Las tecnologías de la Información y su Impacto en la Privacidad: de las computadoras a las telecomunicaciones

Mesa 2:

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA-México.

El doctor Jesús Rubí Navarrete es abogado. Director del Gabinete del Ministro de Justicia, Director General de Relaciones con las Cortes y el Parlamento Español; Asesor Jurídico del Tribunal de Cuentas; Vocal del Tribunal de Defensa de la Competencia; Subdirector General de Inspección y Adjunto al Director de la Agencia Española de Protección de Datos.

Conferencia Magistral: Jesús Rubí Navarrete.

Me sumarme a las felicitaciones a los organizadores, en particular al IFAI y agradecerles a ustedes su presencia.

En primer lugar querría insistir en una idea que ya se ha manifestado a lo largo de la mañana. Hay que distinguir el derecho a la intimidad y el derecho a la protección de datos personales.

El derecho a la intimidad es el derecho que se refiere a una esfera privada de la persona, mientras que el derecho a la protección de los datos personales en parte presume el tratamiento de la información sobre las personas, hace que esa información no sea secreta, sino todo lo contrario, que sea objeto de un tratamiento, inclusive de un tratamiento masivo, pero exige una conducta activa por parte de los que realizan ese tratamiento y esa conducta activa consiste básicamente en que sea una conducta o un tratamiento con garantías, una conducta garantista.

Esta conducta garantista se traduce en lo que se refiere al objeto de la ponencia. En primer lugar, en el tratamiento de datos automatizados en las computadoras; es el tratamiento de datos que podemos distinguir de otros tratamientos que veremos posteriormente, relacionados con el desarrollo tecnológico.

En este ámbito en que el tratamiento automatizado de los datos personales y el tratamiento en bases de datos, en las computadoras que utilizamos en la perspectiva de la Unión Europea, está sujeto a un sistema de garantías que tiene dos bloques.

Por una parte, los principios de protección de datos, que ya se han comentado, el consentimiento, la información, la calidad, la finalidad, la seguridad o el secreto y una serie de derechos, como son los derechos de acceso, de rectificación, de cancelación y de oposición.

Sin embargo, el desarrollo tecnológico, el desarrollo del sector de las telecomunicaciones y de las nuevas tecnologías ha dado lugar a un hecho nuevo, a que ese sistema de garantías, esos principios que acabo de comentar o esos derechos, necesiten adaptaciones específicas ante nuevos fenómenos tecnológicos.

El desarrollo tecnológico obliga a adaptar los principios de protección de datos, en primer lugar, a la seguridad de la red; obliga a recoger, a considerar qué medidas de seguridad, qué riesgos se producen; cuando se producen esos riesgos la necesidad de informar a los usuarios de que se han producido y también la necesidad de ofrecerles soluciones tecnológicas a un costo razonable, para poder evitarlos.

Los datos de tráfico son aquellos datos que identifican la comunicación que se está realizando y que permite la facturación, es un tratamiento que con las herramientas disponibles Data Warehouse, Data Maning pueden dar lugar a perfiles muy exclusivos en la vida de las personas y necesitan una adaptación de los principios generales de protección de datos a sus peculiaridades.

Y lo mismo sucede con los datos de localización que son los datos que permiten la ubicación física de los equipos terminales y que pueden dar lugar al hecho de que se produzca un seguimiento, un control de itinerancia de los usuarios de esas terminales.

También en el sector de las telecomunicaciones se están desarrollando servicios de valor añadido, desde los más elementales, como puede ser la bienvenida cuando llegamos al aeropuerto de México diciéndonos qué tenemos a nuestra disposición, todo tipo de servicios, información turísticas o simplemente una bienvenida, hasta servicios muy sofisticados que pueden llevar a suponer el tratamiento, por ejemplo, de datos relacionados con un problema cardiaco de una persona y que permita atenderle, inclusive sin que él se esté dando cuenta de que tiene una crisis cardiaca.

Por qué no hablar de las comunicaciones comerciales más solicitadas, el Spam, que constituye uno de los fenómenos más graves en el desarrollo de las telecomunicaciones, como también lo constituyen el desarrollo de programas espías que permiten obtener información de las terminales sin conocimiento de los usuarios o los zombis que permiten inclusive acabar casi suplantando al usuario de un equipo terminal y utilizar su terminal para hacer, por ejemplo, comunicaciones comerciales no solicitadas como si lo hiciera ese usuario que es el titular de al terminal.

Y lo mismo sucede también en servicios avanzados de telefonía, puesto que estos servicios permiten la identificación de la línea desde la que se llama, la identificación de la línea a la que se conecta o permiten el desvió o la retirada del desvío automático de llamadas.

Sucede en esta necesidad de adaptación en los directorios de telecomunicaciones, las guías de telecomunicaciones que es un instrumento que se utiliza con carácter público para el tratamiento de datos personales, o con la facturación desglosada. Por tanto, tenemos una primera necesidad de adaptar esos principios generales vinculados a las propias exigencias de la protección de datos personales, cuando éstos se tratan en el sector de las telecomunicaciones.

Pero además, estas nuevas exigencias vienen derivadas de aspectos que son ajenos o sino ajenos, por lo menos no directamente relacionados con la protección de datos personales, como es el desarrollo de los servicios de la sociedad de la información.

La Cumbre Mundial sobre la Sociedad de la Información que se celebró en Ginebra en el año 2003, marcó una serie de objetivos respecto del desarrollo de la sociedad de la información.

Yo he recogido algunos datos los que me han parecido sintéticamente más importantes en cuanto a la protección de datos personales, como son, que las tecnologías de la información y las comunicaciones, permiten un desarrollo más intenso de la educación, del conocimiento, de la información como todos podemos conocer o también marca un objetivo que es que las tecnologías de la información y del conocimiento, las TIC coadyuvan de una manera muy eficaz al crecimiento económico y en particular inclusive en países en desarrollo, porque permiten alcanzar nuevos niveles de eficiencia y de productividad.

Sin embargo, en esta declaración de Ginebra se hace referencia a que, para que pueda desarrollarse la sociedad a la información existen determinadas necesidades.

Primero. Que haya conectividad, sin acceso a la red no va haber, en ningún caso, desarrollo de la sociedad a la información.

Segundo. Que haya una colaboración, una cooperación entre entidades públicas y privadas y también en el ámbito internacional dirigida a tratar de evitar o de reducir la brecha digital, la de aquellos que pueden acceder a este tipo de servicios y la de aquellos que podrían quedarse al margen de los mismos.

Tercero. Se hace referencia a una necesidad de competencia, de que exista un funcionamiento competitivo de mercado, aunque siempre garantizando obligaciones de servicio universal, porque la competencia puede excluir del acceso a estos servicios a aquellos que vivan en locales o territorios o que tengan niveles de rentas que no permitan su acceso a estos servicios y por tanto los poderes públicos tienen que garantizar o establecer obligaciones de servicio universal que permitan a toda la población el acceso a esos servicios.

Y en particular entre estas necesidades se hace referencia a una que está muy directamente vinculada con la regulación de protección de datos, porque se dice que es imprescindible fomentar la confianza y la seguridad. Sin confianza y seguridad por parte de los usuarios no se desarrollarán adecuadamente los servicios de la sociedad a la información. Y esto implica que haya seguridad en redes, que haya herramientas de autenticación, suficientes, adecuadas, que se garantice la privacidad y que se proteja a los consumidores.

Y hace una referencia específica a la necesidad de abordar estrategias y políticas que permitan por lo menos, sino evitar sí reducir este fenómeno que conocemos como el Spam. En esta declaración de Ginebra se hace referencia a la necesidad de que existe un entorno propicio para el desarrollo de la sociedad de la información, cuyo primer aspecto es que exista un marco jurídico adecuado. Una regulación, en esta materia, que sea transparente, que sea competitiva, que sea tecnológicamente neutral, que sea predecible, y que se adapte, esto es muy importante, a las necesidades nacionales.

Tenemos en este momento dos aspectos o dos puntos de vista que obligan a adaptar los principios de protección de datos a las nuevas exigencias del sector de las telecomunicaciones. Uno es derivado de la propia estructura, del propio sistema de garantías de protección de datos personales.

Segundo, vinculado al desarrollo de los servicios de la sociedad de la información.

Y hay un tercer aspecto, que hace necesario o imprescindible el que exista este tipo de garantías en el desarrollo del sector de las comunicaciones, es el que hace referencia a las necesidades de desarrollo del comercio internacional. Se ha comentado en algunas ponencias que la libre circulación de datos personales es un elemento esencial para el desarrollo del comercio internacional.

Se ha hecho referencia a que en realidad el origen último de la propia directiva 95 46 de la Comunidad Europea, que es una norma vanguardista en lo que se refiere a la protección de datos personales, tuvo ese apoyo en las competencias que el Tratado de la Unión atribuye a la Comisión Europea en materia de mercado único o de mercado interior, el garantizar la libre circulación de datos consideraba y se sigue considerando como imprescindible para que pueda haber un funcionamiento correcto del mercado único, y lo mismo sucede en el ámbito de la Unión Europea, que es una organización regional, y por tanto, esa exigencia responde a las necesidades de integración de esta región o a las de cualquier otra región, podríamos citar el caso americano, el MERCOSUR, por poner un caso, hacen imprescindible que para garantizar la libre circulación de datos exista una regulación que prevea un sistema de garantías, y no sólo en el ámbito de una integración regional, sino también en el comercio que se realiza entre unas y otras regiones, entre todos los países, en definitiva, el tratamiento de datos y la libre circulación de datos personales que se produzca en un mercado globalizado.

Y partiendo de estas necesidades yo querría hacer referencia a abordar los criterios que son necesarios o los criterios que deben dirigir esta regulación en el sector de las telecomunicaciones para poder atender los retos de la protección de datos personales, para poder atender el desarrollo de los servicios de la sociedad de la información, y para poder favorecer el desarrollo del comercio y de la actividad económica a nivel mundial.

El primer aspecto que considero importante o imprescindible que se incorpore en cualquier regulación que aborde esta materia, es que se parta del principio de neutralidad tecnológica. En la experiencia europea hemos tenido un ejemplo claro de los inconvenientes que puede generar el no cumplir con este principio.

La neutralidad tecnológica significa que el sistema de garantías que se establezca sea operativo, cualquiera que fuere la tecnología que se utilice, pueda ser operativo para tecnologías que todavía no han sido desarrolladas.

La primera directiva de protección de datos en la Unión Europea, en el sector específico de las telecomunicaciones del año 97, vinculó el sistema de garantías a determinadas tecnologías, fundamentalmente los servicios telefónicos, y olvidó otros servicios u otras tecnológicas, básicamente el desarrollo de Internet y ha sido necesario modificar esa directiva, derogarla y aprobar una nueva, la Directiva 2002/58-C, para garantizar que este sistema de garantías opera con neutralidad tecnológica.

Y esto es muy importante, porque si no fuera así podríamos encontrarnos con un fenómeno que podríamos denominar de deslocalización tecnológica, si las garantías que existen son distintas para unas tecnologías y para otras, si son más rigurosas en unos casos que en otras, el fenómeno que se puede producir es que se incentiven determinadas tecnologías y se aparquen otras en las que pueda ser más complicado de aplicar este sistema de garantías; por tanto, es un principio fundamental.

En la neutralidad tecnológica el sistema europeo se apoya en un concepto de comunicación electrónica, que es un concepto extraordinariamente amplio, lo tienen ustedes en la Directiva 2002/58-C y que parte de la premisa de que siempre que haya una comunicación electrónica que es simplemente una transmisión de información entre un número finito de personas, cualquiera que sea la red que se utilice, siempre que se produzca ese fenómeno se aplica el sistema de garantías.

El segundo aspecto importante desde el punto de vista de esta regulación o el criterio a incorporar en esta regulación, es que este sistema de garantías tiene que articularse como derecho de los abonados y los usuarios y no como obligaciones de los operadores de telecomunicaciones, ni como obligaciones de los

prestadores de servicios de la sociedad de la información.

Porque si se articula como obligaciones acaban produciéndose déficit y omisiones, por ejemplo, el Spam es algo que realizan terceros que no son prestadores de servicios de la sociedad de la información y que no son operadores de telecomunicaciones, de forma que si establecemos un sistema de garantías basado en un régimen de obligaciones habrá terceros en los que no concurre esas características que hagan Spam y que no estén sujetos a las obligaciones propias de los sistemas de protección de datos o de garantía del tratamiento de datos en el sector de las telecomunicaciones.

Ha habido muchos ejemplos en la legislación española y la nueva Ley General de Telecomunicaciones ha tenido que invertir las cosas, es necesario articular este sistema de garantías como derechos subjetivos de los abonados y de los usuarios oponibles frente a cualquiera, sea operador de telecomunicaciones o no sea operador de telecomunicaciones, sea prestador de un servicio de la sociedad de información o no lo sea.

El tercer aspecto relevante es lo que he querido llamar superación del concepto de dato personal, la normativa de protección de datos personales, como se ha comentado esta mañana, es una normativa sujeta a un aspecto crucial, debe tratarse información de personas físicas identificadas o identificables.

Y esto lleva a un debate permanente de si determinadas informaciones son informaciones sobre personas físicas identificadas o identificables, la dirección IP es un dato de una persona identificada o identificable, un número de un determinado celular es un dato de una persona física identificada o identificable, el propio terminal en el que se pueden instalar virus u otro tipo de programas espías que capten la información supone el tratamiento de información personal identificada o identificable.

En nuestra experiencia tenemos argumentaciones jurídicas que permiten afirmar que la dirección IP, que la dirección de correo electrónico, etc., en determinadas condiciones son un dato personal.

Pero es, en mi opinión, necesario superar este concepto e ir a un sistema de protección que proteja el uso de determinadas herramientas, el uso del teléfono celular, el uso del terminal; porque de esa manera, primero, no va a estar excluido del ámbito de protección nadie cuando se debate si es un dato personal y además, porque se puede incluir dentro del ámbito de protección no sólo a las personas físicas, sino también a las personas jurídicas.

Y la importancia de este aspecto ha sido que el legislador español cuando ha incorporado en nuestro sistema legal la Directiva 2002/58, que es la directiva vigente en la Unión Europea para protección de datos en el sector de las comunicaciones electrónicas o de las telecomunicaciones, ha desvinculado este sistema de garantías del concepto de dato personal y lo ha incorporado en dos regulaciones distintas, una parte en la Ley General de Telecomunicaciones y otra parte en la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico.

Y ha atribuido, eso sí, nuevas competencias a la Agencia Española de Protección de Datos de forma que ahora no sólo aplica lo previsto en la Ley de Protección de Datos, sino también, este régimen de garantías predicable inclusive de personas jurídicas o morales que está en la Ley General de Telecomunicaciones y en la Ley de Servicios de la Sociedad de la Información.

Otro aspecto muy importante a considerar para un enfoque o una regulación en el ámbito del sector de las telecomunicaciones es el dotarse o el prevenir herramientas que puedan ser útiles para combatir este fenómeno auténticamente inquietante, que son las comunicaciones masivas o comunicaciones comerciales o no comerciales, los correos electrónicos no solicitados, el Spam.

Ese punto es un problema particularmente amplio en la medida en que vivimos en un mundo globalizado, pero yo sí querría destacar tres aspectos en los que hemos estado trabajando.

En primer lugar el de conseguir una adecuada colaboración entre las autoridades de control, los prestadores y los usuarios.

Frente al Spam no basta con que exista un régimen sancionador, porque puede no ser aplicable, porque el Spam está en un lugar al que no se puede aplicar extraterritorialmente una norma. Por tanto, no basta con una regulación. Es necesario, pero no es suficiente.

En segundo lugar, es necesario contar con los prestadores de servicios de la sociedad de la información, a través de los cuales está circulando este tipo de comunicación y además, es necesario contar con la concienciación y una actitud proactiva por parte de los propios usuarios, tienen que ser conscientes de la importancia de este fenómeno, de los riesgos que corren y como decía, desarrollar una conducta activa de autoprotección.

Y, demás, de esta manera, mediante esta interrelación, se pueden resolver problemas jurídicos importantes. Por ejemplo, si los prestadores de servicios de la sociedad de la información autónomamente establecen sistemas de filtrado de los correos electrónicos, va a suceder inapelablemente que habrá falsos positivos y falsos negativos; habrá correos electrónicos lícitos, que son retenidos y que llegan a sus destinatarios y seguirá habiendo correos electrónicos ilícitos, que sí llegarán a sus destinatarios.

Y eso puede dar lugar, inclusive, a responsabilidades contractuales, a responsabilidades por daños, a sanciones administrativas por interpretación de las telecomunicaciones, en la medida en que sea una decisión autónoma de los prestadores de esos servicios.

Por eso es imprescindible que los prestadores de estos servicios y las autoridades competentes tengan una relación muy fluida con los propios usuarios, les informen de cuáles son los instrumentos de filtrado que los prestadores de servicio puedan aplicar; en la aplicación de esos servicios de filtrado tengan la confianza de que jurídicamente están actuando de una manera lícita, para lo cual, es imprescindible la intervención de las autoridades administrativas competentes y además haya respuesta por parte de los usuarios, para que ellos digan y decidan si quieren o no el filtrado, conforme a qué criterios o conforme a qué no criterios o si quieren utilizar herramientas alternativas, por ejemplo, disponer de dos direcciones distintas de correo electrónico, para tratar de evitar este fenómeno.

Es necesario, por tanto, esta colaboración, y esto nos lleva a que es necesario también una concientización de los usuarios, que van a tener que adoptar medidas propias de adquisición y de búsqueda de programas actualizados, de firewall, de programas que eviten el contagio por virus y que el propio usuario va tener esta disposición proactiva, para autoprotegerse.

Y en tercer lugar es imprescindible un aspecto básico, que es la cooperación internacional. Sin cooperación internacional es imposible perseguir el Spam.

Yo he puesto algunas referencias, algunas iniciativas que hemos tenido. Un memorándum de colaboración entre la Agencia Española de Protección de Datos y la Federal Trade Commission de los Estados Unidos de Norteamérica o también el London Action Plan, que es un plan de acción en el que están participando autoridades competentes de protección de datos, de defensa de los consumidores muy variadas, empresas privadas, etc., para que tratar de combatir este fenómeno.

Y un último aspecto importante a considerar, en cuanto a estos criterios, de un nuevo enfoque en el sector de las telecomunicaciones es el relacionado con el gobierno electrónico.

La tecnología, el gobierno electrónico, el E-government o la administración electrónica va permitir un acceso más sencillo a los ciudadanos, va permitir mayor transparencia, va permitir también una mayor eficacia, una mayor eficiencia en la actuación de las administraciones públicas. Pero estos programas de E-government tienen que estar, en todo caso, sujetos a garantías específicas.

Y estas garantías específicas, yo querría hacer referencia a alguna de ellas, a la vista de lo que ha sido nuestra experiencia práctica.

En primer lugar, que haya sistemas de identificación unívoca razonables de los usuarios a distancia de este tipo de servicios, porque sino, pueden acabar produciéndose suplantaciones en el acceso a información administrativa por parte de terceros, que no son los usuarios autorizados.

En segundo lugar, que el tratamiento de la información dentro de las administraciones públicas tienen que responder al principio de finalidad. Y en el ámbito de la administración pública el principio de finalidad se concreta en que los datos que pueden recabarse y que pueden tratarse tienen que estar vinculados al ejercicio de competencias, de atribuciones específicas que se hayan reconocido a ese órgano, a esa parte de la administración pública. No toda la administración pública, por muy pública que sea y porque toda en general responda a razones de interés publico, tiene porqué tener acceso a toda la información disponible. Es imprescindible que se cumpla el principio de finalidad, que se vincule al ejercicio de sus competencias. Y esto es particularmente importante cuando el desarrollo de estos sistemas llega a un nivel de interoperabilidad.

En tercer lugar, es imprescindible que se introduzcan medidas de seguridad que impidan o que mantengan íntegra la información y que impidan accesos no autorizados o si éstos se producen que permitan su detección.

En cuarto lugar, hay que evitar, con estas medidas de seguridad, que con el cúmulo de información administrativa y la utilización de nuevas tecnologías, sea la propia administración pública la que se dedique a realizar perfiles de la conducta de los ciudadanos en sus relaciones con la administración.

Estos son, a mi juicio, los aspectos básicos de un nuevo enfoque en protección de datos en el sector de las telecomunicaciones. El próximo paso, ¿cuál es? La Red Iberoamericana.

En la Red Iberoamericana, precisamente en este IV Encuentro hemos elaborado un documento de trabajo sobre gobierno electrónico y telecomunicaciones. En ese documento de trabajo se detallan para cada uno de estos aspectos que les he ido comentando, el Spam, los servicios avanzados de telefonía, los datos de tráfico, los datos de localización, los directorios y el gobierno electrónico, etcétera, soluciones y propuestas concretas que entendemos que pueden permitir alcanzar un nivel de garantía adecuado.

Es un documento que vamos a discutir a lo largo de estos días y respecto del que tendremos que llegar a conclusiones cuando acabe este encuentro. Espero que hagamos un debate fructífero que puedan tenerlo pronto a su disposición.

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA-México.

Vinculado con el tema que se señaló de varias de las razones por las cuales urge una regulación en lo relativo a las bases de datos personales, vino a mi mente otra temática y otro esfuerzo internacional que ahorita está preocupando a la comunidad internacional, que es precisamente la cuestión del crimen internacional organizado.

La Convención de Naciones Unidas, relativa precisamente al crimen internacional, contempla la temática de las bases de datos y

en concreto y vinculado con toda la temática del lavado de dinero y el narcotráfico, está la cuestión de la cooperación judicial o la cooperación entre los Estados.

No se podrá cumplir con ninguna de las metas o de los objetivos u obligaciones de los propios Estados de no darse una normatividad precisamente que sea acorde a las necesidades que por un lado tienen, en el lado de la balanza, lo que es el derecho a la privacidad y los derechos humanos de la persona, y por el otro lado la tecnología que a muchos ha sobrepasado en varios Estados, lo que es la propia legislación interna y el esfuerzo de la comunidad internacional por controlar y regular debidamente y que se realicen en el campo de lo lícito y no de lo ilícito varias actividades y comportamientos que desgraciadamente no se han sujetado a control.

Quiero presentar al siguiente ponente, el doctor Fernando Argüello Téllez, especialista en normativa regulatoria y asuntos de competencia; doctorado en Derecho Patrimonial por la Universidad Pompaifraba de Barcelona, España. Miembro de la Red Iberoamericana de Protección de Datos, especialista en protección de datos personales en diversos cursos y seminarios; obtuvo el premio de periodismo en 2003 sobre la protección de datos personales, convocado por la Agencia Española de Protección de Datos, ponente de la XXVII Conferencia Internacional de Privacidad y Protección de Datos realizado Suiza, en el mes de septiembre de 2005.

Ponente: Fernando Argüello Téllez. Superintendencia General de Electricidad y Telecomunicaciones del SIGET de El Salvador.

Quisiera agradecer a los organizadores la capacidad de convocatoria que se ha tenido para un tema que es tan novedoso y tan relevante en lo que es el desarrollo de la democracia de todos los países.

Quiero empezar contándoles lo que me pasó por la mañana. Me encuentro con que el vecino de al lado a la habitación del hotel, tenía puesta la tarjetita que siempre ponen en la puerta de: "Por favor no molestar" o "Haga la habitación". Me llamó la atención ya que en este caso, dice: "Privacy please", en vez de "Not disturb".

Y creo que sería interesantísimo que tuviéramos una tarjetita así como en *Monopolio* o *Gran Banco*, para poderle sacar a los encargados y responsables de los tratamientos una tarjetita para decir: por favor respete mi información personal.

Vamos a empezar con la ponencia, con lo básico, que es Warren and Brandeis, ya el Director de la agencia se refirió a él. Esto lo llevo a colación en lo que respecta a lo que son los inicios de las tecnologías en la comunicación, se empiezan a desarrollar la fotografía, los periódicos, pues resulta que ya ahí en 1890 ya surgen determinados problemas con lo que es la privacidad de las personas.

Al parecer la esposa del señor Brandeis había tenido una fiesta social muy bonita, en los medios salió publicada, y resultó que los comentarios que se hicieron no les agradaron. Tenemos una magnifica ponencia en el Harvard Review mostrando lo que es el derecho a la privacidad y que ahora es esencial citarlo prácticamente en todas las ponencia de datos que puede haber.

También estamos hablando de 1972, algunos hechos relevantes. RL Polk & Co., una compañía norteamericana en Detroit, poseía datos personales de alrededor de 130 millones de personas, pudiendo tras un adecuado tratamiento informativo establecer complejos perfiles individuales. Ahí estamos hablando del inicio de la computación; ya podía haber algún tipo de tratamiento de información, pero todavía no habíamos llegado a ese enlace entre lo que eran las telecomunicaciones con las computadoras y la capacidad que tienen éstas de tratar información al respecto.

Más adelante, a finales de los años 80, principios de los 90 empieza en sí lo que sería la

convergencia informática y las telecomunicaciones.

Las tecnologías de la información, como son la utilización de las computadoras para almacenar, procesar datos; tecnologías de telecomunicaciones, como son los teléfonos, transmisión de señales de radio, de televisión, tecnologías de redes de Internet, con su forma más conocida, tecnologías móviles, voz sobre IP (VOIP). Entonces surge la convergencia entre el Internet y estas tecnologías, y se constituye como un medio de comunicación eficiente y de muy bajo costo, que va a facilitar la interrelación entre ellas. Se logra una integración entre lo que es datos, vídeo, tráfico de voz, etcétera.

Una de las nuevas tecnologías que han surgido a través de todos estos avances es el GPS, un sistema global de navegación por satélite, que nos permite determinar en todo el mundo la posición de una persona, un vehículo, una nave, con un error de alrededor de cuatro metros. Las aplicaciones que hoy puede tener son múltiples: navegación terrestre, marítima, aérea, para labores de rescate y salvamento, ubicación de enfermos discapacitados, para rastreo y ubicación de vehículos robados, entre otros.

Otra de las formas de utilizar esta tecnología es para el rastreo de los empleados, para ver las rutas de los transportistas y se utiliza un sistema GPS para poder determinar su posición, se utiliza para evitar robos, para evitar que se salgan de su ruta, etc., pero también pueden ser tecnologías que irrumpan o invadan la privacidad.

Un caso interesante que hay en Internet. William Bradley Jackson fue sospechoso de haber matado a su hija y enterrado su cadáver, las autoridades andaban tras su pista desde hacía mucho tiempo, al enterarse de que las autoridades ya andaban muy cerca de lograr determinar dónde se encontraba el cadáver decidió cambiarlo de ubicación, lo que desconocía es que las autoridades habían instalado un chip de rastreo en su vehículo. Pasaron 10 días, durante ese tiempo llegó Bradley sacó el cadáver de la hija y lo fue a enterrar a otro lugar.

Al cabo de varios días retiraron las autoridades el chip y a través de la información que leyeron pudieron detectar el lugar exacto donde había sido enterrada, por supuesto lo apresaron y a final de cuentas quedó condenado.

Lo que se vio es la disyuntiva entre la necesidad y cómo tendrían que haber actuado las autoridades; se necesitaría haber requerido de orden judicial para hacer este tipo de acción o bastaría con una mera sospecha para poder poner un chip o cualquier forma de rastreo. Para este tipo de casos podrían ser muy útiles, me parece, y nadie podría negarlo, pero también podría ser utilizado en otro tipo de usos.

Otro de los ejemplos es el implante de chips, esto lo están ocupando en algunos países para evitar robos, secuestros, se instalan los chips para estar totalmente ubicados en cualquier lugar del mundo; hubo en Inglaterra un caso bastante siniestro que se pensó en la instalación de chips a los hijos menores para evitar que fueran objeto de cualquier tipo de secuestro.

La voz "sonoripés" es un ejemplo interesante de lo que son estas nuevas tecnologías; como ya les comentaba, es un abaratamiento de lo que son los precios de las llamadas telefónicas, nuevamente interesantes, se está viendo con mucho interés los diversos reguladores de telecomunicaciones, sin embargo, como tecnología relacionada con Internet tiene sus problema de privacidad y seguridad. Al igual que un correo electrónico puede ser rastreado en Internet igualmente la voz puede ser rastreada en Internet.

El FCC, Federal Communications Commission, está tratando de ampliar el campo de una ley la cual permitía el poder acceder a las telecomunicaciones vía teléfono normal, ahora lo quiere instaurar a lo que es voz sobre IP, esto está sobre cargando, en alguna medida, a los proveedores de servicio de Internet, está utilizando el ancho de banda y causando algunos tipos de perjuicios.

Y nuevamente volvemos a lo mismo, me parece muy bien que traten de evitar cualquier tipo de terrorismo internacional, delitos y demás, pero hasta qué punto llegamos.

Debemos preguntarnos cómo identificar y regular la delicada línea que puede separar un uso adecuado de las nuevas tecnologías de la información y las comunicaciones de lo que sería un uso arbitrario en el ámbito de la privacidad y la protección de datos.

Sobre eso podríamos pensar en empoderar al titular de la información personal, a través de la educación, hacer del conocimiento de que son sumamente necesarias, que existan normas claras, un asentimiento informado que es esencial, porque muchas veces los usuarios firmamos cualquier cosa o donde dice autorizamos ceder los datos a equis y ye persona, sin embargo, desconocemos para qué van a ser cedidos.

También hay que fomentar las tecnologías garantistas de la privacidad que se están desarrollando y van en muy buen camino, que también son un elemento bastante atractivo.

Les quiero pasar un video, creo que refleja lo que es el problema que se podría dar en un uso inadecuado de las comunicaciones. Se llama Spears and Pizza y es hecho por el America Cibers Liberty Marius de los Estados Unidos.

(Proyección de video en inglés)

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA-México.

Corresponde ahora al doctor Sergio Antonio Toro. Es Director Ejecutivo de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia, su país natal. Ingeniero en Electrónica por la UNAM, Universidad Nacional Autónoma de México; Maestría en Ciencias de Computación de la Fundación Arturo Rosemblueth. Ocupó cargos en diferentes instituciones bolivianas, destacándose el Ministerio de Hacienda, la Dirección General de Impuestos Internos, el Gobierno Municipal del Alto y Ministerio de Desarrollo Municipal. Ha sido consultor internacional en varios países de Centroamérica, Sudamérica y África.

Sus inicios profesionales se refieren al Distrito Federal, México, donde trabajó por más de seis años en el Instituto Nacional de Cardiología, Dr. Ignacio Chávez y en el Hospital Metropolitano de la Ciudad de México.

Ponente: Sergio Antonio Toro.

Quiero agradecer a los presidentes, al IFAI, y a México donde me he formado, también quiero agradecer al doctor Piñar Mañas por la inclusión dentro de la Red Iberoamericana de Protección de Datos.

Voy a empezar mi presentación haciendo una reseña de qué es lo que se está haciendo en mi país, qué es lo que se está haciendo en Bolivia.

Voy a decir qué es la ADSIB, suena como remedio, pero no es un remedio, son palabras un poquito difíciles, es la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

La Agencia Boliviana para el Desarrollo de la Sociedad de la Información en Bolivia nace en el año 2002, en el marco de un decreto supremo, no nace como una necesidad o como un tema de que la voluntad política del momento esté de acuerdo con ella, si no más bien como un tema, yo lo calificó como una especie de esnobismo. Todo alrededor, todos los países circunvecinos empiezan a desarrollarse en lo que se llama la sociedad de la información, en tratar de proteger sus datos, en ver la importancia que en el mundo tiene las telecomunicaciones y las TICS y, bueno, hay una declaración que ha sido mencionada hoy, la declaración de Santa Cruz de la Sierra donde varios presidentes, en mi país, firman el convenio para iniciar todas estas labores de proteger los datos personales.

En ese sentido nace una agencia, pero nace una agencia un poco sui géneris porque nace sin presupuesto.

Debido a la situación política que vive el país, el 21 de septiembre del 2004 la presidencia del Congreso Nacional asume tuición de la Agencia para el Desarrollo de la Sociedad de la Información, esto nos hace una entidad sui géneris, una entidad que nos hace transversales a los dos poderes: Ejecutivo y Legislativo, y ahí es cuando empiezo a tener el cabello cano porque tengo de jefes o personas que se creían mis jefes, a todos los diputados y senadores de mi país. Entonces, casi pido la habilitación de un nuevo asiento dentro de mi Parlamento, porque yo me la vivía dando informes que trabajando en mi oficina.

Realmente se me criticó o se criticaba en temas de tecnología de información y comunicación de por qué se utilizaba el gov con ve chica, como government, en lugar de gobierno con be grande como lo tienen en México, por ejemplo. A ese nivel de ridiculez he tenido que responder informes del Parlamento.

La ADSIB no nace sin un presupuesto, cosa curiosa y para suplantar y para vivir de un presupuesto nos hacen el ISP oficial del Estado boliviano y somos los encargados de sistematizar la información, generar políticas estándares del desarrollo de la sociedad de la información en el país, es por eso que estamos aquí presentes.

Nace a partir de dos instancias que existían en el Gobierno boliviano, una de ellas es la UFI (Unidad de Fortalecimiento Informático), que es una unidad que queda del Y2-K. Y otra unidad que es el BolNet, era el que tenía los servicios de Internet en Bolivia, tiene el monopolio del registro de dominios en Bolivia, tiene la administración de los números IP para el acceso a Internet y tenemos los temas de proyecto de conectividad al interior del Estado boliviano.

En ese sentido ADSIB y BolNet son las dos entidades que dan sostén técnico y financiero y que se pueda trabajar fundamentalmente en el tema de la "ticks".

Trabajamos difundiendo las "ticks", haciendo políticas, haciendo la coordinación en el área "tick", tenemos bastante trabajo, y nos nombran operadores oficiales de la estrategia boliviana de reducción de la pobreza dentro de Bolivia en el uso de las "ticks".

Trabajos básicamente, los ingenieros nos gusta hablar en difícil igual que los abogados, en la parte de la derecha, significa que trabajamos en el Setuse o sea, ciudadano a ciudadano, en el gobierno a negocios, en el gobierno a gobierno y en el gobierno a ciudadano, tratando de trabajar en esos campos fundamentales, limitamos nuestra acción. –Se refiere a la presentación que realiza en PowerPoint–

La finalidad de la ADSIB. Somos la encargada de promover políticas, todo lo bonito que puede decir un decreto de creación. Tenemos una misión, que es una misión bastante difícil en un país tan conflictivo como Bolivia. Favorecer las relaciones del gobierno con la sociedad boliviana mediante el uso de tecnologías adecuadas, realmente una misión bastante difícil la que nos ponen, con un país, donde voy a demostrar a continuación tiene muchas gradientes diferenciales.

En la ADSIB nos toca, y le pongo la palabra de ingeniería política, porque Álvaro Díaz de la CEPAL, en su informe a la CEPAL, dice que en la ADSIB se ha hecho una ingeniería política, donde jugamos con los dos poderes. Donde básicamente a mí me toca jugar con los dos poderes.

Yo califico ese jugo como hijo de padres separados, hoy tal cual un adolescente malcriado que cuando me convenía iba con el Ministro de la Presidencia y cuando me convenía me iba con el Presidente del Congreso Nacional para conseguir voluntad política.

Dentro de esa voluntad política hemos conseguido entregar resultados a corto plazo, a mediano y a largo plazo. Uno de los resultados de los cuales me siento más orgullo es que hemos hecho la estrategia boliviana de tecnologías de información y comunicación para el desarrollo.

Hemos participado, hemos elaborado el anteproyecto de ley de comunicación electrónica de datos, firmas digitales y comercio electrónico, se llamaba en un principio, en la versión 63 y ha perdido las firma digitales en el camino, ya se llama comunicación electrónica de datos y comercio electrónico. Participamos en la Red Clara, participamos en Telecentro y otros proyectos más.

En la dificultad vemos la oportunidad de trabajar. Tratamos de aprovechar la coyuntura política para aprovecharnos de eso justamente, de lo que es la voluntad política. Participamos internacionalmente en la Red Geal, en la Red Clara, en la Red Infolac, en la Cumbre Mundial de la Información, y nuestra participación reciente es dentro de la Red de Protección de Datos.

La realidad boliviana no muestra que pertenecemos a un país multiétnico, pluricultural, con más de 50 etnias agrupadas en tres regiones claramente definidas, que se han autodefinido así, poca participación ciudadana en los circuitos económicos del país, especialmente de pueblos originarios, lo que ha marcado la exclusión social, no somos problemáticos, porque sí queremos ser problemáticos.

Tenemos un alto grado de necesidades básicas insatisfechas en el país. Tenemos un país con altos índices de pobreza y marginalidad.

Tenemos la inexistencia de un marco jurídico para el desarrollo de alternativas tecnológicas que ayuden a cerrar la brecha digital. Mucha inversión y apoyo, muchos quisieran tener la inversión que tiene Bolivia, pero cuando está mal orientada y mal organizada se convierte en un fenómeno que yo lo califico "Túpac Amaru"; como Túpac Amaru tuvo una muerte por cuatro bestias, una amarrada a cada uno de los brazos que jaló para un lado distinto. Un poco eso es lo que nos está pasando en este momento con Bolivia, porque tenemos la cooperación jalándonos en distintas direcciones y no nos está permitiendo avanzar como país.

Entonces que ordenar esa cooperación internacional. Somos un país geográficamente muy disperso. Tenemos un millón de kilómetros cuadrados, tenemos 328 municipios, 29 mil localidades pobladas, donde 43 por ciento de éstas no tienen servicio de electricidad.

Y aquí es un dato que habiendo tenido mi formación en un país como México, un país tan democrático como México es un tema que realmente me desgarra y me muestra el país distinto que tenemos, el país con los gradientes que mencionaba que tenemos.

Ahí hay una fotografía en la cual dos autoridades originarias del altiplano y uniformados tras la firma del Programa de Igualdad de Oportunidad, fue el 20 de abril del 2005, este año, primera vez después de casi 200 años de vida republicana que un indígena puede acceder a entrar a un colegio militar, los indígenas no tenían derecho a ingresar ni a universidades, ni al colegio militar, este año se da la igualdad para que los pueblos originarios y los campesinos puedan tener educación militar.

Entonces, ese es el país discriminador del cual les estoy hablando y el país discriminador que presenta niveles de conflicto.

Simplemente llamo a la reflexión que la brecha digital entre los países es de 390 a 1 entre los países desarrollados y los países en desarrollo y esta brecha está aumentando.

El PIB de los cinco países de la CAN, los cinco países de la CAN juntos producen un tercio de lo factura Microsoft, quiere decir que la información sí había sido un buen negocio.

El bienestar dentro de una economía global está basado en el conocimiento de individuos solos, ojalá sea ese individuo que está encargado en la espalda de su madre el individuo que pueda alcanzar un mayor desarrollo dentro de la sociedad futura.

Los reportes de telecomunicaciones muestran indicadores muy buenos, vemos una creciente

desde 1997, muy racional, evidentemente se han instalado teléfonos y se han instalado puntas de conectividad en el país, pero de qué me sirve un teléfono tarjetero en medio de un camino, donde no hay ni las tarjetas, donde no hay posibilidades de desarrollo para la región circunvecina.

La participación de los municipios en Bolivia es de apenas un 51 por ciento del país por departamentos que tienen acceso a Internet.

Bolivia en el área urbana o en el eje central, como llamamos, tiene un índice de 0.48, más o menos equivalente al índice de brecha digital que se tiene entre Chile y España, no estamos mal en las ciudades del eje. Sin embargo, si vemos el porcentual en el área rural vemos que estamos con un 0.96, una diferencia catastrófica entre lo que es ciudad y lo que es campo.

La diferencia al interior. La brecha digital al interior de lo que está sucediendo en Bolivia es más dramática que la brecha digital de Bolivia versus los otros países, tenemos dos países, me permito calificar un país del siglo XXI y tenemos un país que está tratando de entrar al siglo XVII, si es que así se puede calificar.

Pese a eso tenemos la inclusión del Hábeas data que, bueno, la primera Constitución de Bolivia es de 1826, ahora en el marco de los conflictos que se están sucediendo en mi país se habla de una asamblea constituyente donde se va a hacer una reforma total, esperemos que para bien.

Se tienen 17 intentos de reformas, se tiene una Ley de Necesidad de Reformas del año 2002, se tiene una inclusión en el 2004 dentro de la Constitución Política del Estado y se tiene una organización del texto, un texto ordenado en el 2004 también.

El Hábeas data dentro de la Constitución Política del Estado de Bolivia está incluida en un solo artículo, en el artículo 23, y tiene en el párrafo uno, tiene las características y derechos, en los párrafos dos, tres y cinco, tiene los procedimientos para el recurso de Hábeas data y en el párrafo cuatro tiene la incompatibilidad para levantar el secreto en materia de prensa.

Los derechos y deberes fundamentales pese a la inclusión del Hábeas data en el artículo 23, no aparece como un derecho fundamental a la intimidad personal y familiar de las personas, entonces ahí ya estamos vislumbrando un posible problema de nuestra inclusión del Hábeas data dentro de nuestra Constitución.

Las características del Hábeas data. La más importante posiblemente es que está, me parece que surge un poco forzada; es que está redactada en términos negativos, es de carácter procesal para la petición de datos personales, etc.

El acceso de datos a la persona, ratificación, corrección, información obtenida o almacenada, eliminación o exclusión, son básicamente los derechos que tiene cada persona.

Las omisiones que tiene. Es un tema que causa preocupación fundamentalmente, no son subsanadas en la Constitución Política del Estado: la confidencialidad de datos personales y la actualización de datos personales, no son incluidas.

El procedimiento, y aquí hay otro problema dentro de nuestro Hábeas data es que toma a la Corte Superior de Distrito o Juez en Partido, esto es a la necesidad del recurrente. No hay una entidad destinada a hacer la protección de datos, sino son las instancias existentes ya en el país.

Esa es la primera sentencia constitucional, un poquito de la historia, donde el Hábeas data lo contraponen con la Ley de Imprenta y la Ley de Prensa, donde el fallo aprueba la resolución de improcedencia, al corresponder la aplicación de la Ley de Imprenta.

Hay una especie de desconocimiento o una especie de mala aplicación de la Hábeas data o una mala interpretación por parte tanto de los demandantes, como por parte de las entidades que estarían encargadas de la protección de datos.

En cuanto a la legislación relacionada, existe la Ley de Telecomunicaciones, existe el Código Penal, existe el Código Civil, el Decreto Supremo de Acceso a la Información Pública, que menciona el Hábeas data como tal y el Anteproyecto de Ley de Comunicación Electrónica de Datos, que también ya menciona la protección de datos y menciona la Hábeas data.

Las conclusiones que podemos decir en cuanto a nuestra Hábeas data, se precisa una Ley Orgánica para el desarrollo de la misma.

Nosotros queremos aprovechar la coyuntura del Anteproyecto de Comunicación Electrónica de Datos, para hacer el Reglamento específico de la protección de datos personales. Esa es la conclusión principal a la cual puedo llegar y este es el trabajo en el cual estamos abocados en este momento.

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA-México.

Presento al doctor Fernando Martínez Coss, licenciado en Economía por la Universidad Autónoma Metropolitana. Ingresó al sector público en 1983 y desde 1986 se encuentra en la Secretaría de Hacienda y Crédito Público, en donde ha colaborado en el desarrollo de herramientas de apoyo para el cumplimiento de obligaciones fiscales, como Declara-SAT, utilizando para el cumplimiento la presentación de la Declaración Anual de las Personas Físicas, así como la instrumentación de mejoras en servicio de atención a contribuyentes, como los módulos de atención integral a los mismos, esquema de pagos electrónicos de impuestos, sistema integral de comprobantes fiscales, así como la instrumentación de la Guía para Trámites Fiscales y es actualmente responsable del proyecto de la Firma Electrónica Avanzada y Factura Electrónica.

Ponente: Fernando Martínez Coss.

El tema que les voy a compartir esta tarde básicamente versa sobre la firma electrónica avanzada y cómo el Servicio de Administración Tributaria, al cual pertenezco, ha visualizado la forma en la que en la interacción con los contribuyentes podamos tener una relación segura que sea sencilla y, sobre todo, que lleve a una forma de interacción que permita ampliar la cobertura de servicios que tiene el Servicio de Administración Tributaria.

En ese sentido el SAT ¿qué es lo que ha hecho y en qué ha basado su desarrollo? Básicamente ha basado su desarrollo actual desde el año pasado y hasta la fecha, en un esquema que se ha denominado de firma electrónica avanzada.

El primer entendimiento que quisiera que tuviéramos es, ¿qué es una firma electrónica avanzada? Es un conjunto de datos, en este evento estamos hablando de datos, pero sobre todo lo que hemos buscado nosotros como autoridad fiscal es que haya alguien atrás de los datos, que haya una identidad, que haya una persona que de forma segura nos permita tener una relación con el contribuyente. Esto es lo que hemos hecho.

Y la firma electrónica avanzada nos lo ha permitido, de hecho es algo que dentro del marco jurídico que nosotros tenemos ya se encuentra reconocido, es decir, ya tenemos reconocido dentro del Código Fiscal de la Federación los certificados de firma electrónica avanzada.

Con esto abrimos un campo muy interesante a efecto de tener esta relación segura que les comentaba. En este sentido no podría yo estar hablando de un certificado y menos de impuestos si no estuviéramos frente a una obligación.

En nuestro país existe desde el año pasado, el año pasado de manera opcional, la obligación para las personas físicas y las personas morales de contar con un certificado de firma electrónica avanzada.

Este certificado tiene, básicamente, dos segmentos de contribuyentes obligados que es personas físicas con actividad empresarial, con ingresos superiores a un millón 750 mil pesos.

Y el segundo. De personas físicas con actividad no empresarial, entiéndase los arrendadores, los sujetos de honorarios con ingresos superiores anuales a 300 mil pesos y, nuestra legislación, el Código Fiscal consagra un segmento, el cual por su capacidad administrativa no tendrían esta obligación; esto no quiere decir que no pueda optar por ella, en este caso básicamente referido a los contribuyentes del sector agropecuario.

Es decir, tenemos una legislación que nos habilita la posibilidad de tener transacciones seguras, con entes identificados, y me falto un tercero que son las personas morales, que son sujetos ya obligados de presentar, de contar primero con un certificado de firma y de llevar a cabo transacciones electrónicas.

En este sentido tenemos un mecanismo que tecnológicamente nos habilita. Tenemos un marco jurídico que lo define y nos define a los sujetos, pero aquí lo importante es un entendimiento claro. Cuando estamos frente a un certificado de firma electrónica de qué estamos hablando, qué quiere decir esto.

Les quisiera decir que es el equivalente a lo que hoy por hoy tenemos como nuestra firma autógrafa, pero en el mundo de las transacciones electrónicas o en el mundo del Internet.

En mi firma autógrafa yo solo la puedo hacer; sin embargo en la firma electrónica yo solo la sé. Hay una característica fundamental en los certificados que es que en su creación deben de hacerse en absoluto secreto, nadie lo debe de conocer.

Mi firma autógrafa en el mundo del papel es el equivalente a mi certificado de firma electrónica en el mundo del Internet y especialmente en el ámbito de lo fiscal. Es decir, todo lo que tenga que ver con obligaciones fiscales o el mundo de lo tributario tiene un equivalente que se llama certificado de firma electrónica y que tiene básicamente tres características, que es: voy a tener un certificado, voy a tener una llave privada, un mecanismo de acceso seguro y voy a tener una clave de seguridad.

Es decir, en el mundo del papel utilizo lo que ustedes tienen, su pluma y papel y en el mundo electrónico voy a tener estas características que son un archivito punto *cer*, un punto *key* y una llave de seguridad. Esas son las analogías que quisiera que tuvieran.

Ahora bien, ¿cómo le vamos a hacer? ¿Cómo le va a hacer el Servicio de Administración Tributaria para lograr dotar a los contribuyentes de todo esto? Tenemos un mecanismo que es presencial, en donde básicamente lo que buscamos es garantizar la identidad del contribuyente que va a estar atrás de un certificado.

Para este fin lo que le pedimos al contribuyente es que acuda con nosotros previamente validando datos, validando datos de identidad del contribuyente. En los datos de identidad el Servicio de Administración Tributaria tiene la reserva legal de no entregarlos ni revelarlos, esto lo consagra el artículo 69 del Código Fiscal de la Federación, en donde se guarda absoluta reserva de los datos proporcionados por los contribuyentes.

Nosotros no podemos revelar absolutamente ningún dato. Sin embargo, sí nos garantiza que tengamos del otro lado de la computadora a una gente que conocemos, que sabemos quién es y a la cual le podemos proveer un servicio o simplificar que es nuestro objetivo todo esto.

¿Cuál es el ciclo de generación? El ciclo de generación es el contribuyente nos agenda una cita, ahí iniciamos a verificar los datos de identidad del contribuyente.

Segundo, nos llena un requerimiento del lado fiscal suena fuerte, pero finalmente es llenar algunos datos de la identidad del contribuyente, esto lo hace en absoluto secreto. El SAT no conoce las características de esa llave privada que genera el contribuyente. Nosotros no tenemos control de esto. Actualmente tenemos cerca de 370 mil certificados ya generados hacia los contribuyentes, esto nos habla de un número ya importante.

Tengo el dato de la Agencia Tributaria española, que me hablaba el año pasado de cerca de 300 mil certificados generados. En el ámbito de nuestro país estamos ya rebasando ya los 370 mil certificados.

Nos habla de un proceso de cambio paulatino, un proceso de cambio que no hemos hecho, como lo viene previsto en la disposición porque generaría, creemos nosotros, un cambio cultural muy fuerte.

Lo hemos hecho paulatinamente, de forma tal que un aspecto fundamental en estas tecnologías sea la asimilación del cambio tecnológico de forma pausada.

Esto creemos que lo hemos venido logrando con este tipo de cuestiones. El contribuyente, me regreso al ámbito del que estoy platicando, genera su requerimiento, acude con nosotros, vemos que efectivamente se trate de quien es, que es quien dice ser.

Esto lo aseguramos con nuestra información, la cual contamos con el contribuyente, y finalmente, jurídicamente lo que hacemos es cerramos el ciclo.

Es decir, tenemos ya una persona física o moral plenamente identificada y con esto le entregamos un certificado de firma, con el cual podamos llevar a cabo transacciones electrónicas.

Aquí hay una característica fundamental en lo que el SAT ha hecho. Esto, nosotros como autoridad fiscal lo pudimos haber hecho de manera autónoma, sin embargo, el legislador el año pasado previó a un tercero, que en este tipo de fórmulas se le reconoce como confiable, a efecto de garantizar la transparencia de todo esto. En este caso es el Banco de México, en el caso de nuestro país, nosotros, como autoridad fiscal, estamos proponiéndole a Banco de México, cuáles van a ser nuestras prácticas de certificación de identidad.

Es decir, no actuamos de manera autónoma. Eso nos da la absoluta transparencia. Aún siendo autoridad, nosotros, en este caso nuestro país, los legisladores, previeron la posibilidad de que aún siendo autoridad fiscal hubiera un tercero confiable. En este caso fue el Banco de México, a quien le estamos dando estos certificados.

¿Y con esto a qué estamos llegando? Esto habilita desde el mundo de lo tributario a una serie de servicios. Es decir, si en el mundo del papel lo que hacemos nosotros con nuestra firma autógrafa es suscribir o aceptar obligaciones o ejercer derechos, en el mundo de lo fiscal tenemos este escenario, que ahorita es el que vamos caminando.

Es decir, los contribuyentes ya pueden optar por un comprobante fiscal digital, ahí ya estamos teniendo un cambio, un comprobante fiscal digital que en el mundo del comercio electrónico viene a minimizar todas las operaciones.

Con este medio seguro la administración tributaria le permite el acceso al contribuyente a sus datos, es decir, los contribuyentes en nuestro país ya tienen acceso a la información que en materia fiscal el SAT tiene, esto que si lo hubiésemos pensado de manera presencial resultaría algo complejo, hoy por hoy ya es una realidad el que el contribuyente de manera electrónica y remota pueda accesar a sus propios datos.

Adicionalmente, ya lo comentábamos, está la presentación de la declaración anual, los agentes aduanales en operaciones de comercio exterior ya utilizan este tipo de mecanismos.

Y para el año que entra ya tendremos que utilizar este mecanismo de certificado de firma electrónica en los pagos provisionales, es decir, el cumplimiento de obligaciones periódicas que venimos haciendo ya tendrá que ser a través de este mecanismo.

Y bien, si estamos hablando de un encuentro de datos, pues, finalmente yo quisiera cerrar mi

charla con el acceso que pueden tener los contribuyentes mediante este certificado a sus datos, creo que es algo que es muy valioso, sobre todo para los contribuyentes el saber, digo, si hay alguien que conoce de los contribuyentes o de los ciudadanos en este país creemos que es la autoridad fiscal.

Nosotros aglutinamos una gran cantidad de datos que están reservados, sin embargo, lo que ofrecemos ahora es la posibilidad de que sea el contribuyente quien los conozca, que sepa qué es lo que nosotros tenemos, en este caso es la aplicación que hoy por hoy existe en la página del Servicio de Administración Tributaria, en donde a través de estos tres datos: Registro Federal de Contribuyentes, lo que es la contraseña, lo que es su certificado y lo que es su punto *key* la llave privada, puede tener acceso a todos los datos que el SAT tiene de los contribuyentes.

Esto creemos que es una oportunidad muy valiosa que no lo permite y no lo habilita la tecnología, pero sobre todo, que nos garantiza que del otro lado de la computadora hay alguien que es conocido, que nos garantiza la absoluta integridad y que no tenemos la posibilidad de que haya la corrupción de estos datos o que haya el jaqueo de estos datos, son transacciones cien por ciento seguras.

Tecnológicamente, como dato para que ustedes lo tengan, este tipo de llaves son de mil 24 bits, cosa que nos da la amplia seguridad de que difícilmente se podrían jaquear y que nos dan la tranquilidad de quien accede a estos datos es quien debe ser.

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA–México.
Continuamos con la presentación de Alfredo Reyes Krafft, doctor en Derecho por la Universidad Panamericana, Director Jurídico de E-Bussines en BBVA-Bancomer, Presidente de la Asociación Mexicana también de Internet.

Ponente: Alfredo Reyes Krafft.

Yo quisiera retomar un poquito el tema de la mesa y en particular bordar un poquito sobre la misma, estamos hablando de las tecnologías de la información y su impacto en la privacidad, el tema es de las computadoras a las telecomunicaciones.

Yo ahora quiero de alguna manera comentar que estoy representando a la industria de Internet en particular en México y en ese sentido yo quisiera aclarar una cuestión, la tecnología o las tecnologías de la información y comunicaciones, Internet, es un medio, no es un fin en sí mismo; es decir, no podemos hablar de ética de Internet, sino tenemos que hablar de ética de las personas que utilizan este medio que se llama Internet o tecnologías de la información, como quieran llamarle.

Y en ese orden de ideas tendríamos que distinguir entre el uso de la información, el bien informático como un concepto jurídico o técnico y también el bien informático o la informática como instrumento para realizar un determinado acto o un determinado acto jurídico.

En ese contexto y sobre ese punto de referencia no debemos dejar de considerar que Internet es un medio, no es un fin en sí mismo, estamos hablando de las personas.

Ahora, también debemos considerar el tema de privacidad. Nos queda muy claro que la privacidad y el derecho a la protección de los datos es un derecho fundamental, es un derecho fundamental de las personas.

Y en este sentido, este derecho fundamental debe también estar en equilibrio con otros temas también importantes, como serían los intereses de mercado, la libertad de expresión, el libre flujo de información, así como cuestiones relativas al lavado de dinero y lucha contra el terrorismo.

Considerado entonces así y tomando en consideración también el tema que y Fernando,

hace un minuto, había comentado en relación a la delicada línea. Es decir, él hacía referencia a algunas mejores prácticas y a los efectos secundarios que estas mejores prácticas pudieran llegar a tener.

Y tomando en consideración el tema y platicando en particular del tema del Spam, yo creo que también debemos de tomar el punto de referencia.

Por un lado, dentro de Spam se está exigiendo que los proveedores de servicios de Internet cuenten con mejores prácticas de protección y de prevención ante ese problema grave: Filtros anti-Spam, detección y registro de entidades riesgosas, conformación de grupos especializados para su combate, distribución de herramientas, campañas de concientización, atención muy pronta ante reportes.

Pero los efectos secundarios que podemos encontrar ante una situación como ésta, sería el tema a que ya hizo referencia también el expositor anterior de falsos positivos; el tema relativo, por ejemplo, a la diferencia entre Spam y mercadotecnia directa; que los filtros pudieran, en un momento dado, atrapar mensajes que pudieren ser válidos o también el hecho de que la propia auditoría, respecto de los mensajes que yo estoy realizando en los buzones de mis clientes, pudiera considerarse una violación a la privacidad de cada uno de los usuarios.

A final de cuentas no es culpable el proveedor de servicios de Internet respecto de este esquema. A final de cuentas el Spam le genera un problema muy grave al proveedor de servicios de Internet; ocupa ancho de banda del proveedor, el volumen de almacenamiento en cuanto a niveles de almacenamiento es a costa del propio proveedor y no lo puede incidir en el costo por el servicio que está prestando.

Independientemente de eso el ISP no debe dejar de garantizar al usuario una eficaz entrega de mensajes, confidencialidad y respeto y respuesta ante reporte de abusos.

¿A final de cuentas a qué queremos llegar con esto?

Nos queda muy claro que debemos de cuidar este derecho fundamental de privacidad y respeto a la privacidad de las personas. Nos queda muy claro también que en México contamos con legislación, si bien dispersa en algunas entidades o en algunos esquemas, contamos con legislación sobre la materia.

Es muy importante y no es por querer evitar un esquema legislativo, sino por el contrario, es muy importante propugnar por una legislación congruente sobre la materia.

¿Y a qué me refiero con congruente?

Voy a poner tres ejemplos que se han suscitado, a raíz de una Iniciativa de Ley Federal de Protección de Datos Personales, que fue presentada por un senador en México, Antonio García Torres, en febrero del 2001 y fue aprobada por el Senado de la República.

Vamos a poner un ejemplo típico. Un esquema de *opt-in* el requerimiento de un consentimiento previo y expreso de la persona, a la cual se van a tratar estos datos.

Por otro lado, también y dentro del contexto legislativo y como una política de carácter presidencial, tenemos la promoción de la inversión de pequeñas y medianas empresas en ese contexto.

¿Qué es lo que queremos hacer?

Estamos obligando a las empresas a utilizar medios de promoción para las mismas, que puedan generarle un mayor costo, porque requerirá un consentimiento previo y expreso de cada una de las personas, a las cuales les enviarán la información, publicidad o esquema comercial. Y, por otro lado, procuramos incentivar la inversión de estas empresas generándoles un costo.

Otro esquema. El esquema de la prohibición al flujo transfronterizo de datos personales. Se establece en la normativa que queda prohibido el flujo transfronterizo de datos a entidades o países que no cuenten con un nivel de protección, cuando menos equivalente al que se está planteando en ese contexto.

¿Cuál es el problema que tenemos? Contamos con un Tratado de Libre Comercio con América del Norte, con Estados Unidos y con Canadá en donde se establece que no se va a limitar este flujo transfronterizo de datos personales.

No estamos en contra de la legislación. No estamos en contra del respeto a este derecho fundamental de protección de datos personales, lo que buscamos es hacerlo congruente con nuestro esquema jurídico.

Moderadora: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA–México.

Para terminar la doctora Katitza Rodríguez Pereda, Directora del Computer Professionals Social Responsibility –CPSR– de Perú. Su trabajo consiste en analizar disposiciones sobre derechos de autor en el entorno digital, incorporados en el Tratado del Libre Comercio entre Estados Unidos y los países andinos, las propuestas presentadas por los Estados relativos a los derechos de autor en las negociaciones sostenidas en el seno de la Organización Mundial de Propiedad Intelectual y las directrices sobre la privacidad elaboradas en el subgrupo de privacidad del Grupo de Comercio Electrónico, del Foro de Cooperación Económica Asia-Pacífico; también es responsable de coordinar los reportes de privacidad en España y Latinoamérica y de mantener comunicación con autoridades en protección de datos, funcionarios públicos y organizaciones de la sociedad civil en Iberoamérica.

El tema de su presentación es la protección de datos personales y las medidas de protección tecnológicas, piratería de obras contra piratería de datos personales.

Ponente: Katitza Rodríguez Pereda.

Antes de pasar a mi exposición, quisiera hacer dos precisiones; decir que como consumidores debemos exigir que las empresas antes de tratar nuestros datos deban exigirnos el consentimiento previo, informado de que efectivamente deseamos que traten nuestros datos.

Segundo. Si hay países como los europeos que los Estados se preocupan por proteger los datos personales de sus ciudadanos, es justo que si ellos quieren hacer negocios con otros países, el mismo nivel de protección se les den a esos países.

En este panel sobre tecnologías de la información y su impacto en la privacidad voy a tratar un tema importante pero poco conocido, salvo entre aquellos que siguen o han seguido de manera más o menos constante este tipo de casos.

Se trata de la recolección y tratamiento de datos personales que se efectúa a través de las medidas de protección tecnológica o medidas de autotutela incorporadas a las obras protegidas por los derechos de autor.

Antes de que irrumpiera en la vida diaria las tecnologías de la información y que se difundiera el fenómeno de la digitalización, no existía relación directa entre protección de datos personales y derechos de autor.

Una adquiría un libro o disco, lo leía, releía, lo hojeaba, escuchaba la música una y otra vez, todo ello en forma anónima. Hace 20 años no existía cruce de caminos y menos colisión entre protección de datos y derechos de autor.

Actualmente con el desarrollo de las tecnologías de la información y en particular de las medidas de protección tecnológicas el vínculo entre ambos derechos personalísimos se entrecruza cada vez más.

¿Qué sucedió en el entretanto? La digitalización de las obras protegidas por derecho de autor, el abaratamiento de los medios de reproducción y la Internet han facilitado enormemente la publicación, copia, distribución y comunicación al público no autorizada de obras protegidas por el derecho de autor, lo que ha originado que el índice de infracciones a estos derechos sea elevado, y que exista perjuicio económico para los autores y productores.

Lo que se ha traducido, a su vez, en un incremento sostenido y real de los niveles de protección legal de los actuales modelos de negocio en este campo, llegándose al extremo de utilizar el derecho penal, las más graves de las disciplinas jurídicas para reprimir conductas que discutiblemente son consideradas ilícitas.

Como los intentos por disminuir o detener la copia no autorizadas de obras mediante los cauces legales han sido fallidos, ello dio pie a que los titulares de derechos de autor optaran por implementar las denominadas medidas de protección tecnológica, orientada a auto tutelar sus derechos.

En términos sencillos las medidas de protección tecnológica son una suerte de candados virtuales que permiten restringir o controlar el acceso y/o uso de las obras protegidas por el derecho de autor. Estas medidas tecnológicas pueden estar en el sistema operativo, en el software aplicativo, en el hardware o en una combinación de ellos.

Generalmente cumple las siguientes funciones: controlan el acceso a la obra, impiden las copias no autorizadas de las mismas, e inclusive la copia privada, que es un derecho del consumidor.

Autentica la obra con el titular de derechos de autor, e impide que la obra sea alterada, modificada, transformada.

Lamentablemente estas medidas de protección tecnológicas también suelen ser utilizadas por los productores fonográficos y de audiovisuales para controlar los usos que los consumidores hacen, por ejemplo, de los discos, películas y libros digitales.

Pueden registrar el número de veces que se ve una película, escuche un disco o lee un libro digital. Permite verificar si éstos son alterados, copiados, impresos, guardados y permiten restringir, no, perdón, ellos dicen administrar el acceso de una obra.

En síntesis, para los titulares de derecho de autor la respuesta a los desafíos presentados por la tecnología sólo puede estar en la propia tecnología. Sin embargo, las medidas tecnológicas suelen operar violentando nuestra privacía e irrespetando el tratamiento de datos personales.

¿Qué ha pasado con el uso de algunas medidas de protección tecnológica? Pérdida del anonimato. Asistimos al desarrollo de una era en la que progresivamente disminuye el anonimato, no por buenas razones o porque nos hayamos convertido en famosos, sino porque nos está siendo arrebatado por una cultura en la que nos solicitan que nos identifiquemos para todo, en particular para usar los bienes digitales.

Una vez que el anonimato se pierde, los titulares de derecho de autor argumentan que tienen derecho a explotar dichos datos, por tanto es necesario reafirmar la necesidad de permitir transacciones anónimas o con seudónimos en Internet. Esto ha sido establecido por el grupo de trabajo del artículo 29 desde su recomendación sobre el anonimato en Internet, aprobado el 3 de diciembre de 1997, en el que se concluye que el almacenamiento de datos personales en la Internet tiene que respetar los principios de protección de datos personales, al igual que en el mundo “Of line”.

Otro tema. El Código de Identificación Único. Existen medidas de protección tecnológicas que asignan un código de identificación único al contenido o al reproductor de contenidos, y que adjuntan información personal de los usuarios para la identificación y otros fines desconocidos.

Por ejemplo, el Media Player de Microsoft tiene embebido un identificador único global, que permite rastrear a los usuarios. Similar al iBook Reader, también de Microsoft, pide al usuario activar el software y vincularlo a una cuenta de password.

Luego Microsoft captura una identificación de hardware único de la computadora de los usuarios.

El código de identificación único puede almacenar los datos en un fichero, interconectar información personal de diversa índole y vincularla, por ejemplo, como información financiera, obtenida al momento de pagar con tarjeta de crédito o personal, dirección de la oficina, casa, teléfono y mail.

Tercer punto. Recolección innecesaria, información personal, gustos y preferencias de consumo.

Algunos candados tecnológicos van más allá recopilando información personal sobre los hábitos y preferencias de consumo y no sólo saben quién es usted o quién puede ser usted, sino cuantas veces repite la misma escena de una película, qué partes de la película, información que almacena nadie sabe por cuánto tiempo.

Windows Media Player, crea un fichero log, registro, del contenido de las visitas de un usuario IP a un servidor central para obtener títulos de contenidos.

Según el Electronic Privacy Information Center el vincular la información personal identificable con el contenido puede traer como consecuencia una discriminación en el precio, ésta es la venta de un bien digital a precios diferentes a consumidores diferentes.

En el caso, por ejemplo, de Napster To Go, el usuario realiza un pago mensual que le otorga acceso ilimitado a una biblioteca de archivos musicales al que puede bajar y transferir música a otro equipo.

iTunes de Apple, vende *track* individuales de música y los archiva en un álbum, música que sólo puede ser tocada en un equipo específico.

En ambos casos las medidas de protección tecnológicas permiten llevar un control de las actividades del consumidor, frecuencia, orden del uso de las canciones, entre otros, información que nada tiene que ver con el fin primario de proteger los derechos de autor, sino que son recogidas para fines comerciales de *marketing* directo o cualquier otro interés que pueda tener la industria.

En suma, el uso de medidas de protección tecnológica que no respeta los principios básicos de privacidad configuran una situación, por un lado, de ejercicio abusivo del legítimo derecho que tienen los titulares del derecho de autor a proteger su obra, pero que además es trasgresor de los principios de protección de datos personales.

En otro contexto muchas de estas medidas de protección tecnológica serían consideradas spyware.

En conclusión, para suprimir la piratería de obras protegidas por el derecho de autor no debe apelarse a la piratería de datos personales.

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA–México.

Si la mesa me lo permite podríamos dejar unos 10 minutos para responder preguntas.

Pregunta: Mi nombre es Tlacaí Jiménez, soy el titular de la Unidad de Transparencia e Información del Instituto Electoral del Estado de Jalisco.

Mi pregunta es para los señores José Rubí Navarrete y Alfredo Reyes Krafft, si pudieran darme su opinión y versa respecto de algo que en lo personal me pasó hace unos días; como funcionario público lógicamente tengo una dirección de correo electrónico, pero desde hace

varios años vengo manejando una cuenta personal en Yahoo, esta compañía tiene, los que somos usuarios de ella, convenios con Northon para antivirus y un filtro anti Spam.

Hace unos días revisando mi correo veo un título que dice invitación a foro o invitación a congreso, no recuerdo ya bien las palabras, me llamó mucho la atención y lo abrí, normalmente no lo hago cuando no reconozco la dirección de quien me envía el correo, sin embargo, lo abrí e inmediatamente se activa el antivirus, me dice que es un archivo de JPG que no implica, no tiene virus, lo abro y era una presentación muy bonita de unas conferencias, ya no recuerdo ni el tema, pero me llamaba mucho la atención que no podía yo identificar quién me lo estaba mandando, tanto el tema, como supuestamente la dirección eran la misma, decía invitación a foro, pero luego de ver y de checar las fechas y de qué se iba a tratar, hasta abajo venía una leyenda que decía: "Este correo no es publicidad comercial, por lo tanto, no constituye Spam y es único y exclusivo y no se le van a seguir generando o mandando este tipo de correos".

Entonces, me llamó muchísimo la atención por dos situaciones: Primera, ¿de dónde tomaron mi dirección de correo electrónico?; segunda, ¿quién me lo mandó?; y, tercera, si esa leyenda efectivamente podríamos considerar que eso no es Spam.

Del contenido del mensaje, uno de los organizadores decía que era el ITESO, el Instituto Tecnológico de Estudios Superiores de Occidente. Entonces quiero suponer que por allí venía la pista de dónde me mandaron esa información. Pero no encontré yo ninguna dirección y esa leyenda que me llamó mucho la atención.

Ponente: Alfredo Reyes Krafft.

Te voy a contestar en dos planos: En un primer plano como abogado y en ese contexto lo que quiero preguntarte es, seguramente tú, al momento de contratar inicialmente el servicio de Yahoo, seguramente leíste el contrato y al momento de leer el contrato pusiste tus datos y definiste un compromiso, hay un acuerdo de voluntades.

Y dentro del apartado o algunos apartados de este contrato, específicamente se establece la posibilidad de que el propio Yahoo o terceros que con él contraten, puedan enviarte publicidad o asuntos en ese contexto. Esa es una parte.

Y dentro de ese contexto habría que verlo, si nos vamos a un estricto purismo.

Dos. Hay un error grave porque no sigue lo relativo o lo que establece la Ley Federal de Protección al Consumidor, en relación al envío de datos. Debe de identificar quién es el que está generando el envío.

Y esa leyenda que dice al final, pues la verdad es que no tiene mucho sentido, cuando menos en lo que es la normativa mexicana, de inicio.

Ahora, ¿a qué quiero llegar? Es importante el esquema de Spam. Dentro del contexto de Spam queda claro, es un riesgo, es un vicio muy grande, pero ninguna legislación va acabar con el Spam, ¿para qué nos hacemos patos?

Es decir, por más que queramos hacer una legislación restrictiva y prohibir el uso en un país en particular el Spam, pues lo que va pasar es que probablemente las empresas que generan mercadotecnia, que pagan impuestos y que lo hacen de acuerdo con la ley, no lo van a poder seguir haciendo, porque va a haber un control y va a haber una restricción muy objetiva, por parte de la propia legislación.

¿Pero tú crees que dejarías de recibir por ello esos mensajes? No. Los vas a recibir y van a partir, pues yo no sé si China o de alguna otra entidad.

Entonces, ¿qué es lo que tenemos que hacer?

Establecer esfuerzos muy grandes, en un plano internacional. Estoy completamente de acuerdo que es necesario contar con una legislación *ad hoc*, pero tenemos que hacerla congruente con

la propia industria: Uno, Yahoo o el prestador de servicios de Internet no necesariamente es el malo contigo. Y en relación con ese punto debemos de adecuar perfectamente bien qué es a lo que nos referimos por Spam, tomar una definición muy clara y muy precisa al respecto.

Porque la distinción entre Spam y lo que sería mercadotecnia directa es muy pequeña.

Ponente: Jesús Rubí Navarrete.

Me alegro de la pregunta y además de que tengamos debate, porque algún matiz discrepante vamos a tener en la propia mesa.

Efectivamente, en el entorno europeo este tipo de comunicación sólo es posible con un consentimiento previo y expreso.

Y además hay un problema adicional, que es que aunque uno celebre un contrato legítimamente con una empresa que le provee de un servicio, en este contrato lo que no es posible es incluir cláusulas vinculantes, como las relativas a la cesión de datos a terceros o la utilización para fines indeterminados, como es la publicidad o la promoción comercial, que se puede referir a cualquier tipo de actividad, de forma que pasen a formar parte del contenido esencial de ese contrato.

Si ese contrato es la prestación de un determinado servicio a la sociedad de la información, ¿qué tiene que ver con el objeto de ese contrato el compromiso ineludible de siempre y en todo caso tener que asumir la posibilidad de que se reciba publicidad propia o de terceros?

Esto es contrario al principio de calidad de datos y es contrario al principio de finalidad.

Y, en el ámbito en el que trabajamos cabe la posibilidad de revocar ese tipo de cláusulas y, en su caso, esto ya no es una cuestión de protección de datos, de llevar a los tribunales hasta qué punto son congruentes con la finalidad del contrato.

Y el hecho de que se produzca, creo que no se puede comparar a la hora de hacer valoraciones en esta materia, el hecho de que haya tratamientos ilícitos con las empresas que tratan de realizar tratamientos lícitos.

No se puede justificar que las empresas que quieren realizar tratamientos lícitos tengan un margen de maniobra superior, porque sino, en todo caso, recibiremos tratamientos ilícitos de la información. Y como da lo mismo porque los vamos a retribuir igual, pues ampliemos el campo de trabajo o reduzcamos el sistema de garantías cuando se pretende hacer un tratamiento ilícito.

Es verdad que hay que buscar una situación equilibrada, pero ese equilibrio no puede tener como punto de referencia la conducta de los que actúan ilegalmente.

Y en lo que se refiere a la leyenda, efectivamente es necesario delimitar qué es Spam. En la legislación de la Unión Europea el Spam se articula como una comunicación de carácter comercial directo o indirecto.

Probablemente esta promoción que usted recibió, desde el punto de vista de esa normativa tendría que ser considerado Spam, auque el que la emite voluntaria o directamente por sí mismo asegure que no lo es.

Ponente: Katitza Rodríguez Pereda.

Yo quisiera dar una sugerencia como consumidor o ciudadano mexicano.

¿Actualmente se están discutiendo proyectos de ley en tu país en México sobre este tema?

Sería bueno que tomen conciencia para que se incluya el conocimiento previo informado que tal vez algunos sectores como la industria no están interesados en preservar en la ley, que todo el mundo nos involucremos y que también que seamos conscientes que en casi todas las transacciones que realizamos día a día depositamos y soltamos nuestros datos personales que pueden ser utilizados e

incorporados en una base de datos e interconectados con otras bases de datos.

Muchas veces el tratamiento de datos personales es invisible al ciudadano, el ciudadano no sabe que ha sido marginado. Uno va a una entrevista de trabajo y te dicen no, no te contrato. Y el empleador tiene toda una base de datos y por ahí ha visto tu récord médico y a raíz de eso ha tomado una decisión de no contratarte.

Tú nunca te vas a enterar porque eso a veces es invisible al ciudadano. Entonces hay que ser conscientes y responsables en todo momento que uno entrega o llena una forma, una ficha, que rellena sus datos con su nombre, teléfono y pensar si efectivamente esos datos son importantes para el servicio que está contratando o le están pidiendo información adicional. Eso es todo.

Pregunta: Alejandro Coto. TEC de Monterrey.

Yo tengo un par de reflexiones que quiero hacer junto con la mesa y, con todo respeto que se merecen, pero yo siento que el tema de Internet en estos últimos 20 años se ha venido autorregulando y el Spam, se va a autorregular tarde o temprano. Y yo quisiera observar que en lo personal, Alejandro Cota, no agrede un Spam mis datos personales, al menos de que haya dado mi dirección de correo, pero soy muy libre de cambiarlo cuantas veces quiera y de cambiarme de proveedor.

Sin embargo sí me extraña y me llama la atención que no estemos cuidando el hecho de la identidad. Uno de los crímenes más fuertes que hay al día de hoy es el robo de identidad y eso sí está agrediendo mis datos personales, y el robo de la identidad no se debe a quién le di o no le di mis datos, si no se debe a cuál es el nivel de seguridad que les estamos solicitando nosotros como sociedad o nosotros como esta red que se está formando, a las dependencias gubernamentales o todas estas organizaciones a las cuales nosotros les damos la información.

Hay organizaciones internacionales en el área de Estados Unidos o ITSEC en el área de Europa en donde sí marca niveles de seguridad de los sistemas de información.

Entonces a mí me gustaría saber qué es lo que opina la mesa al respeto, porque yo sí esperaría que la mesa estuviera preocupada por ver cuáles son las medidas de seguridad que estaríamos solicitándole a las organizaciones que posean estas bases de datos, porque creo que es inevitable que las tenga.

Hoy, después del terrorismo que estamos viendo en el mundo, la identidad es fundamental.

Cuando yo llego a un aeropuerto y casi me desvisten y me piden mi pasaporte y revisan que sea yo quien digo ser, me da seguridad de subirme al avión al que me voy a subir, de lo contrario me daría miedo hacerlo. Sin embargo, qué tanto está agrediendo realmente mis datos personales en contra de la seguridad que todos queremos vivir.

Entonces, vuelvo a plantearlo. ¿Cómo vamos a hacer para que estas organizaciones que poseen mis datos personales realmente tengan niveles de seguridad de los más altos?

Hoy en día los sistemas de identidad de los gobiernos no se preocupan por estos niveles de seguridad.

En México estamos viviendo un proceso, que no sé si se va a llevar a cabo o no. Hacienda es precursora en esto, que era la cédula de identidad para el país.

Sin embargo el nivel de seguridad que estaban planteando en sus estándares era nulo. Nada más decían que hubiera un nivel de seguridad, un estándar internacional, cuando es considerado por Garner Group y por todas las grandes empresas que se dedican a investigar estos rollos, que el nivel de seguridad debería de ser un ITSEC E6, que es el nivel más alto al día de hoy en seguridad. Y esto no está casado con ninguna tecnología.

Entonces, dejo mi preocupación en la mesa.

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA–México.

Turno la pregunta al que la quiera contestar, pero sí quisiera hacer un brevísimo comentario.

La cuestión del terrorismo, que se acaba de mencionar, ese es el gran conflicto que me da la impresión de que no nos hemos concientizado y que sí va a hacer falta por parte de la sociedad civil, académicos, universidades, y nosotros los abogados también, que hagamos énfasis en el límite que debe de haber precisamente entre lo que es la cooperación judicial para efectos de combatir el terrorismo, el narcotráfico, lavado de dinero, tráfico de personas, tráfico de emigrantes, etcétera, y el respeto a lo que son los derechos humanos de los individuos, porque so pretexto de proteger precisamente ciertos intereses, la verdad es que se alude en la exposición de motivos de estas convenciones internacionales; por ejemplo la de Delincuencia Organizada, que los Estados han perdido control y autoridad, y que entonces la única manera es convencer a los que llaman arrepentidos, que son los que finalmente forman parte del grupo, que son narcotraficantes, o en fin, cambiarles su identidad, darles una vida distinta, ahí está toda la temática.

Y ya con eso gozan de impunidad y finalmente pueden combatir con los datos que les dan al resto de los integrantes del grupo, ya se habla del grupo delictivo. En estas situaciones no hay respeto, jamás se alude en esta Convención Internacional del respeto a la privacidad.

El secreto bancario, expresamente se dice: No opera para esos efectos. Ya con eso uno se puede imaginar que no hay mucha protección ante la cual argumentar frente a precisamente esos esfuerzos internacionales en materia penal, sobre todo terrorismo y narcotráfico, que hacen de lado totalmente los derechos de la persona humana.

Yo me acuerdo que en un foro de discusión se presentó la iniciativa del Presidente, en materia penal, precisamente se distinguían dos tipos de individuos: los que cometen delitos graves y los que no. Los graves no gozan de ningún derecho, se permite la denuncia anónima. Obviamente no se le informa cuál es la causa de la denuncia, vemos que goza del derecho de la presunción de inocencia, en fin, no hay derecho a la privacidad, exactamente igual que en la época de la Inquisición, más o menos ahí podemos ubicar a los que suponen o presuponen que son delincuentes.

Sí hay que tener claro que en estos momentos de presentarse una iniciativa por el buen manejo de los datos personales hay que tomar en cuenta que además del buen manejo y los otros objetivos que se tengan, que es mejorar el comercio internacional, el combate a narcotráfico, la transparencia, etc., finalmente las normas jurídicas están destinadas para gobernar a individuos, a personas y no a instituciones, bueno, obviamente instituciones, pero el principal gobernado, objeto de la norma son individuos y si no se van a respetar sus derechos humanos las cosas no andan bien.

Ponente: Alfredo Reyes Krafft.

Yo quisiera nada más comentar una cosa muy pequeña y es en relación al tema que tú planteaste, es decir, estás hablando de robo de identidad, en dónde va a constar esta identidad, es decir, hoy por hoy una identidad puede constar en una credencial que me puede emitir una autoridad y si yo robo esa credencial o la falsifico, pues de alguna manera estoy usurpando tu identidad.

También esa identidad puede constar en un dato, en un dato pero no necesariamente todos los datos constituyen una identidad y yo creo que aquí habría que hacer un cierto distingo, obviamente es muy importante tipificar como delito, pero no todos los datos que puedo tener referidos a ti van a constituir tu identidad.

Y tercero, otro medio para poder identificarte o para poder definir tu identidad es a través de un esquema biométrico, es decir, conocer que tú eres tú a raíz de la aplicación de una huella digital o el iris de tu ojo.

El problema que existe en la práctica en relación con esos elementos es que no existe un estándar hoy por hoy en la materia.

Entonces, mi huella digital a final de cuentas se va a traducir en un dato, en un uno o cero, y en ese sentido, pues, corre el riesgo de que pudiera ser apropiado por un tercero e interactuar en mi nombre.

Entonces, obviamente se debe de interactuar, se deben de establecer penas muy fuertes en ese sentido y se deben establecer criterios, claro, de custodia de todos aquellos datos que puedan servir para identificarme, que acrediten de alguna manera directa o indirecta la identidad.

Completamente de acuerdo contigo.

Ponente: Jesús Rubí Navarrete.

Yo le diría en lo que se refiere a la parte de seguridad. Efectivamente hay que buscar equilibrios en todos los casos, por ejemplo, en el caso de las investigaciones criminales, nosotros hemos tenido atentados tremendos en Madrid que han implicado su resolución, el tratamiento de determinados tipos de datos de comunicaciones electrónicas.

Pero ese equilibrio se puede contar, se puede encontrar, hemos estado analizado qué tipos de datos son los necesarios para poder realizar ese tipo de investigaciones, cómo no es necesario acceder al contenido de las comunicaciones para hacer ese tipo de investigaciones, hemos estado analizando para qué finalidades se pueden permitir esos accesos, porque no es lo mismo permitir acceso a determinada información para perseguir el terrorismo, que poder utilizar esa información, pongamos por caso absurdo, para perseguir sanciones de tráfico.

Entonces, aunque todos sean fines de interés público, hay que acotar las finalidades y hay que establecer plazos máximos, en su caso, del tratamiento de esta información.

¿Y a qué lleva todo esto? Pues a que desde el punto de vista de la seguridad es imprescindible que las medidas de seguridad sean de un nivel elevado, por dos motivos: Primero, porque esta una información muy sensible, inclusive desde el punto de vista de quien la utiliza para hacer investigaciones criminales y si se producen alteraciones en esa información, las propias investigaciones criminales pueden fracasar. Por tanto, hay que mantener íntegra la información y eso exige un nivel de seguridad elevado.

Y, en segundo lugar, porque hay que controlar adecuadamente quiénes son los usuarios habilitados para acceder a esa información y poder evaluar e impedir que accedan, por ejemplo, nuevas ideas sobre el terrorismo, usuarios no autorizados, y ellos nos vuelva a llevar a la necesidad de que las medidas de seguridad sean de un nivel elevado.

No se pueden poner en marcha proyectos que implican un riesgo desde muchos puntos de vista, no sólo desde la protección de datos personales para el tratamiento de la información, si no se está dispuesto a asumir que tienen que tener unas medidas de seguridad técnica y organizativa de un nivel elevado.