Informe sobre la 35° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad

Varsovia, 23 y 26 de setiembre de 2013

Prof. Dra. Esc. María José Viega

La 35° Conferencia de autoridades de protección de datos y privacidad se desarrolló bajo el lema “A compass in turbulent world”, en la ciudad de Varsovia (Polonia). Entre los días 23 y 24 de setiembre se realizó la sesión cerrada de autoridad de protección de datos y los días 25 y 26 la sesión abierta al público.

El tema de la sesión cerrada fue “appification” of society”, lo que podemos traducir como las aplicaciones en la sociedad. Las aplicaciones son aquellas, que por ejemplo, se llevan en el teléfono móvil, se ve una imagen de una persona dormida y el sistema pasa mensajes sobre su estado (sleep rhythm) o running app, video apps (product advertisement), torch apps, etc. ¿Qué es lo que mandan y envían las aplicaciones? Envían datos que sirven para controlar, fecha, hora y hacer funcionar ciertos servicios, pudiéndose utilizar datos muy variados. La aplicación controla todo, el Androi en dispositivos móviles o Windows.

Las aplicaciones están en todos los ámbitos de nuestra vida haciéndola más divertida. Pero recopilan mucha información personal y en la mayoría de los casos los usuarios no conocen toda la información que recopilan y trasmiten.

La privacidad debe tomarse en cuenta desde el inicio de las aplicaciones y lograr que los usuarios tengan mayor confianza. Es importante que funcionen mecanismos de autoregulación, además de los supervisores del mercado.

Durante el año 2014 las autoridades van a intentar llegar al sector de las aplicaciones para que tomen en cuenta la privacidad, se comenzará con un diálogo intentando que comprendan la importancia de incorporar la privacidad desde el diseño, pero están dispuestos a hacer cumplir las disposiciones legales.

También se analizó como los partidos políticos recopilan información y utilizan los conocimientos de marketing. En Estados Unidos hay sistemas legales, hay libertad de expresión en éste ámbito, sin embargo hay países donde la ley es más restrictiva.

En la sesión cerrada las Autoridades de Protección de Datos aprobaron ocho resoluciones sobre diversos temas:

1. Acreditaciones como miembros de la Conferencia de: Mauritius, Kosovo, Bs.As. (Argentina).

2. Reafirmó la Declaración sobre “Profiling” (Perfiles) de Uruguay.

3. Dirección estratégica de la Conferencia (Grupo de Trabajo Plan Estratégico 2014-2015).

4. International Enforcement Coordination (International Enforcement Coordination Working Group).

5. Protección de datos de anclaje y protección de datos en el derecho internacional.

6. Práctica de apertura de datos personales.

7. Educación digital para todos.

8. Seguimiento en la web y privacidad.

La **apertura de la Conferencia** abierta estuvo a cargo del Ministro de Administración y Digitalización de Polonia, Sr. Michat Boni, quien hizo hincapié en la sensación de libertad que se vive en el mundo de hoy, pero que también provoca amenazas y por ello es necesario analizar la seguridad y la privacidad. Entiende que la privacidad no puede lograrse violando derechos básicos y es necesario pensar en qué estándares son necesarios. Cree que los códigos de conducta son una buena manera de resolver la problemática de las empresas, pero es necesario tomar en cuenta los múltiples riesgos existentes en virtud de que no todas las empresas se ocupan de la protección de datos personales. Afirma que el punto clave en estos procesos es la concientización, por lo que se debería trabajar con las ONGs en crear conciencia, como una forma de resolver los problemas que se presentan.

El primer Plenario de la Conferencia se denominó **Privacidad como un valor cultural**.

Igor Janke, moderador del panel comenzó preguntando: ¿Quién tiene Facebook? ¿Los que tienen Facebook –éramos la mayoría- colocan información personal y fotografías? Entonces, ¿cómo podemos defender la privacidad de otros si no defendemos la nuestra? ¿Habrá algo todavía por proteger?

El Profesor Hiroshi Miyashita, de Derecho de la Universidad Chuo de Japón, planteó que la privacidad depende de las épocas y de los lugares, porque la privacidad refleja la parte cultural y social de una sociedad. He hizo hincapié en que en 1890 se defendía la privacidad como un derecho fundamental y se preguntó: ¿cómo defender la privacidad actualmente en cada sociedad? Dio como ejemplo que en Francia no quieren hablar de los salarios, que se sepa cuánto ganan, pero las mujeres se quitan los sostenes; y por otra parte mientras que los americanos quieren ser famosos, los franceses quieren ser olvidados. Con estos ejemplos afirmó que hoy en materia de privacidad es necesario tener en cuenta el lugar y el momento histórico. Contó que en Japón es un valor el conocerse a sí

mismo y la expresión del individualismo (aunque no es una cultura individualista) y creen que su vida privada debe sacrificarse por el bien de la sociedad. Resaltó la importancia de la confianza, la cual no tiene límites. Los sellos de confianza son reconocidos en China y en Japón. Planteó la posibilidad de cooperar con la Unión Europea, ya que hoy en día es una práctica comunicar las violaciones de protección de datos. Concluyó que la cultura de la privacidad es muy importante, que Japón ha aprendido mucho, que las Directivas de la Unión Europea y el Convenio 108 son fuentes de la cultura de la privacidad, porque todos vivimos en la aldea global y todos tenemos los mismos retos.

En segundo lugar, expuso el Profesor de Norwegian Research Center for Computer and Law, Department of Private Law, de la Universidad de Oslo – Noruega, Lee Bygrave, quien entiende que la cultura es importante en materia de protección de datos. Manifiesta que las personas adoptan estrategias para mantener distancia, que todos nos damos cuenta de la importancia de la protección de datos, pero es algo que se olvida en la vida diaria. Habló de la liberación de la cultura, entendiendo que prevalecían los valores del grupo a los personales. Los países de Asia-Pacífico están pensando en la cooperación.

Finalmente, el Ministro Michat Boni, planteó que nos diferenciamos en la forma de poner límites a la privacidad, estamos perfilados de acuerdo a nuestras preferencias, hay un cambio sustancial de valores. Pone como ejemplo la posibilidad de acceder a Wikipedia y se pregunta ¿cómo vemos la privacidad en este momento? Alguien protege los datos porque antes alguien los ha puesto de manifiesto. Los datos son la moneda de cambio en Internet. Entiende que el mecanismo que nos guía es hacernos públicamente conocidos, por ejemplo ¿Quién tiene más ME GUSTA? Hay personas que dedican mucho tiempo a las redes sociales y se han convertido en algo indispensable en su vida social. En una encuesta se ha determinado que los internautas si tienen que elegir entre el alcohol e Internet, o sexo e Internet, eligen Internet. Entiende que la privacidad no está muerta. Las personas quieren difundir su autoexpresión sin límites, pero se necesitan códigos de conducta y políticas de empresas. A los nativos digitales no les quita el sueño que puedan dar sus datos personales. Entiende que deberíamos hablar de un marco de privacidad, cree que no existe un conflicto entre el sistema regulatorio y por otro la creación de espacio de libertad de movimiento, intercambio de ideas, etc.

Se le pregunta al Prof. Miyashita: en virtud a que la privacidad y la confianza son nociones similares y acceder a los datos en la red es importante, ¿qué se debe hacer para asegurar la confianza pública? El profesor responde que cuanto más abierta es la postura ante el gobierno, éste es garante de la confianza de las personas. La confianza en las organizaciones se ve siempre más vulnerable cuanto más abierto se está. Entiende que deberían abrirse los datos públicos a la sociedad. Por otra parte, hay que proteger a los individuos frente a las autoridades públicas.

También se realizan diferentes aportes, entre ellos se opina que:

a) La postura abierta elimina la confianza.

b) Las personas necesitan que se proteja su privacidad para tener confianza.

c) A los jóvenes no les preocupan sus datos personales porque no tienen datos que proteger, no tienen datos de salud, porque están sanos, no tienen secretos profesionales, porque no trabajan, etc.

d) La falta de cultura abierta no es sinónimo de baja seguridad.

e) Los nativos digitales son más abiertos porque conocen más los medios.

El Panel **Interoperabilidad entre las regiones** contó con la participación de Daniéle Chatelois (APEC) quien hizo referencia a que existen veinte economías nacionales unidas para colaborar en metas económicas y desarrollar proyectos de negocios. También tienen proyectos de regulación, siempre mirando por encima de las fronteras. Para poder obtener sus metas el grupo intenta hacer un catálogo, un código de conducta, un sistema voluntario. Existe un certificado de privacidad en el cual se evalúan las empresas de acuerdo a nueve principios. Para que sea fidedigno se diseñó una serie de mecanismos de control para que se pueda someter a la empresa a un escrutinio profundo.

Michael Donohue (OCDE) manifiesta que la OCDE ha realizado una guía sobre la forma de actuar en Internet. Maneja tanto la cooperación nacional como internacional. Se plantea: ¿cómo alcanzar la interoperabilidad? Después de tener constancia de como se observa a los ciudadanos, la OCDE ha pretendido desde los años 70 no solo asegurar la interoperabilidad, sino también el flujo internacional de datos. Entienden que la interoperabilidad no es un concepto técnico ni legislativo, lo tratan en un nuevo capítulo que inicia con la privacidad por diseño.

Sophie Kwasny (Consejo de Europa) explica que los objetivos son consolidar el derecho y por otro obtener mecanismos de control. En el convenio no hay medidas de control y por eso es necesaria su modificación. No se pretende introducir detalles que puedan ser complicados para los Estados y que obstaculicen su firma. Es necesario alcanzar un nivel de coherencia entre el ámbito público y privado. El uso del ámbito doméstico, dentro del hogar es la única exclusión. También destaca que un Tratado Internacional es el único documento vinculante entre los Estados. En las modificaciones al Convenio 108 hay disposiciones sobre todo lo que se refiere al mecanismo de control.

Jean Philip Albrecht (Member of the Greens/EFA group. Rapporteur for the General Data Protection Regulation in the European Parlamient), expone sobre el Reglamento Comunitario. En Bruselas, en el Parlamento se está debatiendo sobre el acceso a datos, por ejemplo en el sistema Swift bancario. Se pregunta: ¿cuál es la quinta esencia de estos derechos? ¿Qué sucede cuando se violan? ¿Qué sucede con países con los cuales no tienen ningún tipo de influencia? Los países europeos se encuentran en el corazón del debate y de los cambios y se está a la

vanguardia de la protección de estos derechos. Se están buscando las mejores soluciones y están comprometidos para alcanzar un consenso. El desafío es cómo asegurar los derechos individuales en el medio digital. Primero habría que decir cuándo se van a ejecutar esos derechos respecto al individuo, sobre todo si sus datos están protegidos.

El panel referido al **Mutuo reconocimiento entre diferentes tradiciones de protección de datos** contó con la participación de Blair Steward (Assistant Privacy Commissioner, New Zealand), quien expresa que la Declaración de Adecuación no se trata de un mutuo reconocimiento, porque es la Unión Europea la que reconoce a un país. No hay mutuo acuerdo.

Willem Debenckelaere (President of Privacy Commissioner, Belgium) entiende que el sistema de reconocimiento mutuo ha dado frutos positivos. Sin embargo, no solo se trata de oportunidades, sino de visualizar también los riesgos y debilidades, porque no tienen hoy reglas corporativas vinculantes. Cree que existe una gran necesidad de tener un marco legal y el reconocimiento mutuo es algo más que un instrumento. Hay que recordar la existencia de los tribunales arbitrales y su utilidad. Hay que tener en cuenta la guía de la OCDE de 23 de setiembre de 1980, el Convenio 108, la Declaración de la 27° Conferencia de Montreal en 2005, la Resolución de Madrid de 5 de noviembre de 2009 y la Resolución de Varsovia del 25 de setiembre de 2011.

Giovanni Butarelli (Asistente del Supervisor Europeo de Protección de Datos) se plantea si la terminología reconocimiento mutuo es el término más apropiado. Entiende que sería mejor hablar de convergencia de las normas regionales, también podría hablarse de interoperabilidad. El Libro Blanco de Estados Unidos en el 2012 define el mutuo reconocimiento.

Felipe Rotondo (Presidente de la Unidad Reguladora y de Control de Datos Personales, Uruguay) hizo hincapié en los procesos de adecuación, entendiendo que respecto a la Declaración de Adecuación de la Unión Europea no puede considerarse la declaración en forma aislada y por lo tanto un acto unilateral, ya que se dicta a solicitud de un país, el cual ha decidido seguir la línea europea en materia de protección de datos.

Joseph Alhadeff (Vice President of global Public Policy and Chief Privacy Strategist, Oracle), manifiesta que es importante pensar en una relación de muchos con muchos.

El panel referente a **La protección de datos en el derecho comercial** contó con la participación de Rafael Trzaskowki (Spokesman on Constitutional Affairs), quien manifiesta que hay que prestar atención a los problemas del Safe Harbor, es un sistema positivo aunque haya actualmente un problema de confianza. Los Convenios Internacionales, el nuevo reglamento, tienen que prever una actitud mutua.

Anna Fielder (Trustee and Chair, Privacy International) hace hincapié en el hecho de que el Convenio 108 es ejecutable y vinculante. Se ha dicho que no es útil ratificar el convenio, pero entiende que ratificar un derecho humano es muy importante y les solicita a los países que lo consideren. La tecnología va cambiando en forma vertiginosa, si se tienen estándares internacionales es posible ir adecuándose.

Christopher Wolf (Director, Global Privacy Practice, Hogan Lovells US LLP and Leader, Coalition for Privacy and Free Trade), entiende que deberíamos tener mecanismos vinculantes para poder aplicar las normas y recuperar la confianza en el comercio internacional. Cree que los europeos deberían hacer algo para protegerse. Estados Unidos no tiene un sistema como la Unión Europea, pero asegura y garantiza una protección completa, en cuanto a la aplicación y cumplimiento está a cargo de los tribunales de los diferentes Estados. Por ejemplo, California ha adoptado una sentencia que establece que los niños también tienen derecho al olvido.

Rafal Trzaskowski (Spokesman on Constitutional Affairs of the European People´s Party, European Parliament), se presenta como legislador y supone que todos están pendientes de la suerte del reglamento y entiende que el Sistema safe harbor no es suficiente para ellos. Hay ciertos datos que permiten evaluar los puertos seguros. Ellos, como la Unión Europea, están siempre en contacto con el FTC y este tema está siempre presente en todas las discusiones, no es posible decir que no se ha hecho nada. Hay temas nuevos, como cloud computing, big data, que requieren que nos adaptemos y no meter la cabeza bajo el ala.

Elaine Miller (European Commision), está de acuerdo con Rafal en que se pueden negociar temas de derechos fundamentales en convenios comerciales. No podemos negociar los derechos humanos de los ciudadanos, pero sí podemos negociar algunos aspectos. Todo radica en la confianza. Se ha polarizado el debate: el comercio es una cosa y la protección de datos es otra.

Un panel sumamente interesante fue el que versó sobre "**Privacy and Cybersecurity**". Su moderador Charles Raab (Professor of Government School of Social and Political Science. University of Edinburg, United Kindom), realiza una introducción haciendo mención a una serie de temas: protección de datos desde el diseño, desde la infraestructura, hurto de datos, suplantación de identidad, soliviantar cuestiones sobre determinadas razas y también surge la ciberseguridad frente al cibercrimen. La ciber resistencia a los ataques no está definida, puede ser por seguridad del Estado o por temas económicos. En el proyecto Iris están trabajando en el concepto de ciber resistencia. El ánimo es protegerse de los hackers, pero si para ello se menoscaban los derechos, entonces estamos enfrentados a un problema.

Ilias Chantzos (Senior Director, Symantec Government Affair EMEA, Global CIP and Privacy Advisor), afirma que no existe privacidad sin seguridad. Es importante proteger a la empresa. Las empresas deben colaborar con los órganos de

protección de la información. Las amenazas a la privacidad golpean en diferentes direcciones. Todo consiste en la identificación de la persona. Es necesario fijar las posibilidades de las infracciones. Es necesario entregar herramientas a las autoridades y tener en cuenta la privacy by desing.

Interesantísimo el panel **Criminal and administrative enforcement of data protection**, el que comenzó con la intervención del profesor Paul De Hert (Vrije Universiteit Brussel, Belgium), quien plantea que el derecho penal tiene un aspecto simbólico porque parece que es más eficaz que el derecho administrativo y que también tiene un mayor nivel de garantías. El derecho administrativo se aplica con mayor frecuencia. Hay quienes entienden que el derecho penal es una reacción anticuada, casi medieval, porque el estado priva a los ciudadanos de la libertad. Pero en derecho penal se puede determinar un delito en forma muy precisa. Se puede observar que el derecho administrativo se aplica cada vez en forma más brutal. Este límite que separa los dos derechos se va desvaneciendo y siguen apareciendo listas negras.

David Smith (Deputy Information Commissiones, United Kingdom) se pregunta: ¿qué instrumentos son más eficaces y en qué circunstancias? ¿Qué retos aparecerán? Explica el derecho consuetudinario británico. Para ser un regulador eficaz hay que tener la mirada puesta al futuro. En Gran Bretaña se envía una nota diciendo que se tiene que encriptar la información y se le envían los estándares. Se le advierte que si no cumplen sufrirán una pena. Tiene competencias retroactivas e imponen penas que van a influir en la actitud de otras empresas. Se puede imponer una pena cuando se trate de una vulneración seria. Se tiene que evaluar si los estándares han sido violados de manera seria y se tienen en cuenta los perjuicios de la persona que se han vulnerado los datos. Debe demostrar al responsable que no ha respetado la ley. Entre 500 y 600 mil libras esterlinas son las penas más altas. Es posible multar en forma retroactiva cuando la violación se ha realizado antes. Cuando se trata de un trabajador que vende los datos de mala fe, o cuando un trabajador usa mal los datos estaremos ante un caso penal. Pero en la mayor parte de los casos se trata de una empresa, y es importante aplicar sanciones penales porque las multas no son suficientes. Para imponer una multa es necesario llevar adelante el procedimiento adecuado. En casos como la publicidad digital (spam) se puede imponer una multa. ¿Pero cómo podemos asegurar que paguen? Las empresas pueden desaparecer y se abren otras. Esta es una debilidad del derecho anglosajón. Si se inicia un procedimiento penal contra una empresa, está en juego la reputación de la empresa y del director. Se aplican unas 25 multas al año y el equipo está integrado por 20 personas que se ocupan de llevar adelante el procedimiento administrativo. Un aspecto importante es recuperar los gastos si imponemos una multa, es necesario imponer costas judiciales porque la autoridad no se queda con el dinero de la multa y se entiende que esto es correcto porque no sería bien visto. Se responde ante la opinión pública y se tiene que demostrar que la actuación de la empresa causó perjuicios a las personas vulneradas.

Yoram Hacohen (Former Head of Israel Law, Information and Technology Autority) comenta que Israel heredó el sistema de los británicos el cual se ha ido modificando. Plantea el caso del robo de la base de datos con información personal de ciudadanos israelíes. Cinco años después, la autoridad de control ha creado un Departamento de investigación en protección de datos. Otro caso: una lista de tarjetas de crédito de ciudadanos israelíes apareció en la web, en este caso se trataba de un delito informático. Los casos los comenta para demostrar que es necesario aplicar el derecho penal en casos de protección de datos. En Israel las violaciones a la protección de datos pueden terminar con penas de privación de libertad, no solo con una sanción financiera. Pregunta ¿qué sucede si el administrador de la base de datos ha actuado bien pero es víctima de un delito informático? Las privaciones de privacidad son un tipo de delito específico. Debe estar siempre sometido a un peritaje, las pruebas no son evidentes, no son tangibles, no lo puede investigar un policía común. Además, hay que tener en cuenta las prioridades. Otro elemento es que, el papel más importante de una autoridad de protección de datos es el deber de vigilar la protección de datos personales. Cualquier infracción de datos personales debe ser investigada por el órgano de control. En el ciberespacio cada infracción tiene un carácter criminal. A veces son objeto para realizar otra actividad ilícita. Esto desanima a los posibles delincuentes porque nadie quiere tener que formar parte de un proceso en que se puede imponer una sanción penal. El profesionalismo es fundamental, la infracción de normatividad de datos personales da una mayor comprensión como autoridad y se muestra en que aspectos se debería intervenir con un tipo determinado de regulación. ¿Cuáles son las debilidades de aplicar el derecho penal? Relativo a medios, recursos y dedicación de los empleados. Lógicamente tenemos situaciones en que no se tiene información para formular una acusación. Como conclusión, entiende que hay más fortalezas que debilidades a la hora de aplicar el derecho penal.

El moderador del Plenario **Privacy and Technology** Prof. Wojciech Cellary hace hincapié en considerar la falta de conciencia del comprador de la discriminación de la cual puede ser objeto. Se pueden sacar ciertas conclusiones al hacer un análisis ilegal de los datos personales, cuando se obtiene información de Internet y se realizan perfiles de clientes, en esos casos se puede decidir a quién le hago un determinado ofrecimiento y a quién no. Puedo decidir que “X” cliente no me interesa porque es riesgoso y que a otro le puedo ofrecer un peor contrato porque como es su punto débil puedo vendérselo más caro y sé que igualmente lo va a adquirir. No hay herramientas técnicas frente a estos temas, la única defensa es la normativa.

David Hoffman, Director of Security Policy and Global Privacy Officer, Intel Corporation, dio el ejemplo del caso de Henrietta Lacks documentada en el libro “La vida inmortal de Henrietta Lacks”. Ella es la madre de todas las cédulas contra el cáncer de útero, entre otras cosas y su información médica se extrajo y utilizó para investigaciones sin su consentimiento. Hay datos que quedan para siempre. Dejamos cada día un montón de información en todos lados, por ejemplo de un chicle que se tira en la calle y queda pegado en un zapato se puede llegar a definir

la cara de una persona. A esto le sumamos el continuo uso de internet, lo que hace que se pierda el control de los datos. Se necesita un contorno de higiene en el tratamiento de los datos personales, ¿quién?, ¿cuándo?, ¿cómo?, ¿por qué?, están utilizando nuestros datos. El visto bueno de la persona es muy importante y tiene que ser sencillo para ella.

Billy Hawkes, Irish Data Protection Commissioner, expuso sobre la privacidad por diseño y la big data. Refirió a las ciudades inteligentes y la importancia de recolectar datos dentro de un determinado contexto, pero no todo tipo de datos. Mencionó aspectos relacionados con las redes sociales, cómo para las personas mayores puede ser una sorpresa la forma en que los niños comparten datos con todo el mundo. Entiende que las redes sociales no deberían aprovecharse de los datos. Concluye que es necesario darse cuenta que los gobiernos tienen el deber de obrar en bien de la sociedad y para ello hay que permitirle el acceso a determinados datos. Finalmente, afirma que la tecnología sirve como medio, pero solo eso.

Julie Brill, Commissioner, Federal Trade Commission, USA, hace referencia a la big data como uno de los desafíos a la privacidad. Afirma que las empresas que recopilan datos tienen que tener en cuenta la finalidad. No se trata solo de vender o no, el consumidor debe dar el consentimiento previo.

El Plenario final refirió a **Actores: Perspectivas, Roles, Intereses**. Jacob Kohnstamm dividió su exposición hablando acerca del sector privado y del sector público. Con relación al primero de ellos entiende que los datos personales en la economía de la información son la moneda de oro, son como una divisa, un medio de pago. Pone como ejemplo cuando Facebook apareció en la bolsa de valores y su valor dependía de la cantidad de personas de las cuales tenía información. La divisa es la privacidad. Hay empresas que no son transparentes en el tema privacidad y afectan a personas que no saben que se hace con su información. Hace referencia a que lo que se suele decir, es que la confianza es el elemento básico en nuestra sociedad. Pero no resulta tan convincente como podría aparecer a primera vista. La privacidad aparece como una cosa sexy, como un juego, pero deja de serlo cuando comenzamos a hablar de objetivos, de derechos y de obligaciones. Respecto al sector privado entiende que en mayor medida los gobiernos tratan a las personas como consumidores y clientes. Estos mismos gobiernos que tienen que prestar excelentes servicios, pero no solo eso, hay mucha información personal de la que disponen, por ejemplo la base de datos de información fiscal y da como ejemplo el caso de Holanda, en que esta base se filtró a Internet. Se están utilizando datos personales sin consentimiento. En el sector privado se están cuidando los datos, pero en el sector público es aún más importante, el gobierno quiere ser igual de efectivo. Entiende que estos principios tienen que fundarse a nivel supranacional. El proyecto de reglamento es un buen paso para conseguirlo y hay que tener presente que lo mejor no siempre es enemigo de lo bueno. La privacidad debería convertirse en un tema más popular en los gobiernos.

Malgorzata Steiner, Ministry of Administration and digitization, Poland cree que cuando se piensa en privacidad se lo hace en una moneda, una amenaza contra la libertad, una divisa para obtener servicios gratuitos, un obstáculo para los desafíos del futuro, un servicio que se está brindando. Porque lo que es tan evidente para unos, no lo es para otros. Es posible observar muchos puntos de vista, pero es difícil mantener una visión transversal. Hay que mirar a las partes interesadas: clientes, usuarios, ciudadanos. Cuando aparecen las tecnologías los primeros que profundizan en las herramientas son los técnicos. En cuanto al poder, a la fuerza para influir, no tenemos aquí una organización como puede ser Amnistía Internacional, hay grupos pero se manejan a nivel de las diferentes culturas.

De la **sesión de clausura** quiero destacar lo mencionado por Françoise Le Bail, Comisión Europea, quien destaca el gran abanico de ideas que se han tratado en la conferencia. Refiere a Giodo (Autoridad de Protección de Datos Polaca) y al cumplimiento de sus 15 años, implementando las normas europeas con fuerza y compromiso. Hace mención a que estamos viviendo una revolución tecnológica, pero no podemos olvidar la calidad de los datos, el intercambio entre las personas. Otro aspecto que se ha destacado es la confianza, porque en un mundo que vive tiempos vertiginosos (tema de la conferencia) ésta es fundamental. Si hay confianza hay más datos en línea. Con respecto a la reforma, el reglamento ha suscitado gran interés, interés que la ha sorprendido. Entiende que lo principal es abogar por los principios cívicos, dentro de las enmiendas se trata de consolidar el derecho de los ciudadanos. El texto parece complicado a primera vista y quiere que se simplifique, para que exista un solo sistema y no 28 diferentes. Hay que mantener el equilibrio entre los derechos de los ciudadanos y el impulso de la economía digital. En Europa se quiere que el reglamento tenga una garra más fuerte y que exista una única interpretación para toda Europa y que los organismos sean más fuertes.

Finalmente, he de remitirlos al sitio web de la conferencia https://privacyconference2013.org/Resolutions_and_Declarations en el cual podrán acceder a las resoluciones adoptadas.