

Informe sobre la 34° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad

Punta del Este, 23 y 24 de octubre de 2012

Prof. Dra. Esc. María José Viega

La 34° Conferencia de autoridades de protección de datos y privacidad se desarrolló bajo el lema “privacidad y tecnología en equilibrio”, partiendo de la base que en Uruguay fue la Agencia para el desarrollo del Gobierno Electrónico la Sociedad de la Información y el Conocimiento (AGESIC) quien impulsó la Ley de protección de datos, ante la necesidad de dar seguridad jurídica y respetar la privacidad de los ciudadanos en el intercambio de datos a consecuencia de los nuevos procesos de gobierno electrónico. La protección de datos cobra relevancia históricamente a consecuencia de la incorporación de las tecnologías al procesamiento de los datos personales, llegando al día de hoy al enfrentamiento con la llamada “big data”, grandes bases de datos personales en manos de grandes corporaciones, públicas o privadas.

Se pretende, por tanto, plantear el equilibrio entre la privacidad de las personas y la tecnología, considerando que ésta última, además de presentar día a día nuevos desafíos, es también parte de la solución a muchos de los problemas que debemos enfrentar.

El programa se inició bajo esta consigna con tres conferencias, las que estuvieron a cargo en primer lugar del Ing. José Clastornik, como representante del sector público y miembro de la autoridad de protección de datos uruguaya. La segunda conferencia estuvo representada por el sector empresarial, contando con la presencia de Brad Smith, Consejero General y Vicepresidente Ejecutivo de Asuntos Legales y Corporativos de Microsoft Corporation. Por último, el Prof. Wolfgang Kilian representó al sector académico.

Me voy a centrar en la conferencia de Brad Smith, quien inicia su exposición preguntando: ¿Sigue importando la privacidad? A lo que responde que evidentemente sí, porque estamos aquí para discutir sobre este tema. Smith trabaja en una organización donde se centran en el uso de la información. Comenta que algunos dicen cómo puede ser Facebook tan importante si todavía sigue importando la privacidad. ¿Qué ocurrió en los últimos 5 años? My space tiene menos usuarios, en cambio Facebook tuvo un crecimiento exponencial. ¿Por qué ocurrió esto? El conferencista entiende que hay una serie de razones. Facebook incorporó una restricción de privacidad por defecto. Solo se comparte el perfil a los amigos y a las personas que se le quiere mostrar. A la gente le importa el tema de la privacidad, pero esa no es toda la historia, también sugiere que la gente está pensando en la privacidad de una manera diferente, pero tenemos que plantearnos acerca de la nueva forma en que la gente está pensando. La historia de la tecnología es la historia de los cambios en la sociedad.

Destaca que el Presidente Barack Obama captó parte de este problema. La privacidad no es un valor perimido. La declaración más importante quizá sea la de Sonia Sotomayor de la Corte Suprema de Justicia (US), durante más de un siglo la gente en Estados Unidos había buscado las respuestas en la Constitución. Si se cambia la palabra secreto por la palabra privacidad el significado no cambia. El secreto sigue siendo un pre-requisito de la privacidad. La gente se concentra menos en el secreto, hoy se da muchísima información personal, pero eso no quiere decir que no les importe mantener cosas privadas. La gente quiere decidir con quien comparte la información.

El expositor recalca que todos sabemos que no es nada sencillo, porque no podemos olvidarnos de la innovación. Esto es cotidiano en el sector de la tecnología. La big data es un problema, hay que tener en cuenta los términos de búsqueda. Por ejemplo, que medicamentos toma una persona, toma antidepresivos, si toma dos medicamentos de los más comunes que prescriben los médicos, puede tener ciertos efectos secundarios.

Otro tema en que hace hincapié es en la lectura de un aviso de privacidad, que nos lleva unos 10 minutos, si lo multiplicamos por 1462 avisos de privacidad por día, necesitaríamos 76 días de nuestra vida dedicada a leer avisos de privacidad.

Smith ofrece algunas ideas sobre “Do not track” (DNT). DNT es una posibilidad del sistema operativo de Microsoft. Han tenido que pensar mucho en este tema y han tenido que tomar algunas decisiones. ¿Qué quieren los clientes? En Microsoft se valora la relación con los clientes, pero los clientes quieren tener tecnología de avanzada. La empresa quería innovar y dar nuevos beneficios de privacidad. Cree que tomaron la decisión correcta cuando decidieron habilitar el DNT en sus aplicaciones, pero cree que no es lo único que tienen que hacer. Quieren que la w3c adopte un estándar. Cree que el mundo de la privacidad va a ser un mejor lugar si todos conocemos que debemos apagar el DNT y cree que los consumidores deben tener un sistema sencillo para cambiar la configuración. Como empresa, entiende que tienen la obligación de que los consumidores tengan claro que deben ser informados. La tecnología ha cambiado, los usos y necesidades de los consumidores han cambiado. Necesitamos reunirnos y asegurarnos que la innovación de la tecnología asegure la privacidad de la gente.

La Conferencia continua con la primer sesión plenaria acerca de la sociedad de la información, para analizar las nuevas tendencias y la importancia de la privacidad en esta sociedad signada por el manejo permanente de los datos personales. Posteriormente, se desarrollaron una serie de paneles en los cuales la tecnología es muy importante, como es el caso de gobierno electrónico, geolocalización pública y privada, e-salud.

Jesús Rubí, de la Agencia Española de Protección de Datos, moderador del panel de e-salud comienza diciendo que ésta abarca una diversidad de ámbitos y que muchos de ellos se encuentran interrelacionados. El que se ha visualizado con mayor énfasis es la Historia Clínica Electrónica (HCE), pero también se ha tratado

la receta electrónica, la tarjeta sanitaria electrónica o los servicios de computación en la nube (*cloud computing*) para la prestación de servicios de salud.

Un tema relevante es el consentimiento en la HCE: ¿tiene que depender del consentimiento del paciente o del profesional sanitario?, ¿es posible que haya habilitaciones legales que excluyan estos consentimientos?, ¿ha de estar vinculada a intereses públicos? También hace referencia al acceso y la seguridad de la HCE. Es imprescindible una identificación fiable del paciente y una definición muy precisa de los usuarios con acceso autorizado.

Se consideró la receta electrónica, considerando su fin básico que es la dispensa de medicamentos. Sin embargo, se abre también un abanico de posibilidades, como por ejemplo la evaluación del médico sobre la prescripción y uso racional de medicamentos, el acceso por el farmacéutico a prescripciones anteriores, el acceso del farmacéutico a la HCE para labores de fármaco-vigilancia, entre otras.

Finalmente, el cómputo en la nube plantea una problemática importante con la relación al tratamiento de datos en general, que resultan aumentados por tratarse aquí de datos especialmente protegidos.

Un segundo bloque de paneles analiza las diferentes herramientas al servicio de la privacidad, como son las herramientas de concientización y difusión, provocando con la pregunta si estamos preparados para una vida 3.0; herramientas forenses, teniendo en cuenta lo que los dispositivos dicen de nosotros, temas ambos relacionados con la llamada Internet de las cosas y por último, herramientas de cooperación, un camino posible y efectivo en un mundo globalizado, en el cual los datos circulan más allá de las fronteras estatales.

El segundo día se inicia con dos bloques de paneles, el primero vinculado a temas tecnológicos y el segundo enfocados en aspectos jurídicos. Se plantean así los siguientes temas: marketing comportamental en línea, biometría y smart data en primer lugar. En un segundo bloque se analiza la problemática del consentimiento informado como principio y pilar fundamental en los sistemas de protección de datos, la protección de datos como derecho fundamental, en tercer lugar se plantea la discusión de la piratería y privacidad, las discusiones que han existido durante el presente año con las iniciativas SOPA y ACTA, tema que por su actualidad fue objeto de una sesión académica del Instituto. El panel M plantea nuevas iniciativas, presentando proyectos e investigaciones.

La conferencia finaliza con tres plenarios: el primero sobre los diferentes modelos de regulación y privacidad, en segundo lugar sobre la nueva normativa europea y por último y como plenario de cierre la situación de la protección de datos en América Latina, el estado en que se encuentra y el planteo de los horizontes que se vislumbran en nuestros países.

Me correspondió moderar el panel final sobre América Latina. Desde el Comité Académico de la organización de la Conferencia entendimos que era relevante

situar a los participantes en el proceso latinoamericano, ya que era la primera vez que la Conferencia se reunía en América del Sur.

América Latina ha tenido un enorme desarrollo normativo y de gestión en los últimos años. La normativa que existe en los diferentes países, tanto a nivel constitucional como legal, así lo demuestra. Existen países con autoridades de control que están iniciando sus actividades y otros países ya han obtenido la Declaración de Adecuación al modelo Europeo.

Este desarrollo comienza en 1980 con la salida de las dictaduras militares. El primer país en incorporar disposiciones específicas fue Guatemala en 1985, seguida por Nicaragua en 1987 y es simbólica la inclusión en la Constitución Brasileña 1988 ya que consagra el Habeas Data.

El Habeas Data se vislumbró como una alternativa para que las personas pudieran acceder a la información que se poseía sobre ellas en las bases de datos existentes, motivo por el cual la doctrina se pregunta si el Habeas Data es una tercera vía o una alternativa al modelo europeo. De esta manera se indicó que, si bien los países de América Latina han mirado hacia el modelo europeo, también han mantenido particularidades y motivaciones diferentes a la hora de aprobar su normativa de protección de datos.

Desde esta perspectiva, el plenario abordó las correspondientes respuestas a las siguientes preguntas: ¿Cuál es la motivación de los países latinoamericanos para regular la protección de datos personales en forma expresa y autónoma?, en qué aspectos se ha innovado?, ¿cuáles son las dificultades prácticas que se visualizan en la aplicación de la normativa? y ¿cuáles son los desafíos de cada país y de América Latina como continente?

Finalmente, he de remitirlos al sitio web de la conferencia www.privacyconference2012.org donde encontrarán las presentaciones y los videos de las exposiciones.