este tipo de información.

Por último, la Ley de Protección de Datos española recoge una tercera tipología de datos especialmente protegidos, que son los relativos a las infracciones penales o administrativas, para los que únicamente las administraciones públicas, competencia en la materia, estarían habilitadas para realizar estos tratamientos de datos.

Por otra parte, como decía a principio, la seguridad de los datos constituye otro principio básico de protección de datos que está también recogido en la directiva y puesto en el ordenamiento español, en la legislación española en el mismo Título Segundo al que hacía antes referencia, dedicado a los principios básicos de protección de datos.

Este principio establece que el responsable de un fichero o el encargado de un tratamiento de datos especialmente protegidos, con algunas precisiones que haré luego más adelante, de cualquier tratamiento de datos, debe adoptar medidas técnicas y organizativas que garanticen la confidencialidad, la integridad y la disponibilidad de la información.

La aplicación de este principio y el nivel de exigencias para evitar la alteración, la pérdida, el tratamiento o el acceso no autorizado, van a ser más amplios en cuanto a la naturaleza de los datos que se tratan sean más sensibles.

Y cuando hablo de datos sensibles, me estoy refiriendo a las categorías de datos especialmente protegidos que he estado citando. Este principio en la regulación española está desarrollado en el Reglamento de medidas de seguridad que aplicando lo que acabo de decir asigna al tratamiento de datos especialmente protegidos, el nivel más alto de exigencias en cuanto a su cumplimiento.

A partir de este momento voy a centrar la presentación en los datos de salud. Para lo que se debería limitar el concepto de datos de salud y cómo se regula.

Es necesario, lo decía yo al principio, evitar conflictos entre el derecho a la privacidad y el derecho a la vida y a la salud y hay que adoptar medidas que garanticen la recogida, la conservación, la confidencialidad, la integridad, la disponibilidad de esta información al resultar esenciales para la preservación de la vida y la integridad física de las personas.

Por ello se hace necesario articular mecanismos que, garantizando la protección del derecho a la privacidad no dificulte o entorpezca la labor médica, la labor sanitaria, la labor investigadora sin el consiguiente perjuicio del interesado.

La importancia de los derechos de las personas, pacientes, como eje básico de las relaciones sanitarias, se han puesto de manifiesto en el interés que han demostrado un gran número de organización internacionales con competencia en la materia como Naciones Unidas, la UNESCO, la Organización Mundial de la Salud, la Unión Europea, el Consejo de Europa que han impulsado declaraciones o han promulgado normas jurídicas sobre la materia.

El Consejo de Europa en particular ha estudiado las cuestiones relacionadas con la problemática del tratamiento de datos en el ámbito de la salud, desarrollando una serie de recomendaciones sobre bancos de datos médicos, sobre el tratamiento de datos utilizados con fines de seguridad social, datos epidemiológicos, datos relacionados con la salud mental. En particular la Recomendación 5/97 sobre protección de datos médicos. La última recomendación que ha estado relacionada con esta materia sobre protección de datos recogidos para fines relacionados con el sector asegurador.

Todos estos son recomendables si se quiere hacer un estudio o realizar una aproximación de los distintos principios de protección de datos y su aplicación en el ámbito del tratamiento de datos sanitarios o en el tratamiento de datos relacionados con la salud de las personas.

Siendo los más importantes, el Apartado 45 de la Memoria Explicativa del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, que viene a ser la primera definición de lo que se considera datos relativos a la salud, incluyendo las informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo, comprendiendo igualmente a las informaciones relativas al abuso del alcohol o al consumo de drogas, pudiendo tratarse de una persona de buena salud, enferma o fallecida.

La Memoria Explicativa del Convenio 108, la Recomendación del año 97 sobre protección de datos médicos también hacen alusión definiendo datos médicos como todos aquellos datos de carácter personal relativos a la salud de una persona, afectando igualmente a los datos manifiesta y estrechamente relacionados con la salud, incluyendo las informaciones genéticas.

Por último, en cuanto a referencias al reconocimiento que precisa la aplicación del concepto de datos de salud, traía una referencia a una sentencia del Tribunal de Justicia de las Comunidades Europeas, que ya ha sido citado en el Encuentro, la conocida como sentencia “linquis”, en la que el Tribunal viene a aclarar qué es lo que se entiende por datos de salud y simplemente hubo una información que publicaba la señora “linquis” en su página Web sobre la lesión en un pie de un compañero de catequesis, el Tribunal deja claro que se trata de un dato de salud.

Volviendo al principio, en el tratamiento de datos especialmente protegidos relativos a la salud, es necesario encontrar ese equilibrio de la aplicación del derecho fundamental a la protección de datos y la prestación de la asistencia médica o sanitaria.

La Ley Orgánica de Protección de Datos en el caso español, la LOPD, establece con carácter horizontal los principios, obligaciones y garantías de protección de datos, incluyendo ya una serie de limitaciones en cuanto al tratamiento de los datos especialmente protegidos; la normativa de protección de datos se completa con la Legislación Sectorial y la armonización de la Legislación Sectorial con la específica de Protección de Datos es la que va a regular los tratamientos de datos relativos a salud que se recogen algunos de los tratamientos más importantes en los que se están recogiendo datos relativos a la salud, están los tratamientos relativos a la asistencia sanitaria, vigilancia, epidemiológica, ensayos clínicos, investigación, aparte de otros muchos de naturaleza administrativa, como pueden ser los relacionados con la actividad aseguradora, con sus pensiones por minusvalías y muchísimos más.

Ya para terminar, les voy a relatar cómo afectarían las medidas de seguridad, los datos especialmente protegidos en la regulación específica de protección de datos en la situación española, en la LOPD.

El Reglamento de Medidas de Seguridad que ha citado antes que desarrolla el artículo 9 de la Ley de Protección de Datos, establece tres niveles de seguridad: Básico, medio y alto, y en función de la naturaleza de los datos que son tratados en cada fichero, en cada sistema de información establece una serie de medidas que son de obligado cumplimiento y que son complementarias.

Y así, en concreto, en los ficheros de nivel alto, o sea, en el nivel alto de aplicación de medidas de seguridad se encuentran aquellos tratamientos que contemplan datos especialmente protegidos.

Debe estar implementado un buen sistema de seguridad en la organización, pero además, debe realizarse una auditoría periódica cada dos años para controlar que las medidas de seguridad se apliquen correctamente.

Un tema muy importante. Cuando se está tratando información especialmente protegida fuera de la organización, bien si ese tratamiento se hace mediante un soporte que se ha preparado en la organización para llevarlo a otra entidad o bien cuando esa transmisión se ha hecho a través de una red de telecomunicaciones los datos deben ser cifrados, debe mantenerse un registro de accesos para controlar quiénes acceden a la información, y qué movimientos realizan en la información de los datos especialmente protegidos, y además, debe existir una copia de respaldo para que en caso de una pérdida de información se garantice la recuperación de la misma.

Todo esto, sin perjuicio del respeto al resto de los principios de protección de datos y del cumplimiento del resto de los más sectoriales.

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

Le pediría ahora a la doctora María Marván Laborde su presentación, de quien baste decir por el gran reconocimiento que tiene, que es Comisionada Presidenta del Instituto Federal de Acceso a la Información Pública.

Ponente: María Marván Laborde.

Para continuar con la discusión no abundaré mucho en cuáles son los datos especialmente protegidos, son así definidos en la Legislación española en contraposición a otras legislaciones que determinan o los definen como datos sensibles.

Creo, simplemente, que vale la pena decir que mientras más clara y precisa sea la definición más sencillo será su manejo. Lo que hay en los hechos, es un reconocimiento explícito y claro de que existen algunos datos que necesitan

mayor protección y mejores cuidados por las autoridades que los tienen en todo su manejo a lo largo de todo el proceso que comprenden las leyes de protección de datos personales desde su recolección hasta su transmisión.

Hay, de alguna manera, el acuerdo de, como ya bien decía el doctor Roldán que los datos sensibles, y se empiezan a enumerar una serie de características: origen racial, étnico, características físicas, morales, ideologías, opiniones políticas, convicciones religiosas, filosóficas, estados de salud, estados síquicos, vida sexual y otras análogas.

Y ahí empezamos a tener el problema. Cuando ponemos otras análogas, y hacemos de la definición de los datos que necesitan mayor protección o de los datos sensibles "un cajón de sastre" empezamos a perder claridad y certeza de qué es lo que estamos protegiendo, qué datos estamos protegiendo y por qué necesitan una mayor protección.

Creo que hay una cuestión que es importante hacer clara. Hablamos de condiciones especiales de protección en todas las fases que supone la ley, una Ley de Protección de Datos Personales.

La recolección, el tratamiento, la transmisión y la necesidad de crear o determinar medidas especiales de seguridad, relativas a su custodia y a quién puede y bajo qué circunstancias, tener acceso a estos registros.

¿Qué los hace especiales?

Que alrededor de estos datos tenemos la posibilidad, reconocida o no, de formarnos juicios de valor sobre la calidad de las personas y creo que esa es un cuestión importante.

Los datos sensibles, desde mi perspectiva, o los datos que deben ser especialmente protegidos, son aquéllos que de manera mucho más delicada, tocan la dignidad y la intimidad del ser humano y que por diversas razones nos generan o propician motivos de discriminación o de persecución política, social, racial o religiosa.

En la medida en la que reconozcamos esto creo yo que es importante aceptar que hay una evolución histórica y cultural del concepto de datos sensibles, o bien de lo que tenemos que poner en este cajón de datos especialmente protegidos.

Hay un principio inamovible: Debemos proteger la igualdad del ser humano y asegurar que todo ser humano sea tratado de la misma manera.

Al afirmar que la definición puede variar por la situación histórico cultura del país, tenemos la posibilidad de reconocer que lo que es un dato sensible, porque genera ciertas medidas de discriminación o de no tratamiento en condiciones iguales, en un lugar puede no serlo en otro lugar o en otro tiempo.

Quisiera poner solamente dos ejemplos, que son ilustrativos y que nos llevan a aceptar que esto es una realidad.

En México hasta el año de mil novecientos una parte lógica de las preguntas del censo, era preguntar por la raza de la gente: ¿Usted qué raza es? La gente contestaba: Blanco, indígena, negro, etc.

En 1910 no se levantó el censo, en razón de una gran revolución que tuvimos y a partir de 1920 desaparece la pregunta de raza en el censo.

Hay una política de Estado que, sin necesidad de haber hablado o discutido en ese momento de protección de datos personales, hay una política de Estado que identifica la raza como una razón de discriminación y la saca del censo.

¿Fue bueno o malo sacarlo?

No lo sé. Lo que sí es que la regresaron, pero con base en eufemismos.

Hoy día el censo no me pregunta mí raza, pero sí me pregunta si hablo una lengua indígena. En algunas ocasiones se preguntaba si era yo bilingüe, les aseguro que no estaban preguntando si hablaba yo inglés y español o más

bien si hablaba yo tzotzil y español o nada más tzotzil, por poner un ejemplo.

Hay una evolución histórica que tenemos que atender.

A partir del 11 de septiembre en Estados Unidos, pero en todos los aeropuertos del mundo, la relación religión y raza ha adquirido una preponderancia que no podemos negar.

Si una persona es musulmán, tiene cara de musulmán, tiene cara de árabe, yo puedo presumir o las autoridades de los aeropuertos se dan la libertad de presumir que es un terrorista en potencia, Ahí tenemos cómo claramente hay condiciones históricas que transforman lo sensible de los datos.

Insisto, perdón, tenemos que hablar sobre las características especiales de los datos, no solamente en su custodia, sino en recolección, tratamiento y transmisión de los mismos.

Por la relevancia que ha adquirido en México la discusión acerca del expediente médico, a partir de la aprobación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, centraré mis ejemplos fundamentalmente en este caso, pero creo que son generalizables a muchos ámbitos que tocan los datos sensibles.

Desde luego, parto de la lógica que no podemos reducir la discusión del tratamiento de los datos que requieren protección especial o los datos sensibles a los expedientes médicos, pero en México son un buen ejemplo que nos permite abordar la complejidad de esto.

No existe una sola Ley de Datos Personales en la que no se defina el estado de salud como un dato personal especialmente protegido o sensible. Y por ello me congratulo y lo decía hace rato cuando llegamos y nos saludamos, que la CONAMED esté en esta mesa, esté en esta discusión; créanme que ha sido una preocupación constante del IFAI y mía personal, el pensar que se pueda llegar a aprobar una Ley de Protección de Datos personales en México, que solamente tiene la perspectiva financiera de Hacienda, Banco de México y *Buró de Crédito*, etcétera; dejando de lado las preocupaciones de médicos y pacientes cuando claramente están contemplados en esta lógica.

Hablemos un poquito de la recolección. Quizá lo que primero que tenemos que empezar a definir es, ¿qué debe contener un expediente médico, cómo debe llenarse? Reconocer que existen hospitales de primero, segundo y tercer nivel y que esto nos lleva a complejidades específicas en el expediente y desde luego, en el tratamiento de la persona; reconocer que hay hospitales de investigación y que por la protección de datos personales de una cosa estamos seguros, no queremos que al afirmar que el paciente tiene derecho a conocer su expediente médico en su integridad, esto provoque que el médico deje de escribir.

Si ese es el efecto logrado, algo hicimos mal en el diseño de la normatividad y eso creo que tenemos que tenerlo muy claro. El cuidado en el diseño de las leyes en este momento es verdaderamente crucial.

¿Hasta dónde debe llegar una Ley de Protección de Datos Personales? ¿Cuáles son los principios generales que debe sentar? Y, ¿qué le debe encargar a otras leyes?

Ayer hablamos con toda naturalidad de cómo los datos financieros se transmiten o no en relación a las leyes propias de las instituciones de crédito y demás.

De la misma manera tenemos que lograr una armonización entre la Ley de Protección de Datos Personales con la Ley General de Salud. Y esto me lleva a una extraordinaria ponencia del doctor Roldán hace sólo unas semanas en Chile en el contexto del CLAD (Centro Latinoamericano de Administración para el Desarrollo) que tienen que ver con el proceso de la creación de normas.

No basta con que el sector financiero pueda hacer lobbying. No basta con que la CONAMED pueda hacer lobbying. No basta con que la propia Secretaría de Salud pueda opinar y discutir sobre esto. Tenemos que tomar en cuenta, sin lugar a dudas, la perspectiva del paciente.

En esta medida avanzamos sobre la discusión del expediente médico. Hemos discutido ya en muchos momentos quién tiene derecho, quién es propietario del expediente. Hemos hablado de la necesidad de trascender esta discusión por asegurarle al paciente, cuestión que me parece fundamental, el derecho a ver el expediente médico. No podemos privar al hospital o al médico ni de su responsabilidad ni de su posibilidad de tener y organizar los expedientes médicos.

Y en esta medida quiero yo entrar a un punto que me parece crucial en el tratamiento de estos datos sensibles, en la medida en la que son información sumamente valiosa en el diseño de políticas públicas, así como decía hace un momento quien me precedió en el uso de la palabra.

¿Cómo podemos plantearnos, diseñar políticas públicas de prevención, sin identificar claramente a la población susceptible de contraer, por ejemplo, una enfermedad específica?

Y esto me lleva a la necesidad de usar el dato y manejarlo con toda responsabilidad en una definición territorial. Nadie niega, hoy día, que hay lugares donde se concentra la propensión al cáncer en razón de ciertas contaminaciones y demás y la investigación médica tiene que poder contar con esos datos.

Cómo generar un cerco sanitario si no tenemos una ubicación clara de la población que está siendo afectada por una determinada epidemia.

Las cuestiones raciales y culturales inciden también en esta definición de políticas públicas, es claro que hay ciertas razas donde algunas enfermedades o problemas congénitos son más propensos a suceder que en otros.

Cuestiones socioeconómicas. ¿Quién se atrevería a negar hoy en México que la diabetes tiene una relación muy clara con problemas de desnutrición y problemas donde la población se considera económicamente marginada?

Patrones de la vida sexual. Desde el ejemplo más claro que nos ponían en genética cuando estábamos en primaria, donde fue claro que la hemofilia tenía que ver con los patrones sexuales, permítanme una expresión un poco fuerte, de apareamiento, en la manera en la que se casaban entre los reyes, las cortes, hasta hoy día en cuestiones como la propagación del VIH-SIDA.

Como país yo necesito saber quién es VIH-POSITIVO por qué y esto al mismo tiempo que lo necesito saber no debe dar lugar a la discriminación, ese es el punto delicado del asunto, ni una discriminación laboral, ni una discriminación de cualquier otro tipo.

Me atrevo afirmar, un dato se vuelve sensible cuando su difusión o su mal uso se convierte en motivo de discriminación. Muchos de nosotros hemos tenido la posibilidad de conocer un ejemplo clásico que hubo de resolver la Agencia Española de cadena de supermercados que con base en la fotografía de los solicitantes de empleo determinaron quiénes podían y no podían entrar, gorda, chaparra, fea, tiene cara de mexicana, es decir, aparecieron todos estos datos y con esos elementos discriminaron de la posibilidad de que se consiguiera empleo a un grupo específico de personas.

Los datos o el manejo de los datos en manos del Sector Salud pueden tomar una connotación completamente distinta en manos de las aseguradoras, creo que es importante reconocer que existe una tensión entre los intereses públicos y privados.

Ayer dijimos de manera prácticamente natural, en el seno del trabajo de este Encuentro, que

era válido de alguna manera para el Buró de Crédito manejar los niveles de riesgo y premiar al buen pagador cuando solicita un crédito o quiere comprar algún tipo de mercancía. Si bien este principio puede ser muy claro en este ámbito, probablemente no sea extrapolable sin ton ni son sin tomar en cuenta ciertos principios éticos al ámbito de la salud.

Si las aseguradoras médicas sólo conceden seguro contra enfermedades médicas a quienes no tienen el riesgo de enfermarse, para qué compro un seguro.

Permítanme caricaturizar un poquito, si me hacen un análisis de ADN como condición para darme un seguro y me dicen sólo la podemos asegurar a usted contra tal y cual enfermedad, porque es lo que le podemos asegurar por su ADN, que no va a contraer, como para qué les pago una prima todos los meses o todos los años.

Es decir, son cuestiones que nos llevan realmente a tratar de entender y manejar la complejidad que tiene el manejo, perdón, la redundancia, de estos datos sensibles.

Cuando hablamos de datos especialmente protegidos, normalmente se incluye en las legislaciones de datos personales la necesidad de disociarlos, disociarlos de quién, del dueño de estos datos.

Y aquí permítanme también problematizar un poco. ¿Cuándo y cómo debemos disociarlos? Si un expediente médico va a ser utilizado para la investigación, me queda claro que debemos de disociarlo del nombre y rostro del paciente a fin de que éste no pueda ser identificado y en última instancia discriminado por su condición de salud, pero al mismo tiempo tenemos que permitir al Sector Salud, a quien se dedica a la investigación médica, darle seguimiento a las personas desde que nacen hasta que mueren y todavía más, aún yendo hacia sus antecesores o descendientes.

Resulta una verdad de Perogrullo afirmar que problemas de desnutrición en la infancia tienen consecuencias claras en mi estado de salud en la vida adulta. Que la tendencia familiar a la diabetes o el cáncer puede predisponer a mis hijos a tener cáncer o diabetes.

Sin embargo, si esto va a ser razón o motivo para que no se me dé un seguro, para que no se me trate en un hospital, para que no se me contrate, tenemos que tener precisamente un cuidado en donde la ética atraviesa siempre y permanentemente este tipo de manejos.

Los datos especialmente protegidos requieren una reflexión sería de las condiciones de la transmisión. ¿Quién y bajo qué circunstancias tienen derechos a tenerlos y/o recibirlos? ¿Cuáles son las medidas de seguridad electrónica, desde luego, y no nada más electrónica de almacenamiento y custodia de los mismos?

Y aquí venimos a otro punto que en la discusión de las leyes de datos personales es crucial: ¿Qué tipo de consentimiento requiere el manejo de estos datos que ya hemos definido como especiales?

Es claro que necesitamos un consentimiento expreso, firmado y claro que cubra todas y cada una de las partes del proceso. Su recolección, su tratamiento y su transmisión. No es nada más el permiso cuando voy a recolectar los datos, no es nada más el permiso para poderlos manejar y tratar, participar de una investigación o transmitirlos. Cada una de las fases va requiriendo consentimientos expresos, que tienen que estar claramente enmarcados en la ley, de tal manera que sean una realidad operable, pero que garanticen al individuo esta protección de sus datos.

Parto, desde luego, del derecho a saber. Cuando ingreso, por ejemplo, a un hospital-escuela, yo sé que por definición mis datos pueden ser utilizados para la investigación. No es nada más saberlo por definición. Creo que lo menos que merece una persona que es paciente de un hospital-escuela, es que se le advierta y pida su consentimiento de que su expediente médico será parte de una investigación, y asegurarme

que tenga yo este conocimiento. Es decir, en última instancia las leyes de protección de datos personales nos llevan a nosotros, como individuos, a adquirir conciencia de que somos cajas completas de información, y que el manejo de estos datos debe hacerse con todo el respecto a mi dignidad de persona, y en beneficio también individual y también social.

Por eso creo que es importante poner el ejemplo de la importancia del manejo de los datos sensibles en el diseño de políticas públicas.

Tenemos que partir de reconocer en el manejo de estos datos de la capacidad de autodeterminación del ser humano, que en este caso específico nos lleva a afirmar la autonomía del paciente, y a dejar atrás prácticas paternalistas, que nos llevan a suponer que existen seres humanos, hombres y mujeres, que deben o no pueden ser tratados como adultos. O dicho de otra manera, que los tenemos que tratar como eternos menores de edad.

Hablar de protección de datos personales, hablar de tomar conciencia como persona que tengo estos derechos, es en última instancia un reconocimiento de la libertad humana, y un reconocimiento de que todo ser humano tiene y debe protegerse su capacidad de razonar y de escoger.

Creo que ésta es, en alguna medida, la esencia del tratamiento especial que le debemos dar a los datos personales que nos llevan a la necesidad de una definición clara, de previsiones normativas cumplibles en todas las fases del procesos: recolección, tratamiento, transmisión, almacenamiento de datos y acceso a los archivos de los mismos y, desde luego, como ya decía también el doctor Roldán, a sanciones específicas que realmente sean capaces de disuadir al trasgresor.

El día de ayer conversábamos en la cena con el doctor Piñar Mañas. Hay compañías españolas que prevén en su presupuesto hasta 6 millones de euros, para pagar en multas por el mal tratamiento de datos.

¿Qué quiere decir? Que ellos ya hicieron un cálculo que pueden ganar, por lo menos 6 millones de euros más uno, en caso de violar la ley. Esas son las cosas que tenemos que tomar en cuenta en el diseño de una norma y por eso, créanme, me congratulo mucho que estén en la mesa con nosotros.

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

Quiero decirle que en el Sector Salud y particularmente en la Comisión Nacional de Arbitraje Médico, reconocemos este interés no solamente jurídico, legal, de entrar al estudio del tema, sino un interés legítimo que en este momento se reconoce con sus palabras, pues se nota que el Instituto de Acceso a la Información, su Presidenta y el resto de los señores Comisionados tienen este interés en abordar el tema, para beneficio no de las instituciones, sino concretamente, como usted lo señalaba, de los propios pacientes.

Así que muchas gracias por habernos invitado.

Ponente: Fabrique Gallegos.

Quiero aclarar que vengo en representación de Abraham Sotelo Nava; soy Director General en la Unidad de Gobierno Electrónico y Política de Tecnología de la Información. Me dedico a la operación de todos los sistemas electrónicos que ofrece la Secretaría de la Función Pública.

Primero explicaré un poco sobre lo que estamos haciendo en medidas de seguridad y en especial con los datos especialmente protegidos.

Los voy a sacar un poco de contexto en el sentido de que no voy a hablar sobre expedientes médicos, voy a hablar de lo que estamos haciendo en el ámbito de la tecnología.

La Secretaría de la Función Pública, antiguamente la Secretaría de la Contraloría y Desarrollo Administrativo, ha cambiado de funciones a partir de enero de 2004; es decir, ha

tenido nuevas atribuciones y estas atribuciones involucran precisamente a la Unidad de Gobierno Electrónico y Política de Tecnología de la Información, a generar esto: Política en Tecnología.

Para la presente administración el tema tecnológico es de gran prioridad, es una alta prioridad y, por lo tanto, los resultados que nosotros hemos ofrecido y realizado en el tema tecnológico, nos han generado que nuestro sentir, nuestro ser y nuestro saber es ahora el ciudadano. Ese es nuestro centro de atención, es nuestro centro de acción.

Por lo tanto, al tener, como nosotros, al ciudadano en medio, queremos recuperar esa confianza perdida del ciudadano con su gobierno. Es decir que el ciudadano tenga un gobierno que funcione como todos queremos; un gobierno el cual sea eficiente, el cual sea eficaz, el que sea oportuno, el que sea seguro y, por lo tanto, se ha generado una estrategia general, la estrategia de buena agenda, de buen gobierno, que comprende diferentes líneas de acción, en donde le estamos ofreciendo al ciudadano diferentes acciones en materia sobre su gobierno, que tenga un gobierno que cueste menos, de calidad, profesional, digital, con mejora regulatoria, honesto y transparente.

En la utilización de la tecnología, en la utilización de la mejora regulatoria, es precisamente ahí donde la seguridad que hemos dado a los sistemas que producimos juega un papel relevante.

La aplicación y el uso de la tecnología de la información, si bien nos ofrece ventajas para que el ciudadano tenga una calidad de vida mejor, para que el ciudadano tenga facilidades de interacción entre gobierno, sus particulares, las empresas y el propio gobierno, que tenga un mejor desarrollo social y económico.

También la tecnología en una utilización incorrecta puede convertirse en una amenaza. Cuántos de nosotros no hemos utilizado los cajeros automáticos y sentimos amenaza cuando utilizamos un medio electrónico, el que nos pueda dar el dinero correcto que estamos solicitando; cuántos de nosotros también consultamos o hacemos una transacción vía Internet o recuperamos nuestra Curp a través de Tramitanet.

Existe una gran diversidad de trámites y servicios que ahora se ofrecen a través de estos medios y que pueden resultar en una mala utilización, puede resultar una amenaza para el propio usuario, puede formar una manera de exclusión o tener alguna condición de incertidumbre o de riesgo por la propia transacción electrónica que se esté realizando.

Nosotros creemos en principios básicos en la protección de datos, sean datos personales o sean datos no personales.

Uno es el principio de legalidad. Tener los datos precisamente en el ámbito legal que son requeridos, no pedir más, no pedir menos simplemente los que legalmente podemos pedir, los datos que sean de calidad, es decir, no contar con información que sea basura o que sea incorrecta, que sea impropia.

Uso y destino de la información. Precisamente saber cómo se van a utilizar estos datos y dónde van a estar almacenados, es un principio muy importante.

La seguridad que implica diferentes tipos de seguridad, llámese física, lógica y, la custodia y consentimiento para la transmisión de datos. Es decir, hacer una transacción electrónica tenemos que tener el consentimiento de ambas partes y de esa manera van a poder comunicarse y serán válidas sus transacciones.

En el ámbito de la custodia se han generado diferentes acuerdos en donde la Secretaría de la Función Pública tiene en custodia, por ejemplo, bases de datos de servidores públicos conteniendo información muy sensible en donde podemos definir datos que son personales, aquellos que relacionan a la identificación de la persona y aquellos también que comprenden su

información en archivos, es decir, la que tiene relacionada con esa misma persona. Pero aún así existen datos que no necesariamente son personales y que requieren ser también especialmente protegidos.

La Secretaría de la Función Pública ha generado diferente tipo de seguridad y política para la utilización correcta de estos datos.

La política de la seguridad física. En nuestras oficinas seguridad física implica tener accesos restringidos en nuestras propias instalaciones, custodia de los archivos físicos que podemos tener, circuitos cerrados de televisión en donde podemos verificar exactamente las personas que estamos autorizadas a trabajar en el piso asociado a nuestra unidad.

La seguridad lógica que conlleva a la utilización de registros electrónicos que nos permitan la entrada electrónica a nuestras instalaciones.

El acceso a los propios sistemas que implican también una seguridad lógica, implican una seguridad desde el punto de vista de la utilización de las bases de datos, de los roles que juegan los que custodian las bases de datos y los roles que juegan quienes hacen uso de estas bases de datos.

Así también la utilización del correo electrónico en el sentido de no volverse un distribuidor de información, tal vez confidencial. También la seguridad en redes, proteger ciertos segmentos de transmisión de datos por los cuales no pueden transitar los mismos para los cuales la Secretaría de la Función Pública ha generado este tipo de políticas de identificación y de autentificación, utilizando también mecanismos como la firma electrónica, la firma electrónica avanzada, en donde la Secretaría de la Función Pública a través de diferentes acuerdos normativos hemos generado este mecanismo que nos da una confidencialidad de autenticidad de los documentos electrónicos que estamos utilizando, entiendo por autenticidad aquellos documentos en donde podemos ser e identificar al autor del propio y también la confidencialidad guardando el acceso al propio documento y restringirlo a quien únicamente pueden verlo.

Aunado a ambas partes, la confidencialidad y la autenticidad nos da para nosotros lo que utilizamos ahora que es la firma electrónica y la firma electrónica avanzada, utilizado infraestructura de llave pública y llave privada.

Con ello hemos generado diferentes sistemas, como es el sistema Compra-Net, que es el sistema para las compras del Estado, en donde utilizamos este tipo de mecanismos donde protegemos datos sensibles que no necesariamente son personales. También tienen que ver con datos en donde una transacción puede llevar a cabo algo en negocio, es decir, algo en dinero, aquellos proveedores y contratistas que quieran contratar con el Estado pueden enviar sus ofertas a través de este sistema y podrán ser ganadores, tal vez, de un contrato de un concurso; por lo tanto, la protección de sus transacciones es sumamente importante, así como los datos que contienen cada una de esas transacciones, no pueden ser revisadas por nadie más, solamente en tiempo y forma que está adecuado o realizado para la utilización de este sistema.

También este sistema ha sido auditado por el Banco Mundial, precisamente en el aspecto de seguridad.

Tres ejemplos más donde utilizamos protección de datos muy importantes: sistema de Declaranet, que nos permite a nosotros, servidores públicos, presentar nuestras declaraciones patrimoniales; es decir, nosotros como servidores públicos tenemos la obligación de presentar cuánto ganamos, qué propiedades tenemos (bienes muebles, cuentas bancarias) que le asegura poder identificar al gobierno con lo que contamos en el ejercicio de nuestro servicio.

Existe otra iniciativa como es el sistema@campus donde nos permite identificarnos a través de estas llaves públicas y privadas y poder tener acceso como servidores públicos a capacitación en línea.

También existe otro sistema, el Sistema RUPA, que es el Registro Único de Personas Acreditadas que nos permite acreditar la personalidad jurídica de una empresa que quiere hacer trámites y servicios con el Gobierno Federal y cuenta con toda su información y es válida en todas las dependencias; es decir, su información puede ser visible por los interesados para realizar trámites y servicios en las demás dependencias.

Con esto espero haber dado un panorama general de lo que estamos haciendo en la Secretaría de la Función Pública y especialmente en los productos y servicios que estamos ofreciendo a la ciudadanía.

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

A continuación le pediría al doctor Enrique Domville, quien es médico egresado de la Universidad Nacional Autónoma de México, que tiene una amplia experiencia y trayectoria de 25 años en diversas instituciones del Sector Salud.

Fue asesor en tecnología de la información del expediente clínico y actualmente es asesor del Subdirector General Médico del ISSSTE.

Ponente: Enrique Domville Domville.

Los datos especialmente protegidos. En este momento estamos adoptando un lenguaje, pero en realidad estos datos a nosotros nos los enseñaron en la facultad que teníamos que protegerlos y teníamos materias como sería la Introducción a la Clínica, donde nos hicieron hincapié de cómo obtener la información para ayudar a nuestro paciente, por supuesto que esa información tiene que ver con todos los datos que pueda el paciente darnos para poderle ayudar.

¿Cómo se guarda el expediente? Nosotros tenemos en el país actualizaciones del siglo XIX, del siglo XX, siglo XXI, estamos en una época de transición, donde estamos cambiando del papel al óptico, al electrónico. En este momento decir que todo el material está debidamente protegido en todo el país, sería redundar en una necedad y error.

Los Usuarios:
¿Quiénes son los que pueden acceder al tipo de información que nosotros manejamos? ¿El personal del hospital? Me atrevo a decir no legal, sino judicial, porque habitualmente se requiere una orden para la entrega de un expediente, y se puede usar desde el punto de vista comercial.

¿Qué es lo importante? El respaldo. ¿Por qué necesitamos respaldo? Porque hemos visto recientemente, en diciembre del año pasado un tsunami que acabó con información médica en todo el Sureste Asiático. Tenemos un temblor del 85. Tenemos recientemente huracanes en la zona sur del país. La protección no nada más va contra el mal uso de esa posible información, sino a la protección, tiene que ver con guarda, tiene que ver con el poder seguir ayudando a aquel que lo necesita, y por lo tanto su información, porque es muy difícil acordarnos de todo. Tal vez el paciente se acuerde de algunos detalles, pero para eso utilizamos el expediente, precisamente para remarcar y recalcar todos aquellos avances o diagnósticos o bien estudios que se hayan hecho.

¿Cuáles son los peligros? Los peligros son, la consulta fraudulenta. Siempre hay alguien que quiere obtener algo, además de su salud. Alguien quiere utilizar la información para otros fines, no para los que fue creado. A esto nosotros le tenemos que denominar de alguna manera consulta fraudulenta.

Tenemos la sustracción de esa información, se roban los expedientes para fines de personal y tenemos los desastres que ya hacia mención.

La empresa por no decir el sistema médico, que puede ser desde el individuo hasta una institución privada o pública, y el usuario son los responsables, porque ambos tienen derechos y obligaciones.

Mencionaba la doctora hace un momento sobre la importancia de lo que sería el consentimiento informado. De acuerdo a la regulación de nuestro país nosotros utilizamos lo que es el consentimiento informado. En este momento no se practica ninguna circunstancia de orden médico si no está con firma autógrafa en el expediente el procedimiento o lo que se le va a hacer al paciente. Siempre está por escrito con la autorización.

La información tiene un flujo. Tenemos dos tipos de información, una que proviene del hospital y otra que provendría de una delegación.

La delegación tiene varios tipos de unidades. Las unidades podrían ser de primer nivel, podrían ser clínicas hospitales u hospitales generales. Y tienen guarderías, oficinas administrativas, velatorios, almacenes. Todos estos manejan información privilegiada, información que puede ser de uso comercial, esta información privilegiada tenemos que custodiarla.

Pero la más importante es la que se genera tanto en las unidades médicas como en las guarderías.

Ahora, acuérdense ustedes que nosotros tenemos la posibilidad de la dualidad. En determinado momento podemos ser custodios de la información y en otro momento estamos proporcionando la información, porque requerimos nosotros del tratamiento médico.

En los hospitales regionales hay que ver cómo está su estructura, el abasto, el personal, los accesos. En personal tenemos fichas de identificación del personal, que además pueden ser derechohabientes de los propios hospitales. Por lo tanto, aquí se maneja el sistema de que tenemos archivos separados y tenemos varios archivos.

Ahora, cuando tratamos de evaluar la estructura aquí vamos a ver los daños que ocasionó y esos daños nos llevan a verificar la información, si es un daño interno o es un daño externo.

Si es un daño interno tenemos que evaluar si puede seguir operando. Esto quiere decir que si tenemos los recursos para seguir atendiendo a la gente que lo requiere, ya sea a nuestros derechohabientes, población abierta o a nuestro mismo personal, y hay que evaluar los por cientos. Todo esto es información que puede ser privilegiada, aunque en este momento no son datos personales, pero todo esto va influir sobre los datos personales, porque va ser la manera con lo que vamos a poder o no poder hacer nuestras acciones y se tiene que plasmar en un documento, que es el expediente clínico.

Ahora, si el daño es externo poco podemos hacer, pero tenemos que ubicarnos en el lugar de sitio.

Nosotros necesitamos saber qué abasto tenemos. ¿Por qué? Pues porque esto se va reflejar otra vez en le expediente. Nosotros vamos a saber si le podemos dar agua, si le podemos dar medicamentos, si los tenemos o no los tenemos. Todas estas acciones se reflejan o se van a reflejar sobre los datos especialmente protegidos del expediente clínico.

El personal. En un desastre tenemos que saber qué personal estaba, necesitamos saber quiénes estaban y si les ocurrió algo en nuestras instalaciones o si no llegaron a nuestras instalaciones y, por lo tanto, si están ausentes de las áreas.

¿Cómo son los accesos?

El tipo de atención. A cada uno de éstos que le estamos dando atención, nosotros tenemos que hacer un registro de la atención que estamos dando y, por lo tanto, se vuelven datos especialmente protegidos, pero estos datos se toman en circunstancias muy especiales, porque estamos frente a un fenómeno.

La organización. Esta organización, para obtener los datos, guardar los datos y conservarlos durante el desastre, pues es un reto que no está regulado, es un reto que hay que pensar y que hay que trabajar mucho.

¿Con qué frecuencia vamos a actualizar estos datos? ¿Cada seis horas, cada ocho horas, cada 12 horas?

Pues va depender de la organización previa al desastre que tengamos, para el manejo de este tipo de información.

La información en hospitales. Pues toda esta información va estar en relación con el expediente clínico; el nombre del hospital, en fin, etc., la fecha de inauguración, las historias, las anécdotas, la capacidad física de un hospital, el número de camas, consultorios, urgencias. Todo esto influye sobre el documento que estamos hablando, que está especialmente protegido.

El número de camas, consultorios de urgencia, consultorios de gineco-obstetricia para saber, por ejemplo, la capacidad resolutiva. Si nosotros vemos dos pacientes por hora y tenemos un consultorio, pues no vamos a poder ver más de dos pacientes por hora. Los quirófanos de la misma manera para ver su capacidad.

Todos estos auxiliares de diagnóstico son parte importante de lo que contiene el expediente clínico, ya que estos datos hablan de una parte del tratamiento o hablan en especial de algunas terapias que se usaron, como por ejemplo en el banco de sangre, si se ha transfundido, si no se ha transfundido.

Y habitualmente todas éstas traen el diagnóstico presuncional.

El archivo: El número de expedientes que manejamos. En promedio es uno por población derechohabiente, si el ISSSTE tiene 10 millones de derechohabientes, pues vamos a tener teóricamente 10 millones de expedientes, pero no es así. Cada nivel de atención tiene su propio expediente, entonces estamos hablando de la posibilidad de 30 millones de expedientes, mas si fue atendido en otras unidades, aparte, que no le correspondía, entonces estamos hablando de muchísimos datos, de millones de datos.

Estamos haciendo 90 millones de acciones médicas por año. Estos 90 millones de acciones médicas se reflejan en un expediente y en este reflejo estamos hablando de que hay que guardar esos 90 millones de acciones, de alguna manera, para que no tengan un mal uso y puedan hacerse para lo que son, para ayudar a nuestros pacientes.

Ahora bien, antes de llegar a decir que hay una regulación o que estamos en proceso de, nosotros tenemos que llamar a los responsables y decirles, el contexto ha cambiado. Nosotros en este momento vamos a hacer conciencia de los millones de datos que manejamos, que necesitan ser salvaguardados. Por lo tanto, debe de existir un cuerpo colegiado de expertos que dé asesoría, antes de auditoría, primero tiene que dar asesoría para formar y, posteriormente certificar el cumplimiento del mismo. Yo le llamaría asesoría y certificación en lugar de auditoría.

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

Cédric Laurant, voy a señalar brevemente su currículum, es Consejero de Políticas de EPIC, centrado en temas de privacidad internacional y políticas comparativas y aspectos legales de los regímenes europeos y estadounidense; su trabajo reciente se ha enfocado en los ficheros de viajeros aéreos, vídeo vigilancias, tecnologías de identificación de radio frecuencia, en la negociación de las directrices en privacidad, de la APEC y, en el tema de vigilancia electrónica gubernamental; es master en Derecho por la Escuela de Derecho de la Universidad de Columbia.

Ponente: Cédric Laurant.

Voy a explicar principalmente la situación en los Estados Unidos, el concepto por sí mismo no existe. Lo que sucede en los Estados Unidos son diversas regulaciones que cubren tipos específicos de información y en las legislaciones se menciona una referencia donde existen datos sensibles.

Los datos sensibles son algo que se refiere no sólo a muchas cosas, sino a uno muy importante que es la dignidad, que cuando se utiliza de una manera adecuada por las autoridades se llaman realmente datos sensibles.

Entonces, al formar este concepto nosotros podemos ver que estamos rastreando y perfilando un desafío hacia la sensibilidad de protección de datos o la protección de datos sensibles.

Recientemente y posterior al huracán se publicaron y las autoridades empezaron a decir que se podían identificar mejor las tarjetas de identidad, así que ahora en los Estados Unidos existe un gran debate sobre si estas investigaciones son desafiantes o no, y si se puede dar la aplicación de la ley con las agencias gubernamentales que están tratando con esta situación de emergencia.

Yo me enfoco en tres casos principales: El primero, es la supervisión de los niños; la segunda, es la de los empleados en un lugar de trabajo y la tercera de las situaciones importantes.

En el primer caso la vigilancia de los niños tiene un tipo de datos que se refieren a la educación y hacia dónde van los niños desde su escuela o su kindergarten para ver qué es lo que se identifica con respecto a los menores.

Esto fue algo reciente en los Estados Unidos, por ejemplo, en los parques de diversiones como Disneylandia, Six Flags, etc., y se están pidiendo huellas digitales en todos los patrones que incluyen niños.

Si este fuera el caso en la Unión Europea, si fuera una situación de protección de datos entonces estaría prohibida en los Estados Unidos puesto que no hay una situación de datos, de protección de datos unánime, ya que esta recolección de datos no es permitida. Las compañías tienen el derecho de recolectar datos, pero no siempre huellas digitales, lo interesante en este caso es que el propósito es muy sensible, porque la mayoría de las personas en los Estados Unidos creen que las huellas digitales son datos realmente sensibles, la razón para recopilar esto es que evita que las personas utilicen la identificación de alguna otra persona, pero el propósito mismo no es proporcional el tipo de datos y la sensibilidad de esta recopilación de los datos.

Este problema de protección de datos es que no existe una proporcionalidad, la recolección de huellas digitales con el propósito de asegurar los datos y de la persona que necesita utilizar esto de la misma manera, de una manera legal excede esta proporcionalidad.

Otra situación que me interesó es que el 99.9 por ciento de estas situaciones no se dan cuenta de que cuando se les pedía que hicieran una firma, que pusieran sus dos dedos, el índice y el medio, la mayoría de ellos no se daban cuenta de que en realidad estaban proporcionando sus huellas digitales.

Lo que sucede con estos datos es que los propósitos que se están generando se utilizan posteriormente por las autoridades, entonces, la tercera y la más importante es que las personas no dan un consentimiento explícito para que se utilicen estos datos o las huellas digitales como hemos estado diciendo.

Otro caso interesante que se llevó a cabo a principio de este año, se presentó en California, era un rastreo de niños con diferentes implicaciones. Los obligaban a utilizar unos como delantales, donde estaban ocultos estos arsenales, y les podían, les decían que era situación de manejar mejor a estos niños. Y aquí podemos ver que esta situación generaba el propósito que estábamos viendo que había grandes problemas, y que estaban manejando estos datos tan sensibles a su entender, registrando toda la situación que estaba generando los niños en cualquier momento.

La situación de la protección de datos en Estados Unidos principalmente tiene un alcance de la dignidad de los seres humanos, incluso aquí que

estamos hablando de niños, y son niños que no sacan una tarjeta de identidad, ni existe una proporcionalidad entre el tipo de datos que se están utilizando para medir esto y el propósito que éstos tienen.

También se refiere a la implicación del consentimiento y de la transparencia. Esto con una implicación que nos da una situación de los datos y la tecnología, es un propósito que se inicia para tratar a los seres humanos, para rastrearlos como vegetales, como latas o como situaciones de embarque.

También puede tener un impacto. ¿Qué tan fácilmente podría darse que esos niños fueran discriminados en cierta instancia, debido a que esa información que está contenida aquí se puede manejar no solamente por los que se les requirió, sino también por cualquier persona que tenga acceso a esta información y por todas las personas que puedan entrar en contacto con los niños, y podrían leer la información de este niño?

Otro caso interesante es la supervisión o la vigilancia en el lugar de trabajo, en el uso de pactos, de cartas o de tarjetas de identidad.

El uso de tarjetas listas, de tarjetas que se utilizan para dar un acceso, para Internet específico en el lugar de trabajo. Estas tarjetas astutas a veces son realmente seguras.

Pero en general no tiene sentido, por ejemplo, en los hospitales o en algún otro tipo de instalación tampoco tiene sentido si se hace este tipo de situación en todo el ambiente de trabajo.

También eso ha sido terminado por la investigación que se ha dado en el gobierno, que se investiga a ciertas compañías, para entender de una mejor forma cómo estas compañías podrían recopilar o utilizar este tipo de tarjetas astutas y utilizarlas como una referencia futura para definir este tipo de personas que ellos contrataban.

La mayoría de los registros estaban en una forma personal y el empleado podía ser rastreado, podía ser encontrado por sus patrones en cualquier lugar, en cualquier posibilidad o en cualquier región en que éste estuviera; en grupo, en el lugar en que se localizara, con quién se estuviera socializando, con quien se estuviera relacionando, con otros empleados.

Por lo tanto, también es interesante al definir esto, que solamente una de las compañas, dadas las cláusulas específicas y escritas, en las que ellos lo autorizaban, donde no se utilizara este tipo de datos en contra de las personas que estaban siendo empleadas y de unas pólizas especificando cómo más adelante estos datos solamente se utilizarían para el momento en que se estaban contratando.

Así es de que uno de los asuntos más importantes de protección de datos es que esas tarjetas, aunque originalmente se utilizaban primero para abrir puertas, digámoslo así, generaron una gran cantidad de datos que se recopilaban posteriormente con esos propósitos y eran una situación diferente, puesto que en lugar de beneficiar los perjudicaba, a pesar de que se pudieran considerar como situaciones de seguridad.

Y entonces aquí podemos ver que el uso de este sistema de rastreo, que modifica el equilibrio entre la conveniencia personal, la seguridad en el lugar del trabajo y la privacidad, nos lleva a una pérdida de seguridad privada.

En los Estados Unidos esto no se considera dentro de los derechos humanos, puesto que se está hablando de la Constitución, puesto que se considera como valor, que se pone en situación de la supervivencia en el lugar de trabajo. La seguridad y la conveniencia personal, en este caso en particular, son de un uso y un valor de una conveniencia personal, a pesar de que esté atentando contra la seguridad y contra los valores individuales.

La tercera área de supervisión era la situación de poder tener un chip subcutáneo, que muchas compañías estaban utilizando para ayudar a los paramédicos y a los doctores para poder tener en caso de que el paciente permaneciese inconsciente y no pueda dar su información o su historial médico.

Es muy poco probable, es muy poco conveniente que se promueva una tecnología que permanentemente ate al ser humano con un chip, una vez que desde aquí ya no va a tener esta situación de privacidad y de tranquilidad que pudiera lograr.

También se propuso un marco para regular esta situación y pensamos que lo que podríamos hacer con este asunto y los generales, sería identificar y no ocultar de una manera personal la identificación personal, pero si se pudiera encontrar podemos decir que podría ser una situación no permanente, pero que sí se relacionara con el individuo en específico.

Esto debería ser una incertidumbre. Aquí el caso con los pacientes que están etiquetados por este tipo de chips, por seguridades de su privacidad puesto que se está afectando su identidad. También sería el caso del uso de este tipo de tarjetas que están permanentemente ligadas a los individuos, esto representa a las personas que están originando esta identificación. Estaría prohibido este tipo de chip.

Como conclusión general yo quisiera proponerles que pensaran y consideraran. En los Estados Unidos lo que sucede es que la mayoría de las personas piensan en los riesgos, en los tipos de datos específicos, en los duplicados, cuando estamos hablando de los individuos y en general es un marco que el legislador y los que hacen la política deben de valorar cómo estos sectores específicos deberían de ser interrelacionados o cómo estos datos deberían de ser recopilados.

Y también siempre deben enfocarse hacia una situación de una privacidad en general, que conforma no obtener o poseer los datos a través de la tecnología, sino de una tecnología futura y de una protección de este tipo de datos. Estos ejemplos, yo les quiero demostrar que las compañías empiezan a pensar en la tecnología y en el interés de tener una base de datos comprensiva total.

Y por ejemplo esto afecta a Microsoft porque tienen asuntos de privacidad, problemas con su privacidad. También que vean esta situación de que estos tres factores claves se deben apoyar con estas compañías y deben de responder de una manera legislativa.

Primero la conclusión potencial con los congéneres de otros tipos de datos que se podrían cubrir. También el incremento de poder tener más confrontación con la recolección de datos personales que pueda afectar una situación y también incrementar los códigos de acceso para poder mejorar la seguridad.

Y también esto debería realmente hacerse, sobre todo en el trabajo de Microsoft. Han propuesto también un marco específicamente con respecto a la información que influye en los requisitos de obtener un consenso explícito por parte del consumidor para que entre en vigor este año.