# Informe sobre la asistencia a la 30th International Conference of Data Protection and Privacy Commissioners "Protecting Privacy in a Borderless World"[1]

**Dra. Esc. María José Viega**[2]

Los días 15, 16 y 17 de octubre de 2008 se realizó en la ciudad de Estrasburgo (Francia) la 30th International Conference of Data Protection and Privacy Commissioners "Protecting Privacy in a Borderless World". El presente informe traduce a grandes rasgos el planteo inicial de cada panel y los puntos a discutirse en el mismo, destacando además opiniones de panelistas e inquietudes manifestadas por los asistentes.

La Conferencia se desarrolló en seis paneles. El primero de ellos denominado: **¿Es la privacidad un obstáculo o un activo para el crecimiento de la economía mundial?**

La importancia de recientes escándalos nos permite afirmar la importancia de la vida privada en las empresas. Las empresas deben ocuparse cuidadosamente de la información personal que poseen porque de lo contrario, con el tiempo, pierden la confianza de los clientes. Además, la normativa de protección de datos no siempre es fácil de entender y mucho menos de aplicar.

El panel de oradores analizó si la protección de la privacidad es algo más que una onerosa obligación, si puede convertirse en un activo para la empresa y por tanto ser utilizado también para la beneficio de sus clientes.

---

[1] Se asistió en representación de la Agencia de Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC).

[2] Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UR). Profesora Adscripta de Informática Jurídica. Profesora de Derecho Telemático. Asesora Jurídica de la Agencia de Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). Cursos del Posgrado de Derecho Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Miembro Honorario de la Asociación Paraguaya de Derecho Informático y Tecnológico. Miembro de la Comisión de Derecho Informático y Tecnológico de la Asociación de Escribanos del Uruguay. Miembro del Instituto de Derecho Informático (UDELAR). Coordinadora de la Comisión de Jurisprudencia del Instituto de Derecho Informático. Co-editora del Boletín Electrónico de Derecho y Tecnologías (www.viegasociados.com). Autora de múltiples trabajos de su especialidad y conferencista a nivel nacional e internacional.

Las cuestiones de mayor interés giraron en torno a responder cuestiones como por ejemplo:

a) si el no respeto a la protección de datos y de las libertades civiles dentro de una empresa podría constituir un obstáculo para su crecimiento económico,

b) si el apoyo a la protección de datos y a las libertades civiles puede ser un instrumento económico para la protección de los consumidores,

c) como desarrollar políticas de protección de datos como un activo esencial en consonancia con la calidad de los servicios prestados,

d) como pueden las empresas interactuar para intercambiar las mejores prácticas y nuevos conceptos,

e) el aprovechamiento de la protección de datos para aumentar la competitividad,

d) la necesidad de una industria mundial de normas de privacidad para todos los jugadores.

Se analizó la situación de EEUU y China, respecto al primero se hizo hincapié en el papel de APEC y con respecto a China en la necesidad de la aprobación de una ley de protección de datos.

Se recalcó la apertura del Convenio 108 para los países fuera de la Unión Europea y la importancia de hacer un convenio internacional o una organización internacional que se ocupara especialmente de la protección de la privacidad.

Se puso de manifiesto que si bien se estaba tratando el tema de la privacidad en el sector privado, no era menor la importancia del sector público, porque si bien el Estado puede no tener el peso económico que tienen determinadas empresas es sumamente relevante para el ciudadano, por lo que debe dedicar tiempo y recursos para proteger los datos. Hay que tener en cuenta que los mayores escándalos en relación al tema han provenido del sector público, como la pérdida de datos en el Reino Unido. Se plantean, además, las dificultades a superar por parte del sector público, algunas veces

basado en la autoridad y en un segundo lugar trabajar en determinar la línea divisoria entre lo público y lo privado, que muchas veces no es clara.

**El segundo panel se preguntó si "¿El Derecho a la Privacidad está en peligro de extinción?"**

Actividades como consultar nuestro motor de búsqueda favorito, actualizar nuestro blog o nuestro perfil en las redes sociales, hace que todos los días revelemos más detalles sobre nuestra vida privada, como por ejemplo nuestros hábitos, conexiones, gustos, ocio, nuestra situación económica, opiniones políticas o religiosas, nuestra salud, volviéndonos cada día más transparentes.

Internet permite que busquemos conocidos de la escuela, amigos, que podemos averiguar las indiscreciones de un candidato a una contratación, etc. Internet se ha convertido en una enorme mina de información que puede ser utilizada para una explotación infinita.

El internauta es al mismo tiempo quien publica información sobre sí mismo o sobre otros, pero consciente o no, se convierte en un blanco de estrategias de comercialización.

Nos preguntamos entonces si estamos conscientes de esta ambivalencia. ¿Estamos cada vez más indiferentes a la protección de nuestra privacidad? ¿Realmente revelamos nuestra privacidad en Internet? ¿Podemos ocultar nuestra propia identidad, nuestra personalidad en Internet?

Por tanto, vemos que la vida privada y el espacio público se mezclan hasta que se convierten en uno. Algunos afirman el derecho a la propiedad de sus datos personales, la libertad de determinar sin restricciones el uso de sus datos y, por supuesto, el derecho al anonimato como una cuestión de hecho, ¿realmente tienen esa opción hoy?

Por tanto corresponde analizar si en el amanecer de esta evolución es necesario volver a redactar nuestros conceptos de protección de datos, ¿es necesario reafirmar más que nunca nuestro derecho a la protección de los datos personales como un derecho fundamental? Al renunciar a una parte cada

vez más importante de nuestra vida privada, es probable que el daño, sea un proceso irreversible.

En este momento en que presenciamos el desarrollo masivo de la geolocalización, la aparición de la web 3.0, las nanotecnologías, ¿cómo podemos hacer que los gobiernos y los ciudadanos sean conscientes de esta importante cuestión? ¿Podemos o debemos aplicar los principios de precaución a la tecnología de la información?

Mr. Bruce Schneier comienza su análisis reflexionando sobre Facebook como una nueva forma de socialización, una nueva forma de comunicarnos. Así como dejamos nuestras huellas dactilares por todas partes en el mundo real, también dejamos nuestras huellas cuando utilizamos las computadoras.

Hay que tener en cuenta que se terminaron las conversaciones efímeras, porque cuando conversamos por mail, sms, msn, todas pueden ser grabadas y mantenidas, por lo tanto permanecen en el tiempo y pueden ser recuperadas.

Entonces, hay lugares en que el mundo se convierte en una zona de seguridad aeroportuaria, oponiendo seguridad a privacidad, pero hay que pensar dos veces cuando basamos la seguridad en la identidad.

La dicotomía de la libertad contra el control lleva a que se hable del equilibrio de poderes. La privacidad aumenta el poder de la gente y el secreto aumenta el poder del gobierno. Nadie se siente seguro si se siente expuesto y la realidad es que cada vez se nos juzga más en función de los rastros que hemos ido dejando.

Mr. Mozelle Thompson (Facebook Adviser) manifiesta que no cree que la privacidad esté en peligro de extinción ya que existen muchas personas preocupadas por su protección. Hoy en día existen millones de personas promocionándose, un joven de 20 años es el propio promotor de sus relaciones públicas. Esto no es una dicotomía entre lo que sucede en Internet y fuera de Internet. Facebook no crea un mundo virtual, según sus encuestas el 90 % de las jóvenes entre 13 y 17 años interactúan con gente que conocen personalmente y un 63 % utilizan instrumentos para proteger su privacidad.

El sociólogo Dominique Cardon plantea la ambivalencia con la cual nos manejamos respecto a la vida privada, dice que somos exhibicionistas en

Internet pero que a su vez estamos cada vez más paranoicos. ¿De qué tenemos miedo? ¿Del Estado? ¿De la vigilancia interpersonal? La realidad es que cuanto más se expone uno, más se amplía la red social, esto no es un tema de narcisismo o individualismo, es un aspecto socializador. Tenemos diferentes plataformas en la web2, fabricamos identidades, producimos muestras de uno mismo, se conoce con quien discutimos, que música nos gusta, donde viajamos. Muchas veces nos definimos a nosotros mismos por lo que hacemos, nos disfrazamos para ser representados en tal o cual espacio.

La visibilidad se hace también a través de seudónimos y no del nombre real. Las relaciones se llevan a cabo a través de la ficha que una llena. Esto nos permite ocultarnos. Por tanto, las redes sociales han construido una red de claroscuros, se da mucha información a personas restringidas. Entre los jóvenes muchas veces es una extensión de las charlas cotidianas que excluye a los padres o profesores. Por ejemplo, en MySpace se puede construir una identidad para ese espacio, esto forma parte del juego. En función de la plataforma que utilicemos vamos a tener una perspectiva diferente.

Respecto a las relaciones de sociabilidad, antes había anuncios en los periódicos y en las revistas que no difieren de los actuales avisos de Internet. Puede existir una vigilancia interpersonal en la medida que puedo ver en las fotos que mi pareja habló con XX en una fiesta, o hizo tal o cual cosa.

Cardon entiende que esto no es una moda y por tanto no va a pasar, sino que es un individualismo racional y socializador, es una tendencia social. Hay una diferenciación entre quienes tienen una vida rica y aquellos que tienen una vida muy aburrida.

Se intercambian múltiples opiniones sobre la protección de los jóvenes, sobre las posibilidades de encontrar información por parte de los delincuentes. Se realizan afirmaciones como: usted no cuenta algo que no quiere contar. Se critica a Facebook porque se desconoce el destino de los datos que posee, pero por otra parte se le reconoce el valor socializante. Kohnitamm entiende que no estamos discutiendo si nosotros definimos o no, no es ser o no ser, se trata de controlar o no controlar. Los principios no difieren en la protección de datos. No creo que ésta sea una especie en peligro de extinción, porque estamos en condiciones de ofrecer soluciones técnicas para se proteja la privacidad.

Artemi Rallo opina que no es admisible el paralelismo entre las redes sociales y la vida real. En Internet se hace una vida distinta, complementaria a la real. Se decía que un 71 % de los usuarios de Facebook utilizaban mecanismos de privacidad, en España hemos hechos encuestas sobre si se leen las condiciones de privacidad y el 70 % dicen que sí. La realidad es que uno de cada millones de accesos puede ser que lea las políticas de privacidad y los entiendo.

En Alemania se presentan dos posiciones, por un lado quienes dicen que a la gente no le interesa la privacidad y por otro los que entienden que es necesario regularla.

**El tercer panel reflexionó sobre la "Seguridad: ¿hacia una base de datos de identificación en todo el mundo?"**

Se plantea el surgimiento de centrales de bases de datos de identificadores biométricos en Europa y en otros continentes: características biométricas como "identificadores únicos universales", se han convertido en indispensables para la identificación de los delincuentes, extranjeros, los viajeros, los ciudadanos, los votantes, los inmigrantes ilegales. Se utilizan, entre otros, con fines de seguridad en la lucha contra el robo de documentos, para la simplificación de los procedimientos administrativos. Las razones para usar la biometría abundan.

Desde los acontecimientos del 11 de septiembre en la mayoría de los países existe una tendencia a reforzar las medidas de seguridad interna y el control de los flujos migratorios, lo que se traduce en particular en un acceso más amplio por las fuerzas del orden a los archivos, las redes de comunicación, y especialmente datos de tráfico de los usuarios de Internet, sino también en una concepción amplia del desarrollo de la videovigilancia y la biometría.

Con la presión política, los acuerdos de cooperación policial y las normas de interoperabilidad se expanden y aumenta el intercambio de datos, las interconexiones, el uso compartido de datos y la creación de bases de datos espejos.

La identificación de huellas biológicas en la escena de un crimen, poner un nombre en una cara que ha sido capturada en un estadio o en medio de una

multitud, detectar movimientos sospechosos, el comportamiento "anormal" o las comunicaciones de algunos corresponsales, etc … Hay muchas razones que conducen a la identificación de medios para el seguimiento de los individuos.

Mientras que, paradójicamente, el derecho al anonimato, en particular en Internet, nunca se ha destacado de manera prominente, la identidad digital en Internet se debate: ¿cómo me identifico en Internet de manera segura para acceder a una cuenta bancaria, para comprar a través de Internet, para probar que uno no es un menor de edad? El sector privado también está buscando una identificación segura y permanente de las personas.

En el futuro, las exigencias de la lucha contra el ciberterrorismo y la protección de las infraestructuras va a dar lugar a temer que las personas, cada vez más, se encuentren vigiladas en todas las esferas de su vida cotidiana. En un mundo cada vez más interconectado, donde las empresas privadas se convierten en " agentes ayudantes de la policía", ¿cómo preservar la esfera privada de las personas?

La duda legítima por el aumento de medidas de seguridad para los ciudadanos debe conciliarse con el respeto de sus libertades individuales. Tenemos que hacer frente a un reto importante. ¿Estamos pasando a una convergencia de los procesos de identificación? ¿Cuándo habrá una base de datos de identificación en todo el mundo? ¿Con qué fin, a disposición de quién?

Si todos los datos biométricos de identificación se recogen en una base de datos central, y si cada uno lleva "sus elementos biométricos", ¿cuál es el interés en tener un documento de identidad, un pasaporte? ¿Cómo reforzar la seguridad, sin inmiscuirse en la esfera privada de las personas? ¿Hay que establecer límites en un mundo interconectado?

Mr. Stavros Lambrinidis reflexiona acerca de quién toma la decisión sobre si ponemos o no cámaras en todas las casas. La proporcionalidad es fundamental a la hora de definir el objetivo. Plantea el problema de ingreso a EEUU, que exige más información que Canadá y Australia, pretendiendo que cada ciudadano dé su consentimiento. El punto es ¿hasta dónde puedo renunciar a mis datos personales? ¿Hay límites al consentimiento? ¿Cómo y

cuándo se pueden plantear? Este es un tema que se va a comenzar a discutir en los años venideros.

**El cuarto panel hace un interesante planteo sobre las redes sociales, el cual comienza diciendo: "Mi nombre es Clara, tengo 14 años, aquí está mi vida privada, mis logros"**.

El caso planteado relata que todos los días después de la escuela Clara se conecta a Internet, se ha registrado en Facebook, su primo –en cambio- ha preferido MySpace. En este sitio, ella no duda en poner fotos de sus últimas vacaciones con sus amigas en la playa, sus actores y cantantes favoritos. Ella participa en concursos y revela sus gustos de vestimenta, ocio, etc. Ella está registrada en la red social de su escuela, pero también en otras. En su perfil ha expresado su interés en los hombres y tiene más de 100 usuarios como sus amigos. Ella pertenece a una treintena de grupos, incluso ha creado un grupo sobre su profesora de matemáticas a quien considera realmente anticuada, los chats con sus amigos en el "muro", a los cuales les dice lo que está haciendo en este momento. Ella comenzó a interesarse en política, expresó sus puntos de vista y se inscribió con el grupo de seguidores de su político favorito.

"Estar en Facebook o MySpace": lo que es más natural ahora, lo que es más "hip"! Además, es libre y se puede decir lo que quiera, conocer gente nueva, hacer muchos amigos, sin sus padres detrás de ella. Pero Clara es consciente de que ella está entregando gradualmente, a todo el mundo, parte de su vida íntima, datos que serán almacenados durante años, que la información que le regala cada día en su sitio favorito puede ser usado para determinar sus gustos, sus hábitos de consumo, su comportamiento y que todos estos datos permitirán definir un perfil de marketing. Que su identidad puede ser utilizada por personas desconocidas que no tengan propósitos muy loables, y si ella ha dado su dirección, sus fotos, algunas personas podrían intentar contactar con ella. ¿Qué pasaría si, en un plazo de cinco años, un empleador descubriera esta información y le pregunte acerca de ella? ¿Ella lee y entiende la política de privacidad del sitio? ¿Qué significa la protección de los datos para ella? ¿Entiende que podría restringir el acceso a su información? ¿Le han sido dados los medios para eliminar sus datos si así lo desea?

La labor educativa debe realizarse rápidamente a los más jóvenes, que son poco conscientes de los riesgos inherentes a la utilización de Internet. Si

no se hace nada hoy en día, las generaciones futuras podrían reclamar mañana que su privacidad no está segura. ¿Cómo perciben los jóvenes su vida privada en Internet? ¿Y los riesgos potenciales de daños a su esfera privada? ¿Cómo hacer entender a los jóvenes la protección de datos? ¿Deben llevarse a cabo campañas de sensibilización? ¿Los propietarios de sitios web tienen una responsabilidad especial en este sentido? ¿Son conscientes de eso? ¿Cuál es su percepción sobre estas cuestiones? ¿Debemos y podemos regular la difusión de sus datos por parte de los menores en Internet?

Mr. Jacques Barrot señaló que Eurobarómetro realizó encuestas respecto a los jóvenes que determinaron que los niños saben más que los padres en relación a Internet. En las escuelas deberían hacerse presentaciones a los niños explicándoles que sucede cuando sus datos llegan al ciberespacio. Destaca la labor del G29 sobre protección de los niños en el contexto escolar. Los bancos de datos, operadores tecnológicos y autoridades judiciales tienen que trabajar conjuntamente. En diciembre de este año la Comisión Europea pretende lanzar un programa sobre protección de datos, para proponer comunicaciones seguras, e involucrará a los privados.

L. Thoumyre (MySpace) manifiesta que uno de los puntos centrales de MySpace es proteger la seguridad de los usuarios. La empresa tiene reglamentos de seguridad y buenas prácticas en el sitio en forma on line. Se está cooperando con autoridades públicas, así como para detectar situaciones ilícitas. En el caso francés se trabaja con organizaciones vinculadas a la infancia. Clara es posible que sea un caso real. ¿Cómo la protegemos? Tenemos medios de capacitación, información y medios humanos. El sistema tiene filtros en cuando a la edad, existen cookies y también se detecta cierta forma de hablar, la forma en que se expresan los jóvenes. Para que alguien sea amigo de un menor de 16 años tiene que conocer su nombre y correo electrónico, por lo cual deben haber tenido un contacto real.

Mr. Leif Stenström comenta que realizaron una encuesta con 125 preguntas a jóvenes menores de 25 años, de la cual surge que el 98 % utilizan las redes una vez por semana y el 85 % una vez al día. Cada semana se reciben 1500 denuncias por Internet. Cada segundo, uno de cada 3 personas han encontrado fotos publicadas sin permiso y uno de cada 5 ha sido acosado sexualmente en Internet.

La información no es la clave para eliminar el riesgo. Hay que cambiar las actitudes de las personas. Esto no se logra repartiendo folletos. Vamos a las escuelas y damos charlas, hacemos juegos, encuestas. Hay que tener cuidado con las campañas porque se corre el riesgo que a los niños o jóvenes les parezca aburrido. Hay que estar dispuestos a cambiar todos los años porque ellos cambian sus intereses año a año. Para cambiar actitudes hay que comparar las actitudes en líneas con las reales. Se les dice a los niños: mira al cruzar la calle, no hables con extraños, etc. Nos acercamos a los padres, a los profesores, etc. Creo que los actores deberían asumir su responsabilidad. Hay muchísimas organizaciones que pueden verse implicadas. La seguridad de los niños es importante, pero sería importante construir polos integrados por distintos tipos de personas, hay que tener en cuenta que la responsabilidad no es solo de las agencias.

A. Plathe entiende que en un mundo sin fronteras, global, universal, necesitamos principios éticos y mejores prácticas para proteger un derecho fundamental. UNESCO está trabajando en la protección de datos personales. La Cumbre Mundial señaló que debía lucharse contra el uso abusivo de Internet. Se han realizado reuniones y conferencias en Asia y África. Hace dos años publicamos un manual sobre nuevas tecnologías y lo que están haciendo los estados en cuanto a alfabetización informática.

Artemi Rallo realiza un punteo de las intervenciones destacando:

a) Las sugerencias a adoptar códigos de conducta;
b) Clara es consciente de los riesgos, pero puede ser indiferente o privilegiar las ventajas de las herramientas;
c) MySpace va en buena dirección en cuanto a identificar el acceso e impedir accesos indebidos. Sin embargo, el tema de los registros por edad parece ingenuo;
d) Respecto a la información y capacitación en este momento está en manos de los proveedores que son ficticios, virtuales y no reales.

El Sr. Thomson responde que en Facebook, aunque también trabajó en MySpace, hay riesgos diferentes según la herramienta que se utilice, hay que distinguirlas con las redes sociales. La protección que Facebook ofrece es real, no virtual, muchas veces trabajan con la policía, en procedimientos reales. Además, en Facebook nadie puede ver la información a no ser que el usuario invite a un amigo y este acepte.

A esta afirmación se le responde que, tanto Facebook como My Space tienen un scriming que hace que todo lo que se deje en los sitios inmediatamente es enviado a Google.

**En el panel número cinco se expuso sobre "El hombre asistido digitalmente, un ángel digital o un diablo digital?"** La tecnología digital es parte de nuestra vida cotidiana. Desde el nacimiento hasta la muerte, el hombre es "vulnerable" y cada vez más asistido por la tecnología digital: pulseras electrónicas para los niños y los pacientes de Alzheimer, asistencia telemétrica y sensores fisiológicos para las personas mayores, servicios de geolocalización para los niños, los datos biométricos de personas imposibilitadas. En un futuro cercano, en Asia, los robots podrían ayudar a las personas con discapacidad, así como a las personas de edad. Esta evolución dará lugar a un "ángel digital" cuidando de nosotros en cada etapa de nuestra vida, en particular los robots de vigilancia de nuestros hijos cuando están solos en casa e instando a que hagan la tarea. Por nuestra propia seguridad y comodidad, se aspira a una "sociedad digitalmente asistida", que podría dar lugar a una sociedad vigilada por medios electrónicos. ¿Podría el ángel de la guarda ser un diablo digital? ¿No es tiempo de reaccionar y elegir la sociedad digital en la que llegaremos a vivir mañana? En Corea del Sur está en desarrollo una carta ética para el uso de robots.

El panel evaluó las justificaciones y los riesgos inherentes a estas nuevas herramientas electrónicas y analizó las condiciones en que podemos aceptar utilizarlas. ¿Cuáles son los proyectos tecnológicos en este ámbito? ¿cuándo damos la bienvenida a la familia humanoide robot? ¿Y el robot dedicado a la vigilancia urbana? ¿La asistencia electrónica es un signo de dependencia o de emancipación y autonomía humana?

El hombre asistido digitalmente: ¿qué límites debería crearse? ¿Cómo preservar nuestra vida privada y las libertades personales y en particular el derecho a la libre circulación? ¿Debemos promover normas éticas? ¿Es suficiente con confiar en el libre consentimiento de cada persona a ser "asistida"?

¿Cómo proteger la privacidad de las personas con respecto a estos nuevos medios de procesamiento de los datos personales? ¿Han de adaptarse

nuestros principios de protección de datos? Como dijo Isaac Asimov, ¿debemos pensar en nuevas normas en el campo de la robótica?

El Prof. Jeroen van den Hoven cuenta que en su universidad trabaja en nanotecnología y que los chips se pueden dar a la gente o poner en las cosas que absorben información del entorno. Por tanto todo va a ser inteligente, hasta las mesas, y vamos a sacar gigas y gigas de información. ¿Esto es bueno o malo desde el punto de vista moral? Tendrán que pronunciarse sobre ello los filósofos. No podemos verlo como un determinismo tecnológico, sino que hay que tomar decisiones. Habrá que adelantarse y tomar decisiones y ser conscientes que, si no las tomamos, serán tomadas por el mundo de la tecnología. Tenemos que diseñar para promover valores, esa es la finalidad en el s. XXI.

Hablamos de valores y ética, pero tenemos que ir al mundo de Internet, de los protocolos y las especificaciones tecnológicas. Hay que introducirlos al mundo de los ingenieros y que sean parte de su trabajo. Una vez que tenemos diseños adecuados ¿cómo sabemos si son los correctos para llevar adelante lo que políticamente se ha decidido?

La privacidad es uno de los valores, pero también son importantes la igualdad y la responsabilidad. Hay que articular estos valores y tenemos que saber por qué es importante defenderlos y analizar cuando entran en conflicto con otros valores. En Europa la gente se divide entre los que están a favor y los que están en contra de la protección de datos. La discusión es entre los liberalistas y los comunitarios. Cada vez es más fuerte el debate y el peso de aquellos que prefieren sacrificar sus libertades individuales en favor de la comunidad. También están quienes prefieren la privacidad y la sobreponen a cualquier otro valor. Debemos hacer un movimiento de vaivén entre políticos y técnicos.

Rodolphe Gelin de CEA Robótica, distingue la robótica incorporada al cuerpo humano de los robots autónomos, éstos últimos pueden transportar personas discapacitadas, para que los trasladen y los enfermeros no tengan que levantar peso.

Un robot tiene que ser fácil de conducir, tiene que ser pertinente en el momento que los necesitamos. El robot tiene que conocer mi vida privada, tiene que tener una descripción de mi mundo, tener una estructura de árbol de

mi familia. Quien tiene acceso a la información del robot va a tener acceso a mi privacidad, por lo tanto tenemos que proteger la información del robot.

**El sexto panel trató acerca de los "Límites y nuevos instrumentos de regulación para el futuro de la privacidad".** En un mundo globalizado la transferencia de datos personales es una característica común. Sobre la base de los principios generalmente aceptados por organismos multinacionales como la ONU, OCDE, APEC, la UE y otros, las instituciones han establecido normas que regulan y limitan el libre flujo de datos. Tanto las empresas como las agencias encargadas de hacer cumplir las leyes tienen que conocer y cumplir con estas normas.

Pero hay que señalar que estas normativas en el mundo empresarial a veces son percibidas como una carga. Muchos países en el mundo no han hecho hasta ahora esta opción y promueven, al igual que los Estados Unidos, la autorregulación, mientras que algunas empresas como Microsoft o Google, recomiendan la introducción de estándares comunes.

Las leyes y las sanciones, las autoridades de control, la protección de los datos oficiales, normas empresariales vinculantes (BCRs), cláusulas contractuales tipo, auditoría, códigos de conducta… En el momento de la globalización de los flujos de datos, es esencial comparar y evaluar la eficacia de estas herramientas y desarrollar una estrategia común y un enfoque armonizado de protección de datos a nivel internacional. ¿Pero qué enfoque y qué herramientas deben ser apoyados?

¿Estas diversas herramientas pueden ser complementarias? ¿Son necesarias para innovar? El panel 5 analizó los actuales marcos normativos para atender las necesidades de las multinacionales y los organismos del ámbito internacional.

Incluso en el caso de los lugares donde la normativa se considera suficiente, se deberían discutir los retos que se plantean para el futuro. ¿Es la normativa vigente suficiente para proteger a los titulares de los datos? ¿Cómo identificar las deficiencias del actual marco jurídico? ¿Cómo regular la protección de datos en el futuro? ¿Cómo promover la autorregulación, a la luz de los retos actuales? ¿Cómo encontrar respuestas globales en un mundo interconectado?

Ms. Michelle O'Neill destaca que los países de APEC no tenían ninguna normativa de protección de datos personales, pero ahora intentan cumplir con estos parámetros, por lo que entienden que el listón está subiendo. Lo que se trata es de tener enfoques y soluciones que cumplan con las disposiciones y las necesidades de los consumidores.

Mr. Peter Cullen se refirió al papel que están asumiendo los consumidores, quienes tienen demasiadas responsabilidades y entiende que eso no está bien. Plantea que el modelo que tenemos no es sostenible porque son regímenes paraguas. Unos dicen que hay que armonizar los principios, pero no creo que sea así, que si bien a veces se solapan ello no es un problema.

Si pensamos en un mundo con más actores y más datos es un inconveniente, porque tenemos regulación sectorial. Otro problema son las identificaciones geográficas, ya que a veces se menosprecia lo que se hace en otros lugares, en Vietnam por ejemplo.

Se pregunta ¿qué pasa con el modelo de las reglas corporativas vinculantes? Entiende que tenemos que evolucionar, porque los modelos están quedando obsoletos y se necesitan modelos que se adapten más, porque tanto los públicos como los privados tienen que rendir cuentas. Y rendir cuentas significa crear confianza mutua, tener una Agencia que valide los avances y que asegure que se están cumpliendo las reglas.

Mr. Jan Kleijssen hizo hincapié en la importancia del Convenio 108 y en la adecuación a la normativa europea.

El Dr. Kai Rannenberg analizó la utilidad de la normalización. Entiende que la protección de la privacidad no es algo caro y exótico y que ésta es una concepción que hay que superar. Se refirió al WT 5 Identity Management y a diferentes niveles de estándares:

- Frameworks & Architectures
    - A Framework for Identity Management (ISO/IEC 24760, WD)
    - A Privacy Framework (ISO/IEC 29100, WD)
    - A Privacy Reference Architecture (ISO/IEC 29101, WD)
    - A Framework for Access Management (ISO/IEC 29146, WD)

- Protection Conceps
  - Biometric template protection (ISO/IEC 24745, WD)
  - Requirements on relative anonymity with identify escrow – model for authentication and authorization using group signatures (new Work Item Proposal)

- Guidance on Context and Assessment
  - Authentication Context for Biometrics (ISO/IEC 24761, FDIS)
  - Entity Authentication Assurance (ISO/IEC 29115, WD)
  - Privacy Capability Maturity Model (New Work Item Proposal)

Mr. Alonso Gómez –Robledo refirió a las actividades de la Red Iberoamericana de Protección de Datos.

Mr. Marc Rotemberg recuerda que fue el Consejo de Europa el que fijó los parámetros para la protección de datos en el Convenio de Estrasburgo. Hoy nos encontramos con nuevas amenazas, gobiernos que tienen listas de personas que no lo saben y no tienen la posibilidad de cambiar eso. Tampoco tenemos que estar a merced de la industria, pero hay líderes que les resulta fácil sacrificar nuestra privacidad en aras de su autoridad.

A la pregunta ¿cómo se relacionan los nuevos modelos con los antiguos principios? Cullen responde que los principios siguen siendo los mismos, pero tenemos que cambiar los modelos y para ello tenemos que ver cómo funciona el flujo de datos.

¿Cómo hacemos para que dentro de 10 años sigamos con las directivas de protección de datos? Hay que responder a través de las reglas corporativas vinculantes. El G29 ha trabajado en este tema y parece muy interesante por lo que se debería tener una especie de estandarización.

Mr. Jan Kleijssen entiende que hay que poner el énfasis en el Convenio 108 y en su protocolo adicional, que la ratificación del mismo podría ser la base de cualquier otro acuerdo internacional.

Montevideo, noviembre 2008