Relatoría de la 36° Conferencia Internacional de Autoridades

de Protección de Datos y Privacidad – Balaclava (Mauricio)

Prof. Dra. Esc. María José Viega

La 36° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad se llevó a cabo en Balaclava (República de Mauricio). La sesión cerrada de la conferencia internacional tuvo lugar los días 13 y 14 de octubre de 2014 y comenzó con la bienvenida de la Autoridad de Mauricio Sra. Drudeisha Madhub, quien hizo hincapié en la problemática de la Internet de las cosas, tema central de la sesión cerrada.

En segundo lugar hizo uso de la palabra el Presidente de la Conferencia –Jacob Kohnstamm- realizando un informe sobre la sesión cerrada de la 35° Conferencia Internacional llevada a cabo en Polonia en el año 2013.

Scott Peppet, Profesor de derecho de la Facultad de Derecho de Colorado (USA), **Rolf Weber**, Profesor de Derecho en la Universidad de Zurich (Suiza) y **Kate Carruthers**, Business and IT strategist, Co-founder of Social Innovation Sydney (Australia) realizaron una serie de presentaciones sobre la Internet de la cosas, a los efectos de analizar la temática desde la óptica de la protección de datos.

En dicha reunión se tomaron una serie de resoluciones que se encuentran disponibles en www.viegasociados.com y se anunció la realización de la 37° Conferencia Internacional para la última semana de octubre del 2015 en Ámsterdam (Holanda).

La **Conferencia Abierta** (15 y 16 de octubre) inició con la bienvenida de la Sra. Drudeisha Madhub, quien planteó que su sueño es la existencia de un nuevo orden mundial de protección de datos personales.

Cree que debería existir un solo derecho para la privacidad en todo el mundo, que el espíritu humano nació libre y debe permanecer libre. La tecnología con todas sus buenas intenciones no puede restringir este derecho. En Mauricio desean que la protección de datos sea un derecho fundamental en todo el mundo, no protegerlo como un derecho en extinción. Entienden que es fundamental la concreción de una serie de principios para todos los seres humanos en protección de datos y ese es su objetivo.

El **Primer plenario** se denominó **Sistemas interconectados de privacidad: perspectivas desde el otro lado del océano.** Comienza exponiendo **Isabelle Falque-Pierrotin, Presidente de la CNIL**, manifestando que si se quiere que la privacidad sea una prioridad es necesario motivar a los altos mandos, porque la

privacidad no puede verse como un tema únicamente legal, se tienen instrumentos legales, también existen otros instrumentos que son flexibles y hay una conexión entre ellos. En Europa tienen un espacio para intercambiar opiniones en temas de Internet de las cosas, que han sido dichos ayer en la resolución que se adoptó, en primer lugar tiene que estar en control del usuario, el problema es que muchas veces éste no sabe cómo funciona; el aspecto de la seguridad es un aspecto, pero ¿cómo podemos estar seguros? Y en tercer lugar ¿qué tipos de datos se intercambian? Es muy importante tener la seguridad de re identificar la persona. El sistema de internet de las cosas es muy complicado, ¿cómo motivamos a los ingenieros para que incorporen la privacidad a su trabajo?

Edith Ramírez, **Presidente de la Comisión Federal de Comercio de Estados Unidos**, entiende que Internet es algo que va a volverse cada vez más importante y hay muchas acciones que son peligrosas. Es fundamental también el aumento en el volumen de información, que aumenta el ecosistema. Estos ecosistemas están codificando información y es importante saber qué sistemas están utilizando, son perfiles muy detallados que tienen que ser identificados y saber si cumplen con la ley. ¿Cómo nos están calificando como consumidos? ¿Cómo estos datos van a ser utilizados en las aplicaciones? ¿Cómo puede utilizarse big data y cuáles son las consecuencias negativas? ¿Estamos realmente eliminando los problemas potenciales o estamos analizando los vacíos que existen entre las normativas existentes?

Allan Chiang, **Comisionado de Hong Kong,** cree que Internet de las cosas debe trabajarse en el consentimiento. Las organizaciones tienen que considerar al cliente, escuchar sus expectativas y aplicarlas. Estamos en un mundo competitivo, de esa forma tendremos un mejor comportamiento de las empresas en el mercado y para ello es importante presionarlas. Hay que hacerse las preguntas que se haría el cliente. Cuando el cliente se siente ofendido, aburrido, ¿sabe por qué? ¿Qué hay detrás de los números, de los servicios? Si los tienen en cuenta los clientes los van a valorar.

En el **Segundo Plenario** denominado **La privacidad no tiene límites territoriales,** participó **Jacob Kohnstamm, Presidente de la Conferencia,** quien comenzó haciendo referencia al tema tratado en la sesión cerrada, la internet de las cosas. Hace referencia a que hablará de algo muy vinculado con este tema, que es la big data. Hoy hay mucha gente hablando de big data y sus oportunidades. Sin duda ofrece muchas ventajas, predicción de epidemias, incremento de la eficiencia de la energía. Pero se pregunta: ¿estamos listos para big data y para enfrentar sus desafíos? Se trata de recoger la mayor cantidad de información, combinar la información y utilizar algoritmos para descubrir nueva información. El Grupo de Berlín y el Grupo del Artículo 29 adoptaron una

resolución, pero ello no es suficiente. El propósito de la protección de los datos personales es minimizar la sorpresa. Big data está tratando de hacer la maximización de la sorpresa, porque trata de utilizar la información para descubrir cosas que no sabíamos. Ellos pueden estar evitando usar los principios y puede llevar a procesos de identificación. La creación de perfiles es un gran riesgo, es la predestinación digital, nos lleva a una sociedad que está siendo catalogada y se puede tratar a una persona con desconfianza porque cae en el perfil, por ejemplo, de evasor de impuestos. Hay un caso de una chica embarazada, que le enviaron propaganda para bebés a su casa y su padre no estaba al tanto del embarazo.

Mucha información está siendo recogida sin el consentimiento del individuo, la gente proporciona datos personales solo para participar en la sociedad. Todos sabemos muy bien que tanto el sector privado como el público necesitan credibilidad. La credibilidad ha sido resquebrajada en los últimos años. La transparencia es la solución. Es importante la efectiva supervisión del cumplimiento de la ley. Tenemos que ajustarnos muy bien a los principios de privacidad. Los principios pueden funcionar como barreras a la big data. El debate tiene que estar dado sobre el futuro de big data, pero también sobre los riesgos, sobre el mal uso de los datos. Si no trabajamos sobre la big data nuestras sociedades democráticas van a sucumbir al dinero, al poder y a la indolencia.

Peter Shaar pregunta si ¿debemos buscar buenas prácticas o aplicar leyes estrictas por ejemplo en el área de la salud? Julie Brill responde que necesitamos más información, que las mejores prácticas pueden mejorar, pero si hacemos la relación con mercadeo tenemos leyes que aplican en USA, pero debemos ser más claros con usuarios que van a pasar la línea. Ella cree que en USA ha habido mucha discusión sobre este tema, cuando compara con unos años atrás.

Jacob Kohnstamm está muy a favor de la legislación europea, está convencido que si no hay un debate público no se va a poder llegar tan lejos como se necesita, porque no se tiene la masa crítica, porque la gente no sabe lo que está pasando, dan los datos casi que sin saberlo, es gratuito, es interesante, es divertido y parece tan democrático.

El Tercer plenario: Privacidad y protección de datos en un mundo en desarrollo tuvo como expositora a la Sra. **Drudeisha Madhub**, Comisionada de protección de datos de Mauricio. Madhub se plantea una serie de preguntas: ¿la privacidad es solamente una lotería de occidente y un gran obstáculo para progresar? ¿Los países en desarrollo han puesto énfasis en estos temas? ¿La adopción de la Convención de la Unión Africana va a cambiar la percepción de la Unión?

Se menciona la Norma ISO sobre los estándares para la nube. Se está viviendo un momento importante para la privacidad con estas nuevas tecnologías, se está tratando de asegurar que los derechos estén siendo protegidos. La privacidad es donde las tecnologías tienen el papel más innovador. Sin embargo estas nuevas tecnologías llegan a nuestros países sin la información necesaria. Como consecuencia, los países en desarrollo violan cada vez más el derecho a la privacidad. Por lo tanto, los ciudadanos necesitan mayor protección. La privacidad es un derecho fundamental, pero los confines de este derecho son como un juego de nunca acabar y no es un juego limpio, porque los individuos no están informados para protegerse. En los países en desarrollo la ausencia de un marco legal es muchas veces un serio problema. Los gobiernos están espiando a los ciudadanos, las corporaciones están comprando y vendiendo sus datos. Los gobiernos en los países en desarrollo deben revisar su legislación y fortalecerla, haciendo énfasis en la protección de datos. La gente que trabaja en sistemas tiene que estar preparada para la protección de datos. Tenemos la tendencia de mirar a la era digital como tecnológica, pero ésta era está cerrando y hay que saber manejarla. En el 2012 las cifras de Google, Facebook y Twitter son impresionantes, pero los costos de la banda móvil sigue siendo caro para los países pobres.

Marguerite Quédraogo, Presidenta de CIL de Burkina Faso manifiesta que las leyes sobre los datos constituyen un desafío para la vida privada. Es importante saber si la protección de los datos es una necesidad imperiosa o es una opción para los países africanos. Lo más importante es que cada país adopte una ley informática, es el instrumento principal que permite al ciudadano instalarse en un estado de derecho. Los ciudadanos pueden así reclamar por cualquier violación. Lo principal es la protección de los datos teniendo en cuenta el desarrollo tecnológico. Es necesaria también, la existencia de una autoridad autónoma que controle el cumplimiento de la ley.

La Comisión de Burkina Faso es una pionera en África, al sur del Sahara. Concluye que la protección de los datos personales es importante no solamente desde el punto de vista legal, económico, sino también en la educación y en la tecnología, para hacer de internet un sitio seguro.

Patrick Walshe, Director Privacidad, Gobierno & Asuntos Regulatorios, Asociación GSM, comienza diciendo que la GSM es una firma global que se encuentra en 290 países y pregunta: ¿Cuántos de ustedes tienen smartphone? ¿Cuántos pueden manejar su privacidad en su smartphone? También pregunta cuantos de los presentes viajan y usan aplicaciones para comunicarse en los viajes. Estos servicios no están regulados, porque no son comunicaciones. Entonces observa un mundo de mentiras. A los operadores no les es permitido

utilizar los datos, no pueden compartir información. Ha escuchado discusiones sobre la transparencia de los datos, pero a veces se requiere que los datos viajen a través de las fronteras. Se está tratando de competir en un mercado, es posible que no todos puedan aplicar las mismas reglas. ¿Cuántos reguladores de telecomunicaciones tenemos en la sala? No hay. Algo que se tiene que hacer es analizar cómo juntar diferentes reguladores para discutir estos asuntos. Esto necesita nuevos pensamientos, nuevos enfoques.

Hay desafíos, pero no solo respecto a la ley. No se puede decidir sobre los clientes, porque no pueden decidir sobre la credibilidad. Hicieron investigaciones en 11.800 personas y observaron que el 83 % usan aplicaciones sin saber sobre las leyes y sobre el consentimiento. El 60 % quieren reglas consistentes para que sean aplicadas. 8 de cada 10 usuarios no lee las notas legales porque son muy largas o muy técnicas. La gente usa su móvil cuando está caminando, están muy metidos en sus aparatos.

Está aumentando la concientización sobre el uso del móvil y éste es muy importante para las comunicaciones en África. Hay industrias trabajando en forma irresponsable y dicen que big data puede salvar sus vidas. Hoy estábamos viendo cual es el proceso técnico por el cual big data toma sus datos. Uno de los desafíos para muchos países es la falta de instituciones que puedan pelear por esto.

El Panel 1 refirió a la **Ventanilla única: centralización y proximidad.** El primer expositor fue **José Luis Rodríguez**, **Director de la Agencia Española de Protección de Datos**. Nos dijo que la expresión “One Stop Shop” presenta que el controlador tiene varios caminos, pero el establecimiento principal tiene que ser la sola autoridad competente, esta regla nos lleva a la competencia de la autoridad. La autoridad supervisora también tiene la competencia para supervisar los cambios. La regulación prevé mecanismos para mejorar el proceso de decisiones, que mejora el impacto de la autoridad. Otra ventaja de este nuevo criterio es que ahora las cortes nacionales también pueden apoyarse en las autoridades. Este sistema tiene ventajas importantes, y es que tiene varios aspectos que pueden estar vinculados. Una decisión que es válida para toda la Unión Europea. Varias decisiones de las Autoridades de Protección de Datos pueden ser diferentes e incluso contradictorias. Con este sistema eso no sucederá. Una ventaja es que ellos trabajan en favor de la compañía, pero es diferente cuando se consideran las cosas desde el punto de vista de las personas.

Eduardo Urtarán, Socio Hogan Lovells. Lo ideal sería tener una sola ley que gobierne los 28 países, una ley, un regulador, un controlador a través de todo el territorio de la Unión Europea. La idea era armonizar todo, había una razón

práctica para ello. La Unión Europea tiene como objetivo alcanzar algunos aspectos prácticos, como por ejemplo, tener un nivel de comprensión de la ley que no existe hoy, tener una organización que trabaja a través de toda la Unión Europea, entonces todos tienen que trabajar y rendirle cuentas a un solo organismo. El resultado más obvio debería ser un nivel más amplio de cumplimiento de la ley. Las organizaciones están teniendo problemas para tratar todos estos detalles. ¿Cuál es entonces el problema? Esto es visto como un mecanismo de ponerse bajo un regulador que no es potente. Las autoridades son fuertes, pero están distantes. Hay que olvidar si somos suaves o no. Se necesita un trabajo de equipo, los reguladores tienen que trabajar juntos.

Dale Skivington, **CPD Dell Computers**. En Dell están muy conscientes del concepto privacidad por diseño. Ellos primero colaboraron compartiendo las mejores prácticas, y después se volvió una metodología más eficiente para comprobar el sistema de cumplimiento. Cooperan en el cumplimiento en el diseño, es importante tener un marco legal consistente, con estándares, por eso tienen reuniones mensuales con los líderes, en donde aparecen los asuntos que están llamando más la atención y presentan los resultados. Algo que también hacen es estudiar cada programa de cumplimiento. Cada programa está siendo monitoreado regularmente. Esto no es difícil, lo que es difícil es implementar los controles que apoyan las políticas y los estándares y es lo que está generando problemas.

El Panel 3, titulado **Vigilancia frente a la vigilancia de datos**, comenzó con la exposición de **Jan Albrecht,** del **Parlamento Europeo**, quien compartió tres ideas: la primera es que “ustedes piensan que la tecnología va a permitirnos vigilar gastando menos dinero. La segunda es que estas razones están en el marco de una ley. En tercer lugar, que los teléfonos, los email, los mensajes son mucho más extensos de lo que se había pensado”. Entiende que estos mecanismos parecen expresar otras ideas y que estamos siendo desafiados por estas ideas, lo que parece desplazar la misión de las autoridades. Se pregunta: ¿Qué es lo que se ha hecho para este problema? ¿Cómo ha cambiado el mundo lo que pensábamos que estábamos viviendo?

El Panel 6 abordó el tema del riesgo en el marco de la privacidad. Bojana Bellamy, Presidente de Centro de liderazgo para las políticas de información de Hunton & Wlliams. La evaluación del riesgo es importante para que se pueda hacer un balance de la actividad y el riesgo. La eficacia se vuelve una palabra clave, qué es lo que las organizaciones quieren saber, qué es lo que proponen. Hay que darle un lugar especial a la previsibilidad. La evaluación del riesgo y como se calibra es importante, también como se está rindiendo cuenta a los individuos de la sociedad.

Isabelle Falque-Pierrotin, Presidente de la CNIL & Grupo de Trabajo del Artículo 29. La privacidad es un elemento clave de la gestión de riesgo en la empresa. El riesgo es una cuestión de inversión. Hay que ser prudentes con el enfoque de riesgo, conocer las consecuencias jurídicas. Si hoy se tiene en el reglamento un nuevo concepto que es el de rendición de cuentas, se debe ser más práctico y darle un marco a los principios generales, que de lo contrario serían muy teóricos. Se tiene que rendir cuentas y usarlo solo para los tratamientos riesgosos o solo los tratamientos de alto riesgo, pero ¿quién define esto? La empresa, que deberá hacer un análisis de riesgo que es muy sofisticado, normalmente se contrata a una empresa externa y puede resultar muy caro.

Hay otro enfoque que está basado en el perjuicio, que puede generar responsabilidad, pero no proporciona derechos. Los derechos del individuo no se trata solo de los perjuicios al individuo, los derechos son objetivos, los perjuicios debe evaluarlos el controlador.

Willem De Beuckelaere, Presidente de la Comisión de privacidad de Bélgica, dice que el equilibro y el control de riesgo constituye el elemento fundamental del derecho a la privacidad. En los orígenes, en 1890, se decía que las nuevas invenciones no debían menoscabar los derechos del individuo, esto que se escribió en 1890 podría haberse escrito ayer como introducción a este panel. Planteó que hay diferentes tipos de riesgos, pero se centró en el hecho de que el controlador no actúa solo.

Jane Horvarth, Director Senior de la Privacidad Global de Apple. Apple muestra en sus políticas que está comprometido con la protección y con la codificación de los datos. El riesgo puede ser una publicidad muy mala y el cliente puede perder confianza. ¿Qué es lo que hacemos para minimizar el riesgo? Lo llevamos a todos los estados del producto, constantemente estamos con el desafío de incorporar políticas de confidencialidad.

Erik Neuenschwander, Jefe de ingeniería de privacidad de Apple, expresa que ellos trabajan la privacidad y la confidencialidad en el mismo equipo. Lo que hacen es mejorar cada vez más la accesibilidad en sus productos, pero también la privacidad. Tienen otra red de ingenieros con la cual han tenido la posibilidad de influenciar en otras áreas. Los detalles de las transacciones nunca son expuestos, porque esto puede ser visto por los hackers. Todos saben que tener claves en nuestros teléfonos es un tema importante, pero no todos las usan, algunos de nuestros aparatos se prenden con la huella digital. El riesgo es que sea copiada, se transforma en un modelo matemático que no contiene datos, por lo cual no es posible reconstruirla.

Joann Stonier, Vice Presidente Ejecutiva, Oficina de privacidad de Master Card. Dice que las informaciones que vienen de los consumidores, las comunicaciones entre los bancos y los vendedores, entre los bancos y los compradores. Tenemos una gran cantidad de datos y lo que hacemos es combinarnos, utilizamos la privacidad por diseño. Mientras los datos son procesados en nuestro ambiente de negocios cuidamos la información. Tenemos en cuenta cada paso y como se trabaja con los reguladores. Otro tema vinculado al riesgo es el fraude, que es un tema que ha ido evolucionando. Antes era un ecosistema, ahora tenemos una ayuda suplementaria con Apple pay. Siempre habrá gente que hace fraudes, pero también nosotros estaremos tratando de ver cómo trabajan. Esto lo hicimos una vez que adoptamos el enfoque del riesgo. Todo esto es con una visión general, no estamos haciendo perfiles de las personas.

David Smith, **Diputado Comisionado y Director de protección de datos (UK)**. "Integrar este enfoque en nuestro trabajo requiere transparencia, pero como reguladores debemos constatar la transparencia. Estamos muy conscientes de la protección del individuo y de los riesgos del individuo. Somos conscientes que debemos proteger la privacidad y tiene sentido una supervisión basada en el riesgo", dice Smith. Y se pregunta: ¿Dónde se hace la diferencia más grande? ¿Qué es lo que miramos? Si se va a invertir dinero es porque se va a eliminar un riesgo, sea tangible o intangible. El riesgo de perder el número de tarjeta de crédito, de perder el trabajo porque se ha descubierto un pasado criminal, son aspectos que generan ansiedad. Como recomendación, cree que hay un daño que se hace a la sociedad y que debería abordarse. Se miran los riesgos, pero también hay que mirar que tan serios son los daños que pueden ser causados.

Todos sabemos que big data genera zonas de riesgo, nos volvemos como una policía, tenemos un sistema de datos inteligente, nos interesa saber cómo la gente puede ayudar en nuestros procesos. Tenemos muchas auditorías y reflexionamos mucho.

En el **Panel 7** sobre **E-salud y Protección de datos** participó como moderador **Adam Tanner**, **Institute for Quantitative Social Science, de la Universidad de Harvard**, quien comienza realizando el siguiente planteo: a las industrias farmacéuticas les interesa saber quiénes están comprando y consumiendo determinados medicamentos. La farmacia vende su información. También hay compañías que se están vinculando con las aseguradas. Por ejemplo, en Estados Unidos, Medicare tiene un contrato con la empresa IMS que recolecta información. El problema potencial de todo esto se está volviendo más significativo. El moderador le pidió información a varias empresas en Estados Unidos, pero las empresas no quieren dar detalles sobre sus actividades. Las compañías que

compran estos datos están obligadas por contratos a re identificar a las personas, pero verificar que esto efectivamente se realice es otro punto.

David Watts, Comisionado de protección de Datos de Victoria, Australia. Comenta que miró las políticas de privacidad de IMS. Se sabe que las leyes nacionales son diferentes, pero el compromiso para Australia es el mismo que en Estados Unidos. Pide que se imagine que el derecho a la privacidad es un derecho internacional, que está interconectado, porque como otros derechos este no ha recibido importancia durante generaciones. Se pregunta: ¿Cómo establecer un dialogo entre todas las partes involucradas? Piensa que uno de los puntos clave es el desafío tecnológico de internet de las cosas. Con respecto a la salud hay varias cosas, por un lado se relaciona con tres derechos, la obligación de respetar, el derecho a promover el derecho la salud y el derecho a la confidencialidad y son interdependientes. Si tengo determinados datos básicos de una persona, puedo identificar a alguien que por ejemplo tiene cáncer de seno. Nada está libre de riesgos y el análisis del riesgo tiene que ser considerado como fundamental.

Dr. Mukesh Haikerwal, Jefe del Consejo de la Organización Mundial de la Salud recuerda que ayer se hablaba de datos y derechos humanos y sobre trabajar con equidad. Esto también está impactando en la salud. Hay que tener en cuenta que personas saludables hacen a una economía saludable. “Nosotros como doctores tenemos que tener en cuenta la privacidad cada día. Nuestro marco va más allá del marco legal”, dice Haikerwal. Hay que trabajar juntos para cambiar el enfoque desde un simple requerimiento a un derecho pleno. E-salud es un programa complicado, el proyecto analiza muchísimos aspectos y se necesita que la salud sea segura.

Gérard Lommel, Presidente de la “Comisión Nacional para la Protección de los Datos” de Luxemburgo. Plantea que tienen sistemas para tratar electrónicamente la salud y existe la necesidad de que se dé un balance entre el sistema de seguridad social y los profesionales de la salud. En la salud electrónica, el doctor es seleccionado por el paciente y puede hacerlo en el sistema universal de salud. La Comisión Europa está promoviendo cuestiones relacionadas con la salud de la población y se están creando hospitales en línea, como forma de mejorar la salud del paciente.

Se necesitan análisis detallados sobre los riesgos. Se tiene una mirada muy cercana a las herramientas que se les ofrecen para poner bajo su control sus propios datos.

Tenemos un punto sobre la necesidad de sensibilizar al público para que el sistema explique mejor las necesidades del paciente y a su vez el paciente podrá verificar en línea quien vio sus datos. Se han hecho campañas de comunicación, para facilitar la comprensión del tema.

El último punto es la gobernanza de este sistema, cómo va a ser evaluado. Para que habiendo una evaluación critica constante se pueda mejorar permanentemente y mejorar el derecho a la autodeterminación de los pacientes. No quieren que el sistema se convierta en una posibilidad de fuga de datos personales.

El Moderador pregunta si ¿tienen los pacientes derecho a dar su consentimiento para que sus datos sean tratados? El expositor dice que sí. Luxemburgo cree que Europa no está lista, están trabajando para que no se puedan identificar datos, datos que se están utilizando para la información médica, esto va a estar abierto al consentimiento.

El **Plenario V** refirió a **Ética, derechos fundamentales y big data,** comenzó con **Scott Taylor, HP VP and co-chair de la Fundación Proyecto: mejores prácticas de Big Data,** quien parte de la afirmación que está de acuerdo con el concepto de big data que se ha venido manejando. El tema es que debe ser medido, tiene que haber un modelo, tiene que poder ser refinado y corregido, tiene que considerar cuales son las implicaciones, los aspectos vinculados a la discriminación, y también los aspectos legales. Si comenzamos a hablar de la evaluación del riesgo en secuencia, hay preguntas para hacerle respecto al proceso de evaluación con respecto a la ética.

Si trabajamos con el concepto de química, hay una relación entre éste y big data, cambio químico (dos sustancias se mezclan y forman algo nuevo) y reacción química (que algo sea peligroso o beneficioso), esto es lo que hay que aplicarle a big data.

Liumyla Romanoff, Legal Specialist, United Nations Global Pulse. Dice que se encuentran estudiando cómo establecer prácticas para explorar que los datos se estén utilizando para el bien de las personas. El uso ético de big data debe hacerse en privado. Big data puede ser utilizado para el bien, usamos datos de twitter sobre un país que trabajaba con la fundación, información de celulares para ver cómo se mueve una población luego de una inundación. Antes de cada proyecto hay que medir cuáles serán los daños que podrían suceder. Big data es utilizado para el bien público, debe ser proporcional respecto al objetivo y que los riesgos sean muy bien identificados. Hay que tener en cuenta que cuando se usa big data hay que mirar en profundidad. También es importante determinar cuáles

son los límites. Consideramos que se necesita una toma de conciencia porque puede asegurarse el bien público, pero la gente debería estar informada. Es un desafío y hay una gran necesidad de que sea aprobado un código ético.

Brendon Lynch. Chief Privacy Officer, Microsoft. La gente no usa tecnologías en las cuales no tiene confianza. Cuando big data maneja datos tiene que progresar, hace 500.000 años en el período cámbrico hubo condiciones claves: más calcio, más agua salina, etc. y un clima que generó la vida. Hay paralelos respecto a la tecnología. Una explosión cámbrica requiere un uso de las nubes, tener fondos, alcanzar millones de personas en un momento. Gran parte de nuestro mundo físico ha sido digitalizado.

Para concluir, el **Plenario VI** fue un **Panel de relatores,** en el cual cada uno de ellos puso foco en alguno de los puntos tratados. Por ejemplo, **Marie Georges. Especialista independiente y miembro del Grupo de Expertos europeos de derechos fundamentales,** se refirió a que los americanos nos hablaron de rendición de cuentas, y ¿eso qué significa? Se habló del principio de finalidad y proporcionalidad ¿y los demás principio? **Peggy Eisenahuer, Privacy & Information Management Services** hizo hincapié en la interoperabilidad y la protección de datos, la inutilización del sistema legal respecto a la red global, es una definición más grande, no solo sobre la aplicación de la ley, sino sobre otros aspectos, ley + políticas + mejores prácticas. El comisario de Burkina Faso habló del diseño por la confianza, como un concepto clave para la interoperabilidad. **Malcolm Crompton, Managing Director, Information Integrity Solutions PTY Ltd**. El tema principal de la conferencia fue un Nuevo orden mundial de la protección de datos. El verbo “volver” es el tema de la cooperación entre los reguladores. Creo que lo que más importa es que el trabajo de los reguladores aproveche a los ciudadanos. Como reguladores hay que hacer el trabajo de una manera en que promueva el progreso. La conferencia tiene una larga historia. Primero cada vez más los datos viajan a través de las fronteras, esto es un tema de jurisdicción. Otros grandes desafíos: hay que vigilar la nube de big data e internet de las cosas, hay que analizar la diferencia y la combinación de derechos para que se pueda apoyar la adecuación y mejorar la cooperación.

Durante el **Cierre** la principal pregunta que se realizó fue si ¿la privacidad se va a extinguir como se extinguió el Dodo (ave típica de Mauricio) por la voracidad de la big data?