¿10 AÑOS DE LA LEY DE PROTECCIÓN DE DATOS: ¿QUÉ TANTO HEMOS AVANZADO? ¿QUÉ NOS HACE FALTA? LA LEY AL TABLERO

Departamento de Derecho de las Telecomunicaciones

Universidad Externado de Colombia

19 y 20 de octubre de 2022

Bogotá D.C., Colombia

Compilado por:

Diana Marcela Quiñones Zambrano

Universidad Externado de Colombia

Calle 12 No. 1-17 Este
Bogotá, D.C., Colombia

Teléfono: 282 60 66 Ext. 1105, 1106 esdercom@uexternado.edu.co

PRIMER DÍA

Apertura del evento e instalación del evento.

Intervención de la Decana, Dra. Emilssen González de Cancino

La Doctora Emilssen González de Cancino, en nombre de la Universidad Externado de Colombia dio la bienvenida a los conferencistas y participantes, comentando que para nadie en el mundo moderno es extraño reconocer la importancia de los datos personales y por lo tanto el peso que tienen que tener las medidas de protección especialmente establecidas en una ley con alcance efectivo debe ser una ley eficiente y por eso es maravilloso tener la oportunidad de ver a los 10 años cuál es el balance que tiene la ley colombiana.

Así mismo, expresó que en el sector donde se mueve con alguna familiaridad: "los datos son tan importantes tanto para el individuo como para los grupos familiares o los grupos étnicos en los cuales los individuos pertenecen que ya se ha hablado de un cuerpo electrónico y decir de que los datos hacen parte del propio cuerpo y por lo tanto la protección de los datos deben tener la misma altura y representar lo mismo que representa la protección basada en los Derechos Humanos, los datos genéticos suscitaron incluso una declaración Internacional de la UNESCO, que es relativo a la protección de los datos y de aquellos donde están los genéticos como son las biológicas".

Finalmente, manifestó que desde la decanatura se siente satisfecha y congratula el equipo organizador, y agradece a los conferencistas y a los asistentes.

Intervención de la Doctora Sandra Milena Ortiz, directora del Departamento de Derecho de las Telecomunicaciones de la Universidad Externado de Colombia.

La Doctora Sandra Ortiz dio un cordial saludo y bienvenida a los presentes, así manifestó que en su calidad de directora es gratificante instalar este evento dedicado a analizar los 10 años de la expedición de la ley 1581 de 2012, por medio de la cual se dictan disposiciones generales en materia de protección de datos personales.

Así informó que la iniciativa este evento responde a la necesidad de evaluar los aspectos en que se ha avanzado la protección de datos en Colombia, donde de igual forma, este año también se conmemora los 30 años de la expedición de la primera sentencia en

materia privacidad, derecho a la información, contenidos previstos en la sentencia T414/1992, magistrado ponente el Doctor Ciro Angarita, y por primera vez conceptos que van a determinar y van a servir como antecedentes para la ley de protección de datos y material del sector financiero y que posteriormente va a aspirar la expedición de la ley 1581.

Finalmente, dio un agradecimiento a los integrantes del departamento y a los Docentes Andrés Fernández de Castro, Heidi Balanta y José Alejandro Bermúdez por sus aportes a la construcción de la agenda de los dos días académicos y a los panelistas por haber aceptado la invitación, así dio una bienvenida al externado y manifestó sus augurios para que la discusión sea lo más constructiva y que permita generar una actualización de la política de materia protección de datos para Colombia.

CONFERENCIA: ESTADO DE DERECHO Y LOS DATOS

Conferencistas:

1. **Felipe Sandoval Villamil - Regional Head Legal de DiDi**

El Doctor Felipe Sandoval Villamil, dio un saludo y agradecimiento a los presentes, e inició comentando sobre los datos históricos, ya que los conceptos tienden a cambiar, pero cuando uno se guía por los conceptos empieza a tener posiciones futuristas.

De esta manera le dio la palabra a Lorenzo Villegas, el cual comentó que se piensa que siempre que hay un colombiano relacionado con el tratamiento de datos aplica la ley colombiana, lo cual no es cierto porque la ley no está asociada a la nacionalidad o residencia incluso del colombiano, sino al lugar del tratamiento.

Seguido a esto, habló Nataly Perilla, estudiante de la maestría de derecho informático y de las nuevas tecnologías, que comentó que uno de los aspectos más más relevantes es el tema de los incidentes de seguridad como hace poco en España tres tiendas cerraron por temas de ciberataques de datos y como esas filtraciones se pueden proteger desde no solo empresas grandes, que tienen toda la infraestructura física y tecnológica para realizarlos, sino también desde pequeñas empresas.

Con base a esto, el Doctor Sandoval recordó como una anécdota interesante de Benjamin Franklin que cuando dirigió los correos nacionales en Estados Unidos, donde se inventó un juramento para todos los funcionarios del correo, en donde se comprometían a no abrir el correo. Así mismo, contó otra anécdota de Rudy Giuliani, el cual se dedicó a trabajar temas de ciberseguridad, y comentaba que siempre van a existir los hacks, el tema es que tan rápido se van a detectar. Es un tema que cada día se vuelve más complejo por la masificación de datos.

Así comentó, la película de Filadelfia de 1993, y toca la privacidad de datos respecto a las enfermedades, y trata de un abogado que lo despiden porque se entera que tiene sida, y los abogados de la firme alegan que ellos tienen derecho a acceder a esa información.

De igual manera trae un concepto de Privado, referido a que la esfera privada era de la casa y la familia, donde se creía que era el espacio donde se podía desarrollar nuestros deseos y necesidades. La sociedad era muy pública, familias enteras en una habitación, era difícil de llegar a la privacidad.

El primer precedente oficial, fue el caso Semayne en Inglaterra, la decisión es muy bonita porque dice que la casa es el castillo y su fortaleza, cuando se reconoce el valor de la morada, y de tener la privacidad en ese lugar, se empieza a diferenciar de los accesos públicos a los sitios, y que el acceso a una casa se debe hacer con un permiso.

Todo este tipo de desarrollos llevaron a que, en 1890, Warren y Brandeis con el derecho a la privacidad en los Estados Unidos, dieron a entender lo que estaba pasando masivamente con los periódicos, y recuerda al caso Kodak, con su cámara portátil, donde iba a traer problemas, respecto a la privacidad de las personas.

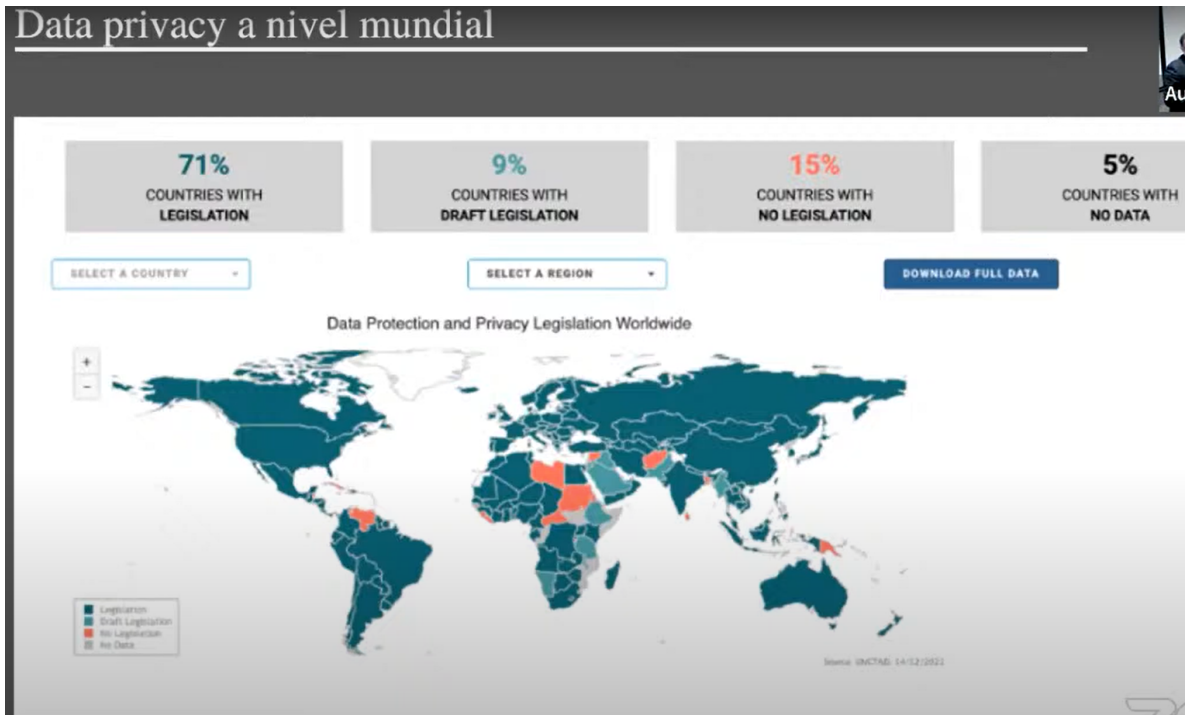
Respecto al desarrollo en las guerras, donde se dice la segunda guerra se ganó por el servicio de inteligencia ingles que logró decodificar los mecanismos claves que los Nazis utilizaban para comunicarse entre ellos. Para que en la posguerra se hable de la Declaración Universal de los Derechos Humanos, y se establezca en su artículo 12 el derecho a la privacidad. Con el Freedom of Information Act de los Estados Unidos se obtuvo el derecho para solicitarle a las entidades acceso a nuestros documentos y entender que pasa con esa información que estaban recolectando.

Desde los años 80, se dio por ejemplo la OECD, que por primera vez se formulan los lineamientos de transferencia transfronterizas de datos, y a nivel del Consejo de Europa, que adoptan normas de privacidad de datos, pero para el uso de los computadores, el internet lo desarrollaron en EEUU para fines militares, y lo que más preocupaba es el uso de los datos privados. Finalmente, en Alemania, con la Corte Constitucional Federal, donde estaban haciendo un censo muy grande, frente a la cual las personas pudieron iniciar estos procesos y anular el censo, y mutar las preguntas.

Ya en los años 90 a la fecha, se termina de masificar el internet, donde son las mismas problemáticas, pero masificadas, ya que tienen un alcance más alto, se hace muchas más transacciones. En la cual se encuentran casos como Yahoo con 3 billones de cuentas hackeadas seguido de Alibaba con 1 billón de cuentas, y los casos de Wikileaks donde personas accedían a las bases de datos y las filtraban o como Analítica de Facebook donde nos enteramos de que usan los datos mucho más allá, como datos y elecciones. Entonces lo que se empieza a mirar, es como se pueden meter las autoridades de un país sabiendo que no fue desde acá.

En Colombia en el artículo 15 de la Constitución de 1991, introduce el concepto de manera directa, y esto es lo que le da la posibilidad a Ciro Angarita de introducir el concepto en la sentencia ya mencionada. Y con la ley 1581 se logra avanzar en una regulación mucha más robusta.

Respecto, a la protección de datos a nivel mundial, respecto a la conciencia a nivel global para tener una regulación al menos, y los países que no la tienen se debe mirar el contexto político en concreto.



Tomado de: Presentación del Doctor Felipe Sandoval Villamil - Regional Head Legal de DiDi

Preguntas y Comentarios.

1. **Intervención de la Doctora Margarita Useche - Docente de la Universidad Externado de Colombia**

La Doctora Margarita comentó que como docente siempre se está viendo que pasa con la SIC, y manifestó que le sorprende el comportamiento de la Corte Suprema de Justicia o su concepto sobre el tema de manejo intimidad en el entorno familiar y datos personales, fue un caso de violencia intrafamiliar, en el cual la esposa se da cuenta que su cónyuge o compañero permanente le estaba haciendo infiel y le dice déjame ver tu celular y entonces se le dice no, y ahí empieza una discusión en el contexto familiar que termina con una agresión de parte de él, porque ella alcanza a quitarle el celular y a ver los mensajes que él estaba teniendo con la otra persona, y como trata la Corte Suprema de Justicia el tema diciendo que ayudó violación a la protección de datos personales en el ambiente familiar. Entonces comentó que se está llegando a un tema en el cual dónde vamos a poner la frontera de lo que en realidad es esa violación especialmente en el espacio íntimo.

2. Intervención del Doctor Andrés Fernández de Castro - Director del grupo de práctica de Tecnología, Comunicaciones & Protección de Datos de Gómez Pinzón Abogados

El Doctor Fernández, comentó el caso de Yahoo, sobre la importancia de que las empresas se deberían enfocar en proteger los datos no solo por el ánimo de cumplir y evitar sanciones evitar, sino por ejemplo por el tema efecto reputaciones que eso termina teniendo, con Yahoo cuando ocurrieron esos incidentes de seguridad, este era un proveedor de correos electrónicos supremamente importante, tenía una posición de mercado, era un buscador de los más utilizados y hoy día nadie usa Yahoo, ya no es el proveedor de correo electrónico de preferencia, tampoco es el buscador de preferencia. Donde puede que al final esa filtración de datos haya tenido un efecto, y no solamente desde el punto de vista de los consumidores, sino como las empresas que incumplen sus obligaciones o que tienen este tipo de situaciones afecta no solamente en su posición de mercado sino incluso el valor de la compañía.

3. Intervención de Camilo Suárez - abogado recién graduado.

Camilo Suárez, hizo un comentario respecto al caso del Canal 1, respecto a su mal manejo de Datos, donde la sanción de la SIC se queda ahí, pero los datos van al otro lado del mundo y es un problema de la globalización, cuando se intenta ir en contra de grandes multinacionales.

4. Intervención del Doctor Lorenzo Villegas - Socio de CMS Rodríguez-Azuero

El Doctor Villegas, hizo un comentario respecto al tema de protección de datos cuando se vuelve autónomo del derecho a la intimidad. Ya que la protección de los datos es un tema operativo, no es un derecho fundamental autónomo y así la corte lo haya dicho, y es controversial ya que un dato es simplemente información y cobra relevancia constitucional cuando se asocia la intimidad y la constitución lo trae en el mismo artículo, solo que después la corte trata de separarlo. Lo que se mira es que todas las primeras leyes buscan es la protección del individuo frente al estado como consecuencia del uso de los datos, por ejemplo, el caso de Alemania para poder perfilar judíos.

Realmente, la protección de los datos se da dentro de un intercambio económico que requiere el flujo de datos, se analizan los antecedentes del convenio 95, donde se debe permitir que los datos fluyan dentro de un marco seguro para poder fortalecer el marco común europeo, eso no se mira en Colombia ni los países latinoamericanos y lo que se hace es una visión prohibitiva del flujo de datos. La ley colombiana de los 80 es prohibitiva, prohíbe el flujo de datos y este no es malo, debe ser libre y es necesario para el intercambio económico, para la formación de empresas, para los beneficios de los consumidores y los usuarios.

PRIMER PANEL: ¿ES SUFICIENTE/ADECUADA LA PROTECCIÓN QUE TENEMOS?

Moderador:

1. **Andrés Fernández de Castro - Director del grupo de práctica de Tecnología, Comunicaciones & Protección de Datos de Gómez Pinzón Abogados**

Panelistas:

2. **Carolina Botero - Directora de Fundación Karisma**
3. **Sol Beatriz Calle D´Aleman - Docente e investigadora del Departamento de Derecho Informático de la Universidad Externado de Colombia.**
4. **Lorenzo Villegas - Socio de CMS Rodríguez-Azuero**

Intervención de Andrés Fernández de Castro - Director del grupo de práctica de Tecnología, Comunicaciones & Protección de Datos de Gómez Pinzón Abogados

El Doctor Fernández inició agradeciendo al departamento de Derecho de las Telecomunicaciones y a los panelistas. Así, planteó que hoy en día lo que se debe buscar es proteger el derecho a la intimidad de las personas, donde dentro de la exposición de motivos de la ley 1581, hace 10 años se veían algunos que motivaron sin duda la expedición de la misma, por ejemplo, la alta automatización en el uso de datos personales, las incertidumbres que los titulares tenían sobre lo que hacían las personas que trataban los datos y otro tema es si Colombia era un país seguro de acuerdo con los estándares de la comunidad europea. De este modo, hoy en día tenemos situaciones similares, la automatización es muchísimo mayor, y en lo personal cree que subsisten algunas incertidumbres por parte de los titulares y los responsables encargados de los datos.

Sin embargo, comentó que, a pesar de los esfuerzos de las autoridades colombianas, Colombia todavía no es un país adecuado bajo los estándares de la norma europea, lo cual dificulta ciertas situaciones en materia transferencia de datos personales, que es uno de los de los focos o de los temas importantes que el mercado quiere regular.

Asimismo, resaltó que la ley 1581 ha sido supremamente importante porque ha permitido que las personas reconozcan la importancia los datos personales (titulares y encargados), de este modo, hace 10 años ninguna compañía en realidad era consciente de las obligaciones que tenía que asumir, y hoy día esto están en la mente todas las organizaciones, independientemente que tengan una base tecnológica o no.

Panel de Preguntas.

1. **¿Cómo usted percibe la apropiación de la ley 1581 por parte de los obligados (personas de derecho privado y de derecho público)?**

Intervención de Carolina Botero - Directora de Fundación Karisma
La Doctora Botero agradeció a el departamento y a los presentes, y comentó que ellos revisan todos los años los informes de transparencia todos los años, en 2015 se fijaron que copiaban y pegaban la ley, hoy en día es diferente, las empresas hacen pedagogía de la ley, ya han mejorado mucho, hay un cambio culturar y se crea un espíritu competitivo, se interesan por los estándares internacionales. Mientras que por el lado del estado es lo mismo, pero el impacto no ha sido tanto como con el sector privado.
Respecto a la evolución en política de protección de datos casi es inexistente, como en la SIC y en Coronapp, la asesoría brindada no fue buena, pudo ser mucho mejor, por lo tanto, se tiene que venir trabajando en esto.

1. **¿Cómo parte de esta apropiación de las normas que regulan estos temas, qué opinión tiene sobre el carácter vinculante de las guías, tienen obligaciones exigibles para los encargados, y otras son a veces una repetición de la guía inicial?**

Intervención de Lorenzo Villegas – Socio de CMS Rodríguez-Azuero
El Doctor Villegas comentó que el marco legal de protección de datos es complejo, el cual arranco en 1991, y durante más de 20 años fue jurisprudencia de la Corte, sobre todo en tutelas, y cambiaban mucho el precedente.
Así, aclaró que en el año 2008 cuando se crea la ley 1266, inicialmente iba a ser general, y la sentencia de la corte saca otros principios que no había traído antes, luego viene la ley 1581, es una ley que está mal hecha por el afán para que los europeos nos validarán para mandar datos, esa ley sería inaplicable en Colombia, sino fuera por la sentencia de la corte, lo que se debe aplicar es lo que dice la corte.
De igual manera, con el Decreto 1377, algunos doctrinantes dice que viola la ley, pero este le da un salvavidas, luego de esto aparecen las guías, donde pone una carga hacía el otro, así debería ser, cada vez que se entra a una página web comenta si queremos las cookies o no, nadie lee las políticas de privacidad, y cuando se acepta, eso no protege a nadie, la autorización es una ficción inventada por los alemanes, donde nos copiamos, y es un modelo que solo sirve si me preguntaran cada 6 meses, pero estos abordan diferente información, lo que se

debe hacer es crear reglas de cómo proteger, si la gente lee políticas de privacidad pasarían 1 mes leyéndolas, se debe mover a un modelo de guías.
De esta forma, respondió a la pregunta diciendo que las guías no son vinculantes, lo que pasa es que a veces la SIC obliga a ciertas compañías a aplicarlas, si no las sancionan, no deberían sancionarlo por la guía.

1. **La mayoría de las decisiones de la SIC y las quejas de los usuarios no se refieren necesariamente a incumplimientos de la ley 1581, sino por el contrario de la ley 1266, pareciera que la ley le importa más la información financiera. ¿Será que hay un problema de información o un énfasis desmedido?**

Intervención de Sol Beatriz Calle D'Aleman – Docente e Investigadora del Departamento de Derecho Informático de la Universidad Externado de Colombia
La Doctora Calle agradeció al departamento y a los presentes, y comentó respecto a la ley 1266 de 2008, que además fue reformada el año pasado por la ley 2157, que vino como norma estatutaria a darle un poco de tranquilidad a todos los deudores después de la pandemia, y si uno se da cuenta de los problemas digamos que les aquejan a los ciudadanos colombianos desde que aparecen las normas de protección de datos personales en Colombia, no debería llamar la atención que justamente lo relacionado con el habeas data financiero sea lo que hoy posiblemente tiene más cabida dentro de las investigaciones de la superintendencia, donde la mayoría de las quejas y de tutelas, casi el 90% se refieren a los datos de las personas reportadas, la permanencia del dato negativo.

1. **¿Consideran ustedes que hoy existe cierta incertidumbre o falta de certeza sobre algunos de los lineamientos de la ley 1581 que ameriten volver a revisar algunos aspectos?**

Intervención de Carolina Botero - Directora de Fundación Karisma
La Doctora Botero explicó que es importante la ampliación de una ley respecto al tratamiento de datos del sector público, hay un vacío que genera un problema que cada vez va a ser mayor, no se conoce ni siquiera los criterios. Otro tema concreto es respecto a las campañas electorales, no se enteran de que hacen tratamiento de datos.

Intervención de Sol Beatriz Calle D'Aleman – Docente e Investigadora del Departamento de Derecho Informático de la Universidad Externado de Colombia

La Doctora Calle comentó que en el año 2003 se presentó el proyecto 64 de parte de la Defensoría del Pueblo, pero esta no se aprobó, por lo tanto, lo que tenemos que mirar es como el Congreso pasa el tablero para poder avanzar. Así mismo, la ley 1581 es una copia de la ley orgánica española, que se vuelve estatutaria y que desarrolla un derecho fundamental, no abarca todo, así esta no ha tenido buenos reglamentos. Por lo tanto, lo que faltan son buenas reglamentaciones, el nuevo proyecto de ley solo trae un nuevo artículo, el resto lo tiene la ley 1581 de 2012.

Intervención de Lorenzo Villegas – Socio de CMS Rodríguez-Azuero
El Doctor Villegas comentó que debería cambiarse el modelo de protección de datos, sabiendo el flujo de datos para que funcione dentro de un marco seguro, sabiendo que el flujo de datos es necesario, para así Colombia poder ser competitivo. Por lo tanto, tenemos que poner la protección de datos en un tema procedimental, como se debe hacer el flujo.

1. **¿El consentimiento por sí solo en todos los casos constituye una medida de protección efectiva para los titulares?**

Intervención de Sol Beatriz Calle D'Aleman – Docente e Investigadora del Departamento de Derecho Informático de la Universidad Externado de Colombia
La Doctora Calle comentó, que la ley 1581 con el régimen de protección de datos personales se volvió una obsesión, y a la norma le falta el interés legítimo, en el cual es posible tratar datos personales sin que el consentimiento se convierta en una obsesión, donde lo podemos crear a través del derecho privado.
El interés legítimo no está consagrado en la ley, pero en la práctica esta, los ciudadanos entregan sus datos, pero a estos lo que más les molesta es quien tiene sus datos, que van a hacer con estos, y la seguridad de sus datos. Por lo tanto, lo más importante es el deber de educar a los ciudadanos y la seguridad.
Así mismo, opinó respecto al principio de libertad, donde no se puede tachar el carácter de derecho fundamental que tiene el habeas Data la intimidad y la protección de datos personales, ya que significaría cambiar la Constitución, los datos personales son atributos, el usuario decide si los expone no, la persona debe saber a qué se expone la persona a tribuir sus datos, lo que se debe hacer es disminuir los procesos.

1. **¿La regulación como está formulada causa algunas dificultades prácticas para los responsables en materia de la obtención del consentimiento y de la prueba de este?**

Intervención de Lorenzo Villegas – Socio de CMS Rodríguez-Azuero

El Doctor Villegas, comentó que es un problema, porque el reglamento 1377, tiene contradicciones, pero permite que la ley funcione, la corte constitucional es clarísima el consentimiento válido es el expreso informado e inequívoco, mientras que la ley 1377 dice que una conducta tácita como las conductas inequívocas, el cual es el más evidente en el mundo del comercio electrónico, es difícil de probar, por lo tanto, se debería dar una primacía al consentimiento, no usarlos para el perjuicio y que no se pierdan y no se los roben.

1. **¿Existe alguna diferenciación respecto de la Superfinanciera y la SIC respecto a la interpretación de la ley 1581?**

Intervención de Sol Beatriz Calle D'Aleman – Docente e Investigadora del Departamento de Derecho Informático de la Universidad Externado de Colombia

La Doctora Calle, comentó que ese choque de trenes entre las dos, se han dado un poco por no entender el sentido real de las normas de habeas data Financiero, y esa famosa excepción que tiene la ley 1581 cuando dice no se aplica a las bases de datos de la ley 1266, donde estos realmente no son datos, porque es en realidad es el proceso el que está por fuera de la ley 1581, que se resume en consulta y reporte en centrales de riesgo.

1. **¿Quién debería tener las facultades sancionatorias del sector público la Procuraduría o la SIC?**

Intervención de Carolina Botero - Directora de Fundación Karisma

La Doctora Botero, expresó que respecto a esto hay un dilema muy grande, ya que la procuraduría hace muy poco viene ejerciendo este rol, mientras que la SIC es la que ha venido ejerciendo por 10 años, hoy en día la SIC puede investigar, pero precisamente como la facultad sancionatoria la tiene la procuraduría y la decisión frente a eso, esta le puede pasar la investigación y queda en manos de la SIC. Así, puede ser interesante el rol que puede realizar la procuraduría si ejerce su función, en relación con los derechos humanos.

Conclusiones

Intervención de Sol Beatriz Calle D'Aleman – Docente e Investigadora del Departamento de Derecho Informático de la Universidad Externado de Colombia

La Doctora Calle comentó que debemos entender que en el artículo 15 hay tres derechos fundamentales y que el derecho a la protección de datos personales

también es un derecho fundamental, es que se puede lograr una protección a la intimidad, y cuando uno entiende que el derecho fundamental a la protección de datos personales busca garantizar el habeas data de las personas y busca garantizar su intimidad, pues entiende que ya no son asuntos separados, sino que es una tríada que si la entendemos desde la perspectiva constitucional, tendrían respuesta esas malas prácticas.
Asimismo, resaltó la importancia de los neuro derechos para ser seres humanos aumentados, que tiene que ver con mis datos de creencia, mi nombre, mis datos y mi dignidad, ya que se potencia el cerebro humano como la máquina más poderosa, y eso nos va a volver a poner en el centro de exposición los derechos constitucionales de las personas, más que pensar el procedimiento o en las reglas concretas.

Intervención de Carolina Botero - Directora de Fundación Karisma
La Doctora Botero comentó, que lo más importante es la vigilancia estatal y la vigilancia de las empresas, precisamente la suma de los datos que hay disponibles, están permitiendo unos niveles de vigilancia en el entorno laboral, en el entorno educativo, en el espacio público, en todos lados, por lo que los datos son los movilizadores.
Así mismo, expresó que el problema más grave va a estar en torno al Estado, que considera que la protección de datos no le aplica y que la intimidad se justifica por sus fines legales, etcétera y allí hay temas interesantes que se discuten hoy a nivel internacional, como es el acceso de los estados a los datos de los privados, el cual tiene tres mecanismos para hacerlo: dándole la orden de que se los entregue; comprándolos y cuando las empresas se los dan por voluntad propia, los cuales tienen que ver con el lenguaje que se usa en protección de datos.

Intervención de Lorenzo Villegas – Socio de CMS Rodríguez-Azuero
El Doctor Villegas opinó que este tema tiene que dejar de estar en el lado procedimental, se debe enfocar en los problemas éticos que están de fondo, en el fondo es un debate que debe existir como debe ser el desarrollo del derecho a la intimidad en un mundo globalizado y lleno de tecnología.

SEGUNDO PANEL: PRIVACIDAD VS. DERECHO A LA INFORMACIÓN Y LIBERTAD DE EXPRESIÓN

Moderador:

5. **Juan Carlos Upegui – Docente Investigador de la Universidad Externado de Colombia**

Panelistas:

6. **Gustavo Gómez – Director Ejecutivo de Observacom**
7. **Lucia Camacho – Abogada de Dejusticia**

Intervención de Juan Carlos Upegui – Docente Investigador de la Universidad Externado de Colombia

El Doctor Upegui, inició el panel resaltando que el tema central de este panel es la protección a ese derecho fundamental, como lo ve la concepción europea, y como lo llamamos en América Latina como Habeas Data y después por la influencia europea derecho a la protección de datos, en el cual reside unas situaciones problemáticas, las cuales se incrementan cuando traemos otros derechos, en este panel se intentará identificar los debates en el derecho comparado.

Así, les pregunto a los panelistas sobre casos en donde las relaciones entre estos dos derechos el derecho a la protección de datos o habeas Data y el derecho a la libertad de expresión o acceso a información sea especialmente problemático, y a partir de esos casos, empezar a preguntar de forma más específica por cuestiones regulatorias y por los distintos escenarios en donde estos derechos concurren de forma problemática.

Intervención de Lucía Camacho – Abogada de Dejusticia

La Doctora Camacho invitó a los presentes a leer un artículo denominado “La instrumentalización de las acciones de protección de datos del reglamento europeo de protección de datos”, en el cual dice que las acciones dirigidas por grupos de poder buscan silenciar a través de solicitudes de reparación millonarias los ejercicios legítimos de la prensa, buscan prevenir la posición política y enviar un mensaje contundente donde se les castiga por publicar este tipo de información, en este se da el caso de Forbes en el año 2019, donde pretendió publicar un listado anual de los más ricos, e informa a cuatro personas de una misma empresa, que hacían parte de la misma familia, estos objetan el uso de sus nombres, pero Forbes dice que esta información lo consiguió por fuentes y registros públicos, en este caso el juez no le da la razón a Forbes, ya que esta

información en realidad no es de interés público, por lo tanto Forbes no podía hacer uso de estos datos de esa manera.

Intervención de Gustavo Gómez - Director Ejecutivo de Observacom

El Doctor Gómez agradeció la invitación y a los presentes, así inició explicando que cuando se habla de privacidad se habla de protección de datos personales, su identificación, su posición, y demás. Hoy en día en América Latina, si se habla de privacidad se incluye el derecho de imagen, como parte de un derecho personalísimo, el cual ha sido usado para limitar la libertad de expresión y la libertad de prensa, por ejemplo, cuando funcionarios públicos o candidatos impiden que sean usado su imagen por otros partidos o la prensa.

De igual forma, comentó que respecto en la regulación privada, en el marco de protestas en Ecuador un medio digital y comunitario denunció que una plataforma una red social le eliminó un contenido donde difundía violencia contra una de sus periodistas, porque según la plataforma esa publicación era información sensible de terceros sin consentimiento, entonces se está viendo la remoción de contenido de internet por denuncia de terceros o por la propia plataforma. Otro caso fue en Uruguay donde se dio la desindexación de notas periodísticas sobre vínculos de lavado de dinero en el narcotráfico, por aplicación europea, ni si quiera de Uruguay por protección de datos personales, por denuncias de algún involucrado en esas notas.

Panel de Preguntas

2. ¿Cómo se ve la capacidad regulatoria del régimen de protección de datos sobre ejercicios de libertad de expresión y demás términos relacionados?

Intervención de Lucía Camacho – Abogada de Dejusticia

La Doctora Camacho, comentó que las expresiones gozan de lo que no gozan la protección de datos es una presunción de cobertura, donde tiene mucho más poder regulatorio frente a la libertad de expresión, esto se puede ver en el escenario colombiano con la cantidad de acciones o mecanismos con los que cuenta alguien que hace un reclamo por protección de datos frente alguien que busca proteger su libertad de expresión, ya que primero cuenta con los mecanismos internos de la plataforma o red social para solicitar la eliminación de la publicación, las mismas redes sociales están haciendo litigio en favor de la protección de datos de usuario frente a terceros que usan de manera ilegal los datos obtenidos en la red social, la judicialización vía acción de tutela, medidas cautelares por solicitud de medidas de bloqueo cautelar, acciones propias de protección de datos, y por último la vía penal y civil para solicitar reparación. Por lo

tanto, podemos ver que la libertad de expresión esta más desprotegida en Colombia.

Intervención de Gustavo Gómez - Director Ejecutivo de Observacom
El Doctor Gómez comentó que desde un punto de vista debería, ya que se habla de privacidad y libertad, estos dos derechos son constitucionales, es decir, así como la Convención Americana de Derechos Humanos en su artículo 13 reconoce el derecho a libertad de expresión, el artículo 11 reconoce al derecho a la intimidad, donde estos no son absolutos, entonces, desde un punto de vista teórico, no se puede decir que el derecho a la protección de datos o el derecho a la privacidad no pueda afectar el derecho a la libertad de expresión, la discusión es la proporcionalidad y legitimidad de esos límites, por lo tanto, se puede ver que no hay ningún tratado internacional que ponga un derecho encima del otro.
Así mismo, expresó que desde una perspectiva de la doctrina del derecho a la libertad de expresión se hacen advertencias muy claras de que ciertos aspectos legítimos como regular la privacidad o los datos personales, no debería afectar la producción o difusión de cuestiones de interés público, el tema es hasta donde es legítimo la protección de datos personales para no afectar indebidamente otros derechos, sin que estos sean superiores.

3. **La ley de habeas data es muy clara en excluir el régimen de protección de datos personales de las bases de contenido periodístico y otros archivos editoriales. ¿Esta excepción es operativa? ¿Cuál es el sentido del legislador al incluirla?**

Intervención de Lucía Camacho – Abogada de Dejusticia
La Doctora Camacho, comentó que es muy interesante, y desde la acción de bloqueo temporal de datos, que es una medida cautelar temporal que puede interponer la autoridad de protección de datos, donde se ha dictado en casos de libertad de expresión, y esta excepción ha relucido.
Así, esta medida si ha sido elevado la solicitud de bloqueo por la persona afectada, si existe un riesgo cierto para la vulneración de su derecho fundamental a la protección de datos y otros derechos fundamentales, se interpone para proteger ese derecho de manera temporal, y si no se trata de ninguno de los eventos exceptuadas por la ley.
De esta manera, comentó un caso sobre el indebido uso de fotos, los cuales son considerados como datos personales en Colombia, y este trata de unas fotos de una mujer que han sido publicados con el propósito de publicitar contenido sexual, en este caso la Superintendencia de Industria y Comercio, realizó un análisis de la excepción, y dice que este no es un caso de libertad de expresión, y si lo fuera estaría excluido de la aplicación de la ley 1581, pero hay que recordar que incluso

a los eventos de excepción les son aplicables los principios de la ley, por lo tanto, la aplicación de los principios de obligatoria, por lo que, la aplicación de la ley se hace obligatoria y podría ser alcanzada para dictar medidas de este tipo para la protección de esos principios, la excepción es relativa no restrictiva.

Intervención de Gustavo Gómez - Director Ejecutivo de Observacom

El Doctor Gómez comentó que esta cláusula común en el derecho comparado, en estos casos debería primar la libre expresión sobre el derecho de habeas data, además de que esta excepción es operativa, ya que en el nuevo mundo de internet, aunque algunos no tienen acceso, hoy se constituye los nuevos espacios públicos alrededor de las redes sociales, donde eliminar contenidos en base de archivos de medios de telecomunicación cada vez es más irrelevante, ya que hay tanta información en internet, y donde van apostando toda la artillería para impedir el acceso a la información de interés público, que pudiera afectar a corruptos, torturadores, violadores de derechos humanos, etc, no es ir al medio y pedirle que verifique el archivo que tienen en la red y que lo actualicen o lo borren, sino lo que están haciendo es ir a quien indexa ese contenido para que alguien lo encuentre.
De esta manera, expresó que hoy en día no se busca la protección de los archivos de los medios tradicionales sino en los buscadores, por lo tanto, es irrelevante, ya que hoy no se van a cada medio de comunicación, sino que se van a un solo buscador para que lo baje del buscador, es decir, la información está ahí pero nadie lo encuentra, así hoy el esfuerzo por restringir el acceso es mínimo frente a un impacto que finalmente es el mismo de perseguir a medios de comunicación que tienen diez notas sobre el mismo caso.

4. **¿Dentro de esos posibles ajustes que se le harían a la ley, debería estar el derecho a bloquear, rectificar, actualizar informaciones personales contenidas en archivos de contenido periodístico y otros contenidos editoriales o cualquier información personal que esté disponible en internet, como una red social, que suponga un supuesto tratamiento ilegítimo de protección personal?**

Intervención de Lucía Camacho – Abogada de Dejusticia

La Doctora Camacho comentó que hay un relegamiento de esa figura que aparece en escenarios de coyuntura política donde el derecho al olvido ha sido puesto en la discusión pública por figuras que accionan contra medios y que, por su descontento, por el actuar del medio y del intermediario internet deciden impulsar, porque tienen la capacidad política, impulsar proyectos de ley.
Así mismo explicó que en Colombia el derecho al olvido ha sido reconocido jurisprudencialmente, donde se delega la tarea de desindexación de la noticia a cargo del editor y no tanto de los buscadores, que no tienen ni deberían, porque determinar si un contenido es de interés público o satisface ese criterio o no para que merezca ser actualizad, no debería pasar. Así, la Doctora manifestó que las necesidades regulatorias van por otro lado, ya que recientemente las

modificaciones al reglamento y reflexiones del reglamento europeo de protección de datos que es un norte al que va ir apuntando nuestras legislaciones, donde se ha ido apuntando a la necesidad de fortalecer no tanto los instrumentos de la aplicación de la misma ley, sino las capacidades de aplicación de la misma ley, como las capacidades de la autoría de protección de datos para imponer sanciones, actuar de manera proactiva oficiosa, ampliar el conjunto de obligaciones que tienen los responsables en materia de protección de datos, cambiar los criterios de aplicación extraterritorial y obligar a los responsables en materia de tratamiento de datos a que tengan presencia en los países a través de una figura como la del representante o autoridad local de del tratamiento de datos, para que la excusa de que no estamos domiciliados allí, y que por lo tanto su ley no me alcanza, deje de serlo y la ley en verdad tenga una mayor aplicación.
Teniendo en cuenta esto, la Doctora Camacho cree que el debate sobre el derecho al olvido se debería dejar que se siga dando, para entender cómo va en la jurisprudencia constitucional, que ha acertado en el abordaje que ha hecho en Colombia, y que, por lo tanto, hace falta que madure un poco para entender como luego podría ser la recepción legislativa, si es que conviene o no hacerla.

Intervención de Gustavo Gómez - Director Ejecutivo de Observacom
El Doctor Gómez manifestó que comparte las previsiones de Lucía, donde se deben plantar unos escenarios de protección en materia de libertad de expresión, ya que las herramientas son de tipo reactivo y de impedir, por lo tanto, se podría avanzar, pero no necesariamente debe ser un tema del congreso.
Por lo tanto, comentó que se tiene un problema con las legislaciones públicas que pudiera avanzar y reconocer para aplicar un derecho al olvido, que no se recomienda seguir como una idea en nuestras legislaciones de América Latina. Además, se necesita impedir que nos apliquen derecho al olvido por decisiones propias de las empresas transnacionales, dueñas de las redes, ya que nosotros al tratar de impedir o impulsar esa revisión normativa para que el estado no aplique indebidamente la aplicación de datos personales que pudiera afectar indebidamente la libertad de expresión, donde tenemos un elefante blanco donde todos los días está bajando o des indexando contenido que no deberían, por lo tanto, se debería decir, el estado no debe hacer esto y estableciendo obligaciones para que las empresas tampoco lo hagan, no se puede aceptar que el estado ponga a las empresas privadas como policía privada, para definir por sí mismas, que información de interés público, donde hay protección de datos sensibles, y seguir aceptando que todos los días lo hagan sin ningún tipo de control, por lo tanto, se necesita por lo menos que se coloque la obligación de transparencia sobre lo que hacen por decisión propia, ya que no nos aplican ni la propia legislación, sino leyes europeas o de estados unidos, y no notifican a los usuarios

que lo bajaron, des indexaron o le redujeron el alcance, además de tener el derecho a apelar una decisión que nos parece injusta.
De esta manera, se debe ser cuidadoso y prudente al momento de innovar en la legislación, y poner más atención en cómo podemos con la legislación existente proteger más los derechos, pero sin embargo, se tiene mucho por hacer, donde hoy estamos frente a un actor privado mucho más poderosos que algunos estados nacionales, que están afectando de manera sistemática el derecho a la libertad expresión en aras de proteger los datos personales, donde esto no se debería permitir, por lo tanto, se deberían implementar leyes para evitar que haya no solo entes privados sino también públicos que estén afectando los derechos de los usuarios.

Conclusiones

Intervención de Lucía Camacho – Abogada de Dejusticia
La Doctora Camacho comentó la necesidad que se tiene de cara estos primeros 10 años de la ley 1581 de diagnosticar cuales son los problemas de la ley, donde los más urgentes están por el lado de la libertad de expresión o el ejercicio del derecho a la protección de datos en las plataformas de internet, que como se ha visto este año, ni siquiera las redes sociales ante solicitudes de protección de datos de sus usuarios, de mirar donde están los datos, que han hecho con ellos, y que ante leyes como las nuestras, incluso diseñadas con las mejores intenciones podrían responder de la manera más garantista para la persona, por lo tanto, se necesita hacer esos ejercicios de diagnóstico para saber en dónde están las oportunidades para introducir las mejores.

Intervención de Gustavo Gómez - Director Ejecutivo de Observacom
El Doctor Gómez manifestó que comparte la opinión de la Doctora Camacho, ya que las soluciones no deben surgir de la nada y deben ser una respuesta del diagnóstico, para identificar si es un problema de texto legal o es un tema de otro nivel, además es importante incluir las dificultades del entorno digital por la masividad, la velocidad, la globalidad, la existencia de empresas que ni siquiera están instalados en el territorio colombiano, para una aplicación de los datos personales más efectiva en general, pero se debe advertir que no siempre la mejor forma de proteger la dignidad delas personas, su privacidad, la existencia de información que es inexacta es la vía de la protección de datos personales, ya que también ayudaría a plantear otras herramientas complementarias, como justicia civil por daños y perjuicios.

TERCER PANEL: LEY 1266 DE 2008.

Moderador:

8. **Carlos Salazar - Director de investigación de Protección de Datos Personales de la SIC**

Panelistas:

9. **José Manuel Gómez - Vicepresidente jurídico de Asobancaria**
10. **Gloria Urueña - Directora Ejecutiva del COLCOB**
11. **Natalia Tovar - Vicepresidente Jurídica y de Asuntos Corporativos de Experian**

Intervención de Carlos Salazar - Director de investigación de Protección de Datos Personales de la SIC

El Doctor Salazar dio la bienvenida a los presentes, comentando que el panel tratara sobre la protección de habeas data financiero, donde esta es una norma que tiene que ver con todos los ciudadanos, ya que en la SIC en el año 2021 se rompió el récord de las quejas presentadas por violación de estas normas, recibieron 36.000 quejas de las cuales el 87% están relacionadas con la aplicación de habeas data, y mirar la aplicación de la ley 2157, ya que fue la modificación de esta ley, que fue la incorporación de la responsabilidad demostrada y políticas internas efectivas.

Panel de Preguntas

5. ¿Cuáles son las acciones que ha adoptado Expirian para aplicar estos principios de responsabilidad demostrada desde la órbita de la ley 1266 de 2008?

Intervención de Natalia Tovar - Vicepresidente Jurídica y de Asuntos Corporativos de Experian

La Doctora Tovar expresó su agradecimiento por la invitación y a los presentes por su asistencia, así comento que, respecto a la responsabilidad demostrada, uno a veces piensa que es un tema de llenar muchos documentos y hasta allí llego la responsabilidad demostrada, ya que en Expirian una de las líneas de negocio es Data Crédito, por lo tanto, el centro de la compañía es la información.

Así comentó que respecto a la responsabilidad demostrada, empezó hace mucho tiempo, desde el código de conducta de Data Crédito, que es de 1998, el cual tenía unos procedimientos, después con la ley 1581 viene la responsabilidad demostrada, pero cuando se ve la reglamentación se mira que el corazón de la compañía es la 1266, y que por lo tanto, se tiene que empezar a implementar la

responsabilidad demostrada para esta ley, en la compañía Expirian se hizo un inventario de principios y deberes, desarrollados por las leyes y la Corte Constitucional, y definieron 5 pilares, los cuales son, finalidad, calidad, acceso y seguridad, tratamiento leal y transparente a la información y atención al ciudadano, y con estos se definieron los estándares que le aplicaban a cada uno de esos estándares, y a partir de esto se adoptó una política.
A partir de esto, la Doctora comentó que se implementó una política, donde cada uno de esos estándares se le ponía un responsable, y que políticas y procedimientos les aplicaban a esos pilares, y se registraron en la herramienta de riesgos para que se ajustaran, y con base a esto se generaron indicadores, y se empezó a generar un tema de cultura con la gente, para que se apropie del tema.

6. ¿Cómo se ha enfocado el principio de responsabilidad y políticas internas efectivas en el sector y que faltaría por hacer?

Intervención de Gloria Urueña - Directora Ejecutiva del COLCOB
La Doctora Ureña expresó su agradecimiento por la invitación al gremio, y así comentó que hicieron de mano con la SIC un recorrido a nivel nacional socializando la ley 1266, la ley 1581 y el principio de responsabilidad demostrada, donde las empresas asociadas entendieron que tendrían que desarrollar teres puntos orientados a robustecer su tema documental, como son (i) políticas o procesos enfáticos frente al correcto cumplimiento dela ley 1266 (ii) enfocarse a reforzar esos controles y fomentar capacitación permanentes a toda la organización, ya que se puede poner en riesgo la privacidad de los datos (iii) incorporar auditorias que se hacen en la mayoría de organizaciones, para identificar y corregir esos hallazgos.
De este modo expresó que todo esto le abrió un camino a COLCOB, para construir un estándar de privacidad que es una guía que fue exclusiva para la industria y que se compartió a la SIC, la cual fue asociada con todo el gremio, donde su objetivo primordial fue mitigar esas confusiones de la ley 1266 y 1581 en su interpretación y darle claridad al sector, y que entendieran que son leyes complementarias.

7. ¿Cómo se aborda el principio de responsabilidad demostrada en el sector financiero?
Intervención de José Manuel Gómez - Vicepresidente jurídico de Asobancaria
El Doctor Gómez agradeció por la invitación y a los presentes, así comentó que para el sector es muy importante el manejo de toda la información de sus clientes y de sus eventuales clientes, donde este tema se viene trabajando desde el siglo pasado y que surgió desde la asociación bancaria todo el manejo de centrales de

información en los años 90, era muy complicado en esa época porque era través de papel y la consulta no era tan fácil y ágil como se hace hoy.
De esta manera comentó, que para las entidades financieras es muy importante y son cuidados en el manejo de esa información, y de la necesidad de implementar unas políticas y procedimientos de ese manejo, así mismo en la ley del año 2021 esta obligación de tener una responsabilidad demostrada, pero eso ya existía en el sector financiero y no solamente para la ley 1266 o para la ley 1581, ya que las entidades financieras no solo manejan información financiera sino también información personal en establecer políticas en establecer procedimientos capacitación.
Así, expresó que este tema es muy alto en las entidades financieras, ya que se designa los responsables del manejo de la información, además que hay un esquema de capacitación, de formación y educación importante para la propia entidad, sus trabajadores y los terceros que trabajan para ellos.
En este sector se ha hecho mucho por el esquema de responsabilidad demostrada, ya que obliga a ser mucho más proactivos en el manejo de la información, pero lo más grave es que con el desarrollo tecnológico esto no termina, ya que este va introduciendo nuevos esquemas de manejo de la información, donde la responsabilidad implica que se tiene que implementar un esquema nuevo para esas nuevas tecnologías de la información, donde en 10 años va a ser distinto a como se maneja hoy, pero siempre implementando políticas procedimientos, capacitaciones y un equipo que maneje la información al interior de las de las entidades.

8. **En el 2019 la SIC encontró que se incrementó la suplantación de identidad en un 142%, la pandemia hizo que se incrementará este fenómeno. La ley 2157 adicionó a la ley 1266 relacionados con la suplantación de identidad. ¿Desde centrales de riesgo cómo han visto estos nuevos instrumentos?**

Intervención de Natalia Tovar - Vicepresidente Jurídica y de Asuntos Corporativos de Experian
La Doctora Tovar comentó, la ley 2157 tiene dos mecanismos, el primero es cuando una persona que ha sido objeto de suplantación puede acudir a la entidad, y esto ha hecho que el mecanismo sea más expedito y que las entidades presenten más atención.
Así, desde las entidades de centrales de riesgo estaban preparados para sacar un sistema, en el que todos los ciudadanos pueden inscribirse, dejar su correo electrónico y así se les puede avisar tan pronto se reporta una nueva obligación en la central de riesgos, en utilizar cada día lo vemos, de esta manera las centrales

de riesgo ven cada día como se va moviendo el número alertas, es una buena forma para ver si uno está siendo objeto de suplantación.
De esta forma, para la Doctora Tovar hay dos mecanismos que es un tema de educación financiera, ya que la consulta del historial crediticio es gratis, y es importante que la consulta del crédito, pero en suplantación tener la constancia de revisar esta, se puede prevenir la suplantación. En Experian hay una herramienta de cuando creo que estoy siendo objeto de suplantación, como cuando se pierden los papeles, se puede entrar y poner una alerta, y cuando las entidades van a evaluar van a ver la alerta.

9. ¿Cómo ha abordado el gremio el tema de suplantación de identidad?

Intervención de Gloria Urueña - Directora Ejecutiva del COLCOB
La Doctora Ureña comentó que el mecanismo implementado ha permitido que se pueda dar mucha más celeridad a este trámite, en el cual se ha identificado obligaciones que venían de vieja data y nuevas que caen en mora, y se identifica que es una suplantación, a esos reclamos se les han dado una respuesta efectiva y eso acerca más a los sectores originadores y a los clientes del común, eso hace más grata la relación y nos ayuda a mantener al cliente en un sistema formal crediticio.
Seguido a esto, la Doctora Ureña comentó que se debe implementar espacios de trabajo para buscar que en la toma de decisiones de estas situaciones de suplantación se pueda hacer la resolución evitando criterios subjetivos en los que se puede caer, donde todo el gremio han hecho grandes desarrollos en temas de inteligencia artificial, servidores, herramientas tecnológicas en general, en aras de identificar plenamente a los usuarios y evitar la suplantaciones, y a pesar de mecanismos más modernos como la biometría facial, validación de datos con huella, reconocimiento de voz, entre otros, la regulación no irá a la misma velocidad que va la tecnología y que va la delincuencia, entonces se debe trabajar para anticiparnos a lo que sucede, y pedirle a la fiscalía que le den más celeridad a la búsqueda de las bandas delincuenciales.

10. ¿Cómo van las entidades financieras respecto a la suplantación de identidad y las nuevas normas?

Intervención de José Manuel Gómez - Vicepresidente jurídico de Asobancaria
El Doctor Gómez manifestó que la ley 2157 tiene un esquema de implementar un mecanismo para que las personas puedan recibir retroalimentación cuando hay una nueva obligación, pero este mecanismo para que funcione, la persona se tiene que registrar. Desde Asobancaria, se tiene un esquema de biometría para

que cuando una persona va abrir una cuenta, a pedir un crédito o cualquier vinculación financiera, pues se conecta directamente la entidad financiera con la registraduría para confirmar la huella, esto ha disminuido la suplantación en las entidades de una manera significativa, sin embargo, no todas las entidades están vinculadas a ese esquema de biometría, pero se espera que se vinculen, así mismo Asobancaria tiene un boletín de seguridad donde se invita a profundizar más sobre la suplantación de las personas.

De esta manera comentó que, respecto a la ley de recientemente expedida, puede ser un poco complicado el texto de la parte inicial o del primer artículo que habla de suplantación, en donde simplemente con la manifestación de la persona se elimina la información, donde interpone un esquema de manejo de quién tiene la razón sin que haya una investigación anterior y antecedente.

Intervención de Natalia Tovar - Vicepresidente Jurídica y de Asuntos Corporativos de Experian

La Doctora Tovar aclaró que en este caso la entidad debe solicitar los documentos que considere pertinentes para validar esa suplantación o antes de hacer una modificación en el registro de la central de riesgo, y tienen diez días hábiles para cotejar la documentación que aporten los titulares. Entonces, la entidad recibe la solicitud y baja el reporte de las centrales, y si determinó que existía la suplantación elimina el dato o en caso contrario lo vuelve a subir, por lo tanto, el esquema es garantista para ambas partes.

11. El régimen de transición de la llamada “Ley de borrón y cuenta nueva”. ¿Qué conclusiones se puede tener desde los gremios y los operadores de información de este régimen de transición?

Intervención de Natalia Tovar - Vicepresidente Jurídica y de Asuntos Corporativos de Experian

La Doctora Tovar comentó que cree que lo mejor que trajo esta ley fue la responsabilidad demostrada, donde estamos en un mundo donde hay nuevos actores, nuevos datos e ideas, y cuando se tratan datas se debe pensar en la ética y en la transparencia, y la herramienta de la responsabilidad demostrada, da la posibilidad de moverse en el marco de la ética y la transparencia para generar confianza con los titulares, con los empleados de la compañía, con el mercado y con el regulador, y la responsabilidad demostrada se enmarca en esto como una obligación de los actores del sistema.

De igual manera, expresó que esta ley trajo una amnistía que se denominó “ley de borrón y cuenta nueva”, que trae primero un aspecto general donde los tiempos de caducidad de la información disminuyen en un período específico, que era el año siguiente la vigencia la ley, entonces normalmente en Colombia se maneja un concepto que solamente en Colombia, y es que la información dura el doble de la mora, no es una sanción sino una historia, que se maneja generalmente de

máximo 4 años, y si la mora fue inferior a 6 meses es el mismo tiempo de mora, entonces, varias personas se acogieron para que caducará anticipadamente su información.
Con base a lo anterior, comentó que “más información, más crédito”, ya que las centrales de riesgo son algo que construye la garantía de reputación, la gente que no tiene garantías reales como un carro o una casa, nace esto denominado garantía de reputación, para decir que la persona cumple con sus obligaciones, está hecha para democratizar el crédito, para mirar cómo la gente paga sus obligaciones, y en Colombia el 93% de información es positiva, por lo tanto, toca mirar en un futuro como se comportaron las personas que se acogieron y que incidencia tuvo, sin embargo, esto no es bueno para un sistema, fue en un momento especifico, por la pandemia, por lo tanto, el camino es construir una historia del crédito más que pretender que se borre un dato esporádicamente, es un tema de hábito, por consiguiente, al eliminar estos datos hace que no se generen más créditos.

Intervención de Gloria Urueña - Directora Ejecutiva del COLCOB
La Doctora Ureña comentó que la industria siempre se ha intentado alinear con las disposiciones normativas en materia de habeas data, no se han tenido inconvenientes, salvo en compra de cartera, y se puede decir, que esos son instrumentos que permiten dinamizar la economía concediendo oportunidades a esos clientes que han tenido dificultades, y estas se van a el vendedor de cartera, donde esté en la mayoría de los casos no suministra a los compradores de la industria los soportes que demuestren el cumplimiento de estas normas de habeas data, por la dificultad de encontrarlas, puede ser en créditos antiguos, entonces se traslada está dificultad a los compradores de carteras, lo cual no tendría ninguna dificultad si el requerimiento si se hiciera de la misma manera que se asume, que esto ha sido validado por la superintendencia.
De modo que, se debe dar un dinamismo a la compra de cartera, que es el que al final devuelven a clientes en dificultades a un sistema formal crediticio bajo unos principios de equidad, derechos y deberes, y que además nos tenemos que enfocar también en las microfinanzas, ya que son sectores para atender poblaciones más vulnerables. De esta manera comentó que es saludable dar amnistías para pagos, pero no a mediano y largo plazo.

Intervención de José Manuel Gómez - Vicepresidente jurídico de Asobancaria
El Doctor Gómez manifestó que la ley trajo unas cosas interesantes como la responsabilidad demostrada, y genero posibilidades de recuperación, pero el periodo de transición es preocupante, ya que cuando la información que se utiliza para hacer un análisis de riesgo se vuelve sospechosa, esta se vuelve

sospechosa para todo el mundo, entonces, por beneficiar a un número muy pequeño, se termina afectando a todo el mundo y las reglas que se interpusieron fueron diferenciales.
De igual forma, comentó que se debe pensar en la transcendencia que tiene este beneficio, porque como comentaba la Doctora Natalia casi el 93% de la información que está en la central es positiva, entonces, es como si fuera un diamante para el titular de la información, para tratar de mantenerla incólume como si fuera para el análisis del riesgo y del crédito.

Intervención de Natalia Tovar - Vicepresidente Jurídica y de Asuntos Corporativos de Experian

La Doctora Tovar comentó que en Colombia 7 de cada 10 créditos, se entregan a estratos 1, 2 y 3 por ese 94% de información positiva, entonces ahí es donde se puede dar cuenta que esa amnistía genera una democratización en los créditos, pero la invitación es que las personas mantengan y cuiden su historial crediticio.

SEGUNDO DÍA

CUARTO PANEL: EL ESTADO COMO GARANTE DE LOS DERECHOS DE LOS CIUDADANOS

Moderadora:

12. **Sandra Milena Ortiz, directora del Departamento de Derecho de las Telecomunicaciones de la Universidad Externado de Colombia.**

Panelistas:

13. **Heidy Balanta - Directora de la Escuela de Privacidad**
14. **Juan David Gutiérrez – Profesor de la Universidad del Rosario**
15. **Nelson Remolina – Docente de la Universidad de Los Andes**

Intervención de la Doctora Sandra Milena Ortiz, directora del Departamento de Derecho de las Telecomunicaciones de la Universidad Externado de Colombia.

La Doctora Sandra Ortiz dio un cordial saludo y bienvenida a los presentes, expresó el honor de estar moderando el panel, comentó sobre el tema central del panel sobre analizar el tema de cómo el estado es un garante y como administra datos personales, y desde la Constitución del 91, con esa consagración de derechos en materia proyecto de privacidad y datos, se ha desarrollado una línea jurisprudencial y legal.

Intervención de Nelson Remolina – Docente de la Universidad de Los Andes

El Doctor Remolina agradeció la invitación para conversar sobre los 10 años de esta ley, y comentó que además de mirar el cumpleaños de la ley se debe mirar y comparar como estamos, mirar el nivel de cumplimiento, y el estado tiene dos roles en ese tema, el primero como garante porque la ley estatutaria confiere a una delegatura que se encargue del tema de la protección del debido tratamiento de datos, y segundo el estado como un sujeto obligado cumplimiento estás normas y de la constitución.

De esta manera, comentó que tener una norma de protección de datos no es fácil, en Colombia el primer proyecto de ley de protección de datos fue de 1985, o sea solo 23 años después salió la ley 1266 de 2008, es una ley sectorial, y por eso salió la 1581 de 2012, no es fácil porque existe muchos intereses en relación con los datos, ya que estos

son el zumo determinante de la economía digital, no solo el estado sino las empresas viven de los datos de la explotación de los datos, cosa que no es ilegal, la regulación se da para exigir que se haga determinada manera, que no se ponga en riesgo los derechos de los ciudadanos.

Hoy en día quienes tienen más datos son las empresas privadas, hoy la tecnología da para que empresas extranjeras recolecten datos, y estas son las que tienen más datos de este país, lo cual refleja la regulación el estado llegó tarde, internet principalmente se ha regulado por normas corporativas, políticas, documentos privados que emiten las empresas, el principal instrumento regulador de internet son los contratos e instrumentos, especialmente los contratos de adhesión, pero esos instrumentos son los que vinculan a más de 3.3 billones de ciudadanos, por ejemplo de la política de Facebook.

Por lo anterior, la regulación de datos, viene también desde las empresas, una política de datos de una compañía impacta más de 3.3 billones de personas en el mundo, más que cualquier ley de la República de cualquier país, incluso de Colombia, y hay que mirar el debate porque muchas de esas empresas crearon sus políticas basándose en el modelo de negocio explotación de datos, una regulación de datos que expidan va a afectar eso, es como una reforma tributaria, por lo que las empresas deberían ser tan celosas y diligentes en el manejo de datos, como exigen en la protección de sus secretos empresariales, porque afecta los derechos de cualquiera de nosotros. Así, se debe plantear si actualmente los estados deben someterse a las políticas de las empresas, o las empresas a las leyes de los estados, y esto se debe ver desde los proyectos de ley, si se regula con un fin constitucional, debe haber un equilibrio entre derechos, innovación y explotación de los datos.

Así mismo, comentó que el tema de datos no solo debe ser un tema de intimidad, ya que el único que lo menciona es la recomendación de la OCDE en 1980, pero de ahí para allá todos hablan de tratamiento de datos, no se puede decir que datos o tratamiento de datos, es igual a intimidad, esto es un error, hoy en día no solo afecta la intimidad, sino el buen hombre, su libertad, hay mucha gente detenida por error por órdenes de captura erróneas, esto se encuentra en la sentencia T310/2003, los datos son igual a la identidad digital, las decisiones de los ciudadanos cada vez más se toman fundamentado en bases de datos en perfiles que se crean, pero esto debe hacerse bien de manera transparente, hoy existen 45 países con regulación de datos general y más de 95 con una autoridad de protección de datos.

Por lo anterior, Colombia no puede ser un país que se dedica únicamente a cortar los datos de los colombianos a todos los países, Colombia debe ser un país donde lleguen datos de todas partes del mundo para que nuestras empresas sean competitivas, porque si tenemos genios haciendo proyectos de Inteligencia artificial más grande de algoritmos en Colombia, pero no tenemos los datos de todas partes del mundo que lleguen acá para procesarlas, pues no estamos haciendo nada.

El estado como sujeto obligado, tiene unos deberes desde la constitución, no puede hacer lo que quiera, las entidades públicas tienen unos deberes, como los artículos 2 y 6 de la Constitución. Respecto a las estadísticas, hace 2 años, solo cerca del 28% de las entidades públicas estaban haciendo un registro, mientras el sector privado está cerca del 75%, esto pasa porque principalmente solo lo cumplen las entidades del orden nacional, pero las entidades públicas a nivel departamental y municipal, no conocen la Ley de protección de datos, pero el hecho que no se conozca no significa que no deba aplicarse porque una parte del deber de un funcionario público, es cumplir la Constitución y la ley.

Respecto, a las entidades públicas si bien la ley 1581 crea unas excepciones frente a la autorización, que es un tema de legitimación, la gente se preocupa más por incumplir la ley de 2009, ya que contempla el delito de violación de datos personales, la autorización es una forma de facultar el tratamiento datos de manera legítima, pero no es la única, el estado por regla general no requiere autorización de los ciudadanos para tratar sus datos, siempre y cuando sea para cumplir unas finalidades.

La calidad de la información de las bases de datos del estado, según las estadísticas que tiene la SIC, en leyes como la 1266, el principal motivo de queja de los ciudadanos el 75%, es la calidad de la información, entonces hay que mirar tenemos bases de datos o basureros de datos, porque si eso es lo que tiene el estado y con eso es que toman decisiones políticas públicas, pues hay un gran error, simplemente partiendo de la calidad la información.

La información confidencial, el estado no debe manejarlo como quiera, sino para unos fines específicos, la ley 1581 tiene unos deberes para todos funcionarios públicos o no, de mantener confidencialidad, debe haber medidas de seguridad de la información, porque si no se enfatiza en esto se estaría afectando derechos humanos.

Intervención de Heidy Balanta - Directora de la Escuela de Privacidad

La Doctora Balanta, manifestó que la ley 1581 tiene tres principales problemas, por un lado, (i) la instrumentalización de la ley, y en ese punto se mira cómo están las entidades públicas en la apropiación de la ley, y muchas se rajan en esto, (ii) los encargados, mirar como esos proveedores que tratan los datos de los ciudadanos, para cumplir temas de transmisión de datos, o por ejemplo, Colombia Compra Eficiente, acuerdos listos que no se pueden modificar para el tema de tratos de datos, intercambio de bases de datos, pero no hay una claridad en esas transferencias u organizaciones. (iii) Expedición de leyes, donde se ven varios proyectos de ley que no tienen sentido, ya que existe una ley estatutaria, que define y establece unas reglas en materia de protección de datos, y sale un proyecto de ley que sale con otras palabras o adornando otras cosas que no es necesario, como el de suplantación de identidad y el de los mensajes de texto, porque no hay una entidad que les ponga freno, y del lado judicial también, las decisiones judiciales tienen unos retos desde la seudonimización o anonimización, los avances en la divulgación de decisiones judiciales, la Corte Constitucional expidió la circular 10 de 2022, donde establece algunas reglas en materia de seudonimización. De esta manera, se tiene que ver como en cada sector su aplicación o su cumplimiento.

Así mismo, expresó el tema de la Procuraduría General de la Nación, la cual es muy poco el ejercicio de la aplicación de la ley 1581, ya que esta le informó a la Doctora Balanta, que tenían 110 investigaciones contra servidores públicos, y de estas ninguna termino con una sanción, y otra respuesta que dan es que la resolución del 2019 donde se le asignaban funciones a la Procuraduría para investigar a funcionarios públicos ya no está vigente por la modificación que hicieron este año, y además se lavan las manos diciendo que no harán ninguna investigación preventiva, eso le corresponde a la Superintendencia de Industria y Comercio, desconociendo lo establecido en la Ley 1581 de 2012.

El manejo de los datos por parte de las entidades públicas y la explotación de estos, como los sistemas biométricos, tema de reconocimiento facial, la inteligencia artificial es muy importante, para mirar la garantía de protección de estos.

Intervención de Juan David Gutiérrez – Profesor de la Universidad del Rosario

El Doctor Gutiérrez agradeció la invitación y comentó la importancia de hablar que el estado necesita explotar datos, así los primeros censos se hicieron en Egipto para mirar la producción de trigo, la importancia del contexto actual, es que el estado colombiano está creando una estructura masiva para recopilar datos personales y no personales, lo que está bien para tomar decisión y crear valor público adicional a través de los datos, y por

eso hay CONPES a la explotación de Bigdata, a la inteligencia artificial, hay un Plan Nacional de Infraestructura de Datos.

En la automatización, el estado tiene un rol de consumidor de tecnologías y de datos, pero al mismo tiempo es regulador, y los estados tienen fama que no son eficaces, por lo que el atractivo a veces son las apps o la tecnología, pero el estado no debe olvidar que es regulador, ya que la entidad encargada de verificar no lo está haciendo. De esta manera, con CoronApp, la Corte Constitucional expidió dos sentencias, la primera la T-143/2022 interpuesta por 4 ciudadanas periodistas que le exigieron descargar la app para ingresar a un vuelo, y esta aplicación implicaba datos personales y acceso a la ubicación, la Corte Constitucional le recuerda al estado que aún en una situación excepcional como la pandemia, siempre debe cumplir con los principios y el núcleo duro de la protección de datos personales, y recuerda la sentencia de control de constitucional informático de la ley 1581. El segundo caso, es de un Ciudadano que solicita a la Agencia Digital que le dé acceso al código fuente de la APP, y esta le dice que no puede hacerlo porque implicaría violar los datos personales de las personas y los derechos de autor, la Corte no ha expedido una sentencia, pero la discusión tiene que ver si se debe dar acceso a la aplicación con los datos usados, ya que se puede separar el código de los datos.

1. **¿Cuál es la responsabilidad que tiene el estado frente a las fugas de información y ataques a las páginas web? ¿A quién se le puede imputar responsabilidad? ¿Esta función la debe tener la Superintendencia o se debe crear un organismo independiente?**

Intervención de Nelson Remolina – Docente de la Universidad de Los Andes

El Doctor Remolina, explicó que el modelo de una autoridad de protección de datos es el que funcione de acuerdo con cada país, toca medir las autoridades no solo por cuantos funcionarios, sino por resultados, en la Superintendencia de Colombia se tiene autonomía y en los últimos 10 años se ha fortalecido la autoridad, hay más herramientas, y mayor personal.

Si se miran las estadísticas de la SIC, al 2022 son 112 mil quejas ciudadanas, anualmente crece el 39%, la mayoría son quejas de privados, las entidades no deben esperar a que los ciudadanos se quejen sino actuar, de estas 112 mil quejas 48% se archivaron, es decir, no se encontró ninguna irregularidad, lo cual es bueno, ya que significa que esta ley se puede cumplir, solo 1% han llegado a multas, y un 7% de órdenes, que no son sanciones, se usa para proteger derechos o prevenir, la SIC actualmente ha hecho en los últimos 3

años estudios de seguridad con base al Registro Nacional de Base de Datos de 33 mil organizaciones, ese estudio ha servido para tomar acción, ha expedido casi 8 mil érdenes, la mayoría de oficio, ya que si ponen No, se expiden medidas para evitar usos indebidos.
Cuando se pensó en la ley 1581 se pensó en no multar a las entidades públicas, ya que sería multar a todos los ciudadanos del país, entonces lo mejor era que se manejara disciplinariamente por la Procuraduría General de la Nación, le SIC ha dado órdenes a entidades públicas sobre temas de seguridad, como a la Alcaldía para implementar medidas de seguridad con las Apps.

Así mismo, la ley 1581 sobre datos no es ningún obstáculo para labor periodística porque queda excluida, sí ha habido hasta acciones algunos periódicos por utilizar los datos recolectados para hacer marketing y publicidad, que ya no es labor periodística como tal.

2. **¿Cómo solventar el tema de la procuraduría? ¿Cómo manejar la protección de datos y la transparencia en la publicación de hojas de vida o la publicación de declaraciones de renta?**

Intervención de Heidy Balanta - Directora de la Escuela de Privacidad

La Doctora Balanta manifestó que no se puede decir que la ley se rajó, sino que fue la institución, respecto a las multas y las sanciones, el comisionado de información del Reino Unido manifestó que se debe bajar las multas a las entidades públicas, ya que cuando se multa a una entidad pública por protección de datos es castigar al público dos veces, lo que se debe hacer es ayudarles a conocer sus necesidades, parte de la necesidad de la apropiación de la ley debe tener una visión preventiva.

Así mismo, tenemos el principio de confidencialidad y de acceso y circulación restringida de la ley 1581, que aplica a entidades públicas y privadas, y con la ley 1712 que tiene el principio de máxima publicidad, pero ahí empieza esa contradicción, dos normas que regulan un mismo objeto, que viene generando diferentes problemáticas, Colombia debe hacer una clasificación de información, mirando el contexto de la intimidad (personal, familiar, social, gremial), se tiene que mirar las esferas, hasta qué punto se debe proteger la intimidad de sus funcionarios publicando sus hojas de vida.

3. **¿Cómo el estado debe ser garante? ¿Cómo se explotan los datos por parte del estado? ¿Qué nos hace falta para lograr esto?**

Intervención de Juan David Gutiérrez – Profesor de la Universidad del Rosario

El Doctor Gutiérrez manifestó que no hay regulación algorítmica o de transparencia algorítmica en Colombia, estamos quedados, hay un formulario que deben diligenciar las entidades públicas todos los años que es el Formulario Único de Reporte de Gestión, tiene más de 100 preguntas y una pregunta es qué tecnologías emergentes usan como sistemas automatizados, y de los resultados de 2021 se sabe que más de 200 entidades respondieron que usan IA o RPA, el gobierno creo una página web denominada inteligencia artificial para registrar sus herramientas de inteligencia artificial, pero solo están registradas 7, en realidad hay más, debe haber un principio básico de transparencia para que se sepa como usan mis datos, donde se debe explicar para cuándo se usa sistemas automatizados explicar cómo usa y como entrenó el algoritmo, la transparencia no solo es publicidad sino la explicación que se deba dar, y hoy no tenemos mecanismos jurídicos para que el estado responda efectivamente relacionadas con protección de datos y de transparencia.

4. ¿Cómo usar esa política de prevención frente a los datos que se tiene o la explotación que se puede dar frente a una emergencia futura?

Intervención de Nelson Remolina – Docente de la Universidad de Los Andes

El Doctor Remolina comentó la importancia del principio de veracidad o calidad de la información, la norma dice que “se prohíbe el tratamiento de datos que induzca a error”, por lo tanto, depende de la información que se introduzca, se tiene que también mirar el interés legítimo, de preguntar si se pueden usar estos datos o no.

En Colombia el mecanismo de SIC Facilita, que es una alternativa de solución de controversias, para datos de 2019 con 10.000 acciones, se logró el 78% de acuerdo voluntario en menos de 20 días, lo cual demuestra que es un mecanismo expedito, gratuito y eficiente, por lo que se debería implementar un sistema alternativo de solución de controversias en materia de protección de datos.

5. ¿Cómo generar una cultura de protección de datos en entidades no solo del nivel nacional?

Intervención de Heidy Balanta - Directora de la Escuela de Privacidad

La Doctora Balanta manifestó que se requiere una reforma a la ley de protección de datos, a pesar de que es una buena ley, peor hay que adoptar las figuras que han funcionado, como las autorizaciones para usar los datos. Hay que trabajar el tema de la portabilidad de datos personales, y de la clasificación de datos personales, o ampliar el concepto de dato personal y dejar el tema de elemento identificatorio.

QUINTO PANEL: EXPLOTACIÓN COMERCIAL DE LOS DATOS PERSONALES

Moderadora:

16. **Mónica Morales - Docente investigadora de la Universidad Externado**

Panelistas:

17. **Andrés Contreras - Director de Protección de Datos Personales del Banco AV Villas**
18. **Sarah Osma - Experta en protección de datos personales**

Intervención de Mónica Morales - Docente investigadora de la Universidad Externado

La Doctora Morales agradeció a los presentes su participación, y explicó que el panel tratará de cómo la empresa privada debe realizar el tratamiento de datos personales especialmente para fines personales, este es un tema muy importante, ya que se dice que los datos son el nuevo petróleo, donde se dice que se puede hacer perfilamiento de sus clientes, y la información es el combustible que permite a las nuevas tecnologías de Bigdata y de inteligencia artificial, pero jurídicamente estamos frente a derechos fundamentales personalísimos, donde estos dos discursos se deben ponderar, para encontrar en la ley respuestas y buscar mejoras para proteger al ser humano.

6. **¿Cuál es su opinión respecto a que el consentimiento sea la base de legitimación para el tratamiento de datos personales para fines comerciales?, teniendo en cuenta de que se habla de la paradoja de la privacidad, ya que los usuarios manifiestan en la toma de decisiones por el comportamiento del tratamiento de datos personales, pero en realidad no nos comportamos así. ¿Es necesario acudir a otras bases de legitimación?**

Intervención de Sarah Osma - Experta en protección de datos personales

La Doctora Osma explicó que si bien es cierto, la ley 1581 fue pionera en su momento, en cuanto el tema de la autorización que es muy importante y que sea lo primero que se analiza, se debe considerar otras bases legitimadoras para el tratamiento, en esa medida sería bueno implementar el artículo 6 del GDPR, y aunque cada vez hay más una cultura del dato, ya que cada ciudadano se acercan más a sus derechos tratar de imponer una serie de categorías como base legitimadora como tratamiento de datos no es necesaria. El tema más

puntual es promover la cultura de implicación de la cultura de datos, más que modificar lo que tenemos ahora en materia de autorización.

Así, debería existir una regulación por parte del estado, de la dimensión de compartir los datos con terceros con fines comerciales o de manera estadística, si va a ser gratuito o va a tener una contraprestación.

Intervención de Andrés Contreras - Director de Protección de Datos Personales del Banco AV Villas

El Doctor Contreras agradeció la invitación, la autorización de la ley 1581 da la posibilidad de que los ciudadanos se sientan dueños de sus datos, desde su perspectiva de entidad financiera, de cara al proyecto de decreto, se busca un enfoque a un acceso adecuado a la información por parte de las entidades financieras frente al uso de la información, y desarrolla la visión de estándares tecnológicos, donde el uso de los datos debe estar autorizada previamente por una autorización previa, expresa e informada.

Respecto a la comercialización de información de datos personales, se debe tener una autorización expresa, pero en materia financiera es más específica o especial, para entregarla a un tercero para no tener una injerencia. Esta autorización debe ser expresa y clara, para que no haya confusión para el usuario. Debe haber una cláusula expresa para la transferencia de los datos. Así se plantea la portabilidad de datos, donde el usuario puede elegir el destino de sus datos no a un banco x, sino a un producto en específico, desde el punto de vista del responsable puede no estar consciente de lo que dice la autorización, por lo tanto, se debe dar una cultura a nivel corporativo.

7. **¿Cómo ver lo que prevé la Ley 1581 vs las tecnologías que usan grandes datos? ¿Los principios o deberes son suficientes o hay algo que revaluar?**

Intervención de Sarah Osma - Experta en protección de datos personales

La Doctora Osma expresó que es muy importante dirigirse a los principios rectores y aposiciones académicas, como a la transparencia, donde todos los sectores se deben remitir, para dejarles claros que es un proceso tecnológico y explicarles, que se socialice la manera de cómo se toman las decisiones, como en materia de salud, el valor de estas bases de datos es muy alto, como en las aseguradoras, como las apps que rastrean que como o la actividad física podría

llegar a las aseguradoras, para mirar cómo nos comportamos, y que pueden tener una gran responsabilidad o perjuicio en la vida de los titulares.

Así mismo, comentó que respecto a la ley 1581, esta no se debería modificar, sino que se debe realizar una interpretación más consiente de los principios, es parte del operador jurídico y de la entidad, para usar como guía estos principios rectores.

Intervención de Andrés Contreras - Director de Protección de Datos Personales del Banco AV Villas

El Doctor Contreras comentó que cuando se habla de decisiones automatizadas basadas en al análisis de datos sensibles, es ir mucho más allá del avance de la tecnología, permitiendo a veces generar un sesgo de discriminación, por lo que se debe proveer a la máquina y al humano principios éticos para alinearse a la finalidad de por qué se creó el procedimiento o la máquina.

De esta manera, comentó que desde el análisis de lo que ha dicho el ente regulador independiente de la tecnología se aplican las fuentes normativas, la ley 1581 y la ley, por lo que no se puede aplicar esto a un punto en específico.

8. Dadas las prácticas de publicidad, desde la perspectiva de los empresarios que el principio de responsabilidad demostrada ¿es suficiente para que los empresarios se vean persuadidos para cumplir la ley o deben establecerse otras medidas, como las sugeridas por el CONPES de comercio electrónico como sellos de calidad o códigos de conducta?

Intervención de Sarah Osma - Experta en protección de datos personales

La Doctora Osma, explicó que se ha manejado como una opción, si se mira como una herramienta tiene un beneficio, como en el momento en que la autoridad adelante una investigación implemente un criterio de morigeración de que se ha implementado ciertas herramientas, este tipo de decisiones podría motivar a los empresarios, para ser más relevante para las políticas de las decisiones.

En cuanto al tema de las certificaciones, explicó que puede ser una muestra de responsabilidad, que puede ser un tema muy importante para la organización, que la matriz de riesgos materializa este tipo de situaciones que se podría caer en un incidente de seguridad que no es voluntario, pero se optó por un sistema

de consultoría y de capacitación, por lo que los empresarios le pueden ver la utilidad.

Intervención de Andrés Contreras - Director de Protección de Datos Personales del Banco AV Villas

El Doctor Contreras comentó que recientemente la Superintendencia, respecto al uso de los datos con fines publicitarios expidió una serie de deberes para concluir que el cumplimiento de la normatividad de datos personales se debe cumplir independiente del sector, se le dice al responsable que se debe proveer las herramientas para que informe si quiere seguir recibiendo esa publicidad y revocar la aprobación que le ha dado al responsable, y es interesante porque a veces los canales de revocación son diferentes a los de la aprobación, a partir de esto se mira la ausencia de importancia que le da el legislador a esto, y que genera que el empresario va a buscar cumplir con lo menos, para que actuar con algo que me puede llevar a una sanción.

9. **¿Cómo ve los retos en materia de confidencialidad en comercio electrónico y de apps?**

Intervención de Andrés Contreras - Director de Protección de Datos Personales del Banco AV Villas

El Doctor Contreras explicó que los procesos de estos datos distan mucho de lo esperado, en la forma en que se registra en el Registro Nacional de Bases de Datos, las empresas prefieren evitarse la sanción a no responder a una pregunta y mirar después que se hace, donde se trabaja con estándares de seguridad mínimos, en la práctica no se tienen efectiva esas medidas para cierta protección de datos personales, por lo tanto se debe informar la importancia de estos datos y realizar medidas de seguridad privilegiando al titular más no al modelo de negocio, para decirle al empresario como puede ajustar eso que tiene para cumplir.

10. **En relación con los incidentes de seguridad ¿Cómo estamos en Colombia?**

Intervención de Sarah Osma - Experta en protección de datos personales

La Doctora Osma expresó que hay una falta de claridad de cuál es la entidad para reportar los incidentes, debería haber la posibilidad de ampliar una manera

de cuáles sin las condiciones en las que se generó el incidente, y mirar quien es el responsable de hacer el reporte y las circunstancias de tiempo modo y lugar.

Intervención de Andrés Contreras - Director de Protección de Datos Personales del Banco AV Villas

El Doctor Contreras, manifestó que ese reporte no solo se debería informar a la autoridad sino a los titulares que se ven afectados con ese incidente de seguridad, bajo el entendido que el titular de los datos revise la autorización de datos que di, para ejercer un control sobre mis datos, por lo que adquirirá un mayor peso, ya que son pocas veces que genera un incidente ante la autoridad.

SEXTO PANEL: TRANSFERENCIA INTERNACIONAL DE DATOS

Moderador:

19. **José Alejandro Bermúdez - Socio de Bermúdez Durana Abogados**

Panelistas:

20. **Jonathan Mendoza – Secretario General de Protección de Datos del INAI de México**
21. **Sam Schofield – Policy Advisor del International Trade Administration del US. Department of Commerce**
22. **Michael Panzera – Federal Trade Commission**

Intervención de José Alejandro Bermúdez - Socio de Bermúdez Durana Abogados

El Doctor Bermúdez inició agradeciendo a la universidad por la invitación y explicó que el panel de hoy es un tema muy importante para el comercio internacional y para cumplir los objetivos de la OCDE de como generar protecciones efectivas a los titulares de datos personales.

De esta manera, comentó que en Colombia hace unos días el Centro Financiero de Dubai había reconocido a Colombia como un país adecuado en materia de protección de datos, dando luz a la ley de protección de datos que se ha venido implementando en Colombia, con una autoridad de protección de datos personales, que ha venido con la delegatura trabajando por generar guías, dar órdenes, abriendo investigaciones administrativas e ir promoviendo esa cultura que termina en estos reconocimientos.

Intervención de Jonathan Mendoza – Secretario General de Protección de Datos del INAI de México

El Doctor Mendoza agradeció la invitación, así inicio explicando que la protección de datos no puede ser una barrera para la economía digital, lo que se debe entender para desarrollar consideraciones.

Uruguay tiene 14 años con su legislación tiene en el ámbito latinoamericano que tiene un ámbito internacional más robusto, con la adecuación y con la Directiva 9546 que ya está abrogada y que está siendo revisada con GPDR y el Consejo de Europa. Mientras que México tiene una regulación de 12 años, que no ha sido modificada, inspirada en la Directiva 9546, especialmente en el reglamento.

Los países que han actualizado su regulación ha sido Ecuador, Brasil, Panamá, Cuba, Barbados y Bermudas, con conceptos tomados en el GDPR, donde se tiene un escenario donde hay muchas simetrías en la regulación. En Europa el GDPR es el paradigma, entro en vigor en 2018, hay países adecuados en el GDPR. Relevante es hablar de países como Singapur o Japón que tiene regulación nueva y que tienen un estándar mejor.

Así mismo, comentó que respecto al tema de la Portabilidad que, en México, que puede ser una vertiente al derecho de acceso o un quinto derecho si está regulado en el sector público, pero no está regulado en el sector privado. Las evaluaciones de impacto si está en el sector público, pero no en el sector privado, y así con otras, lo que refleja que se puede ir a normativas internacionales para robustecer la normativa mexicana.

Por lo anterior, expresó que se debería crear un sistema unido para todo Latinoamérica, donde haya modelos de convergencia y de reconocimiento mutuo, para que se genere un libre flujo de datos personales sin requisitos adicionales, pero para esto se debe tener un estándar convergente para todos los países.

Intervención de Sam Schofield – Policy Avizor del International Trade Administration del US. Department of Commerce

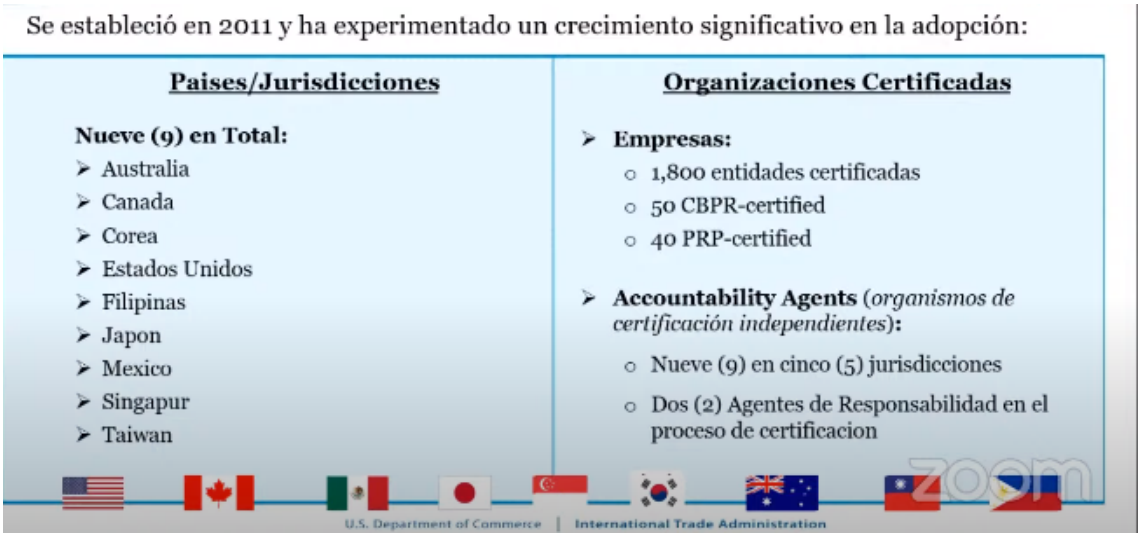
El Doctor Schofield manifestó su agradecimiento a la universidad por la invitación y explicó que trabaja en el departamento de Comercio en los Estados Unidos, así hoy en materia de protección de datos y privacidad las prioridades y objetivos de la administración de Biden con respecto a la privacidad de los datos y a la regulación del flujo transfronterizo de datos son los siguientes:

Tomado de : Presentación del Doctor Jonathan Mendoza – Secretario General de Protección de Datos del INAI de México

Así comento, que el Sistema CBPR, es un sistema de certificación de privacidad de datos respaldado por el gobierno creado en 2011 dentro del Foro de Cooperación Económica Asia-Pacífico (APEC), y cuando un país participa en el programa de CBPR, todos los requisitos de este programa son exigibles en las leyes domésticas, entonces un país puede tener otros requisitos, pero empresas que tienen la certificación CBPR la empresa debe cumplir con los requisitos de esto, y permite un sistema multilateral que genera interoperabilidad entre las leyes de los países miembros para que los datos puedan fluir entre las direcciones, además de flujos de datos transfronterizos a través de diferentes regímenes de privacidad.

Así mismo, el CBPR obliga a la cooperación de enforcement entre las autoridades de las jurisdicciones participantes, y asegura que protecciones comunes de referencia se trasladan con los datos entre jurisdicciones, consumidores en México no pierden sus derechos cuando los datos fluyen a los Estados Unidos, por lo tanto, esta Certificación de CBPR es reconocida en leyes nacionales y tratados de comercio como el T-MEC (México, Canadá y Estados Unidos).

La participación actual es el siguiente:



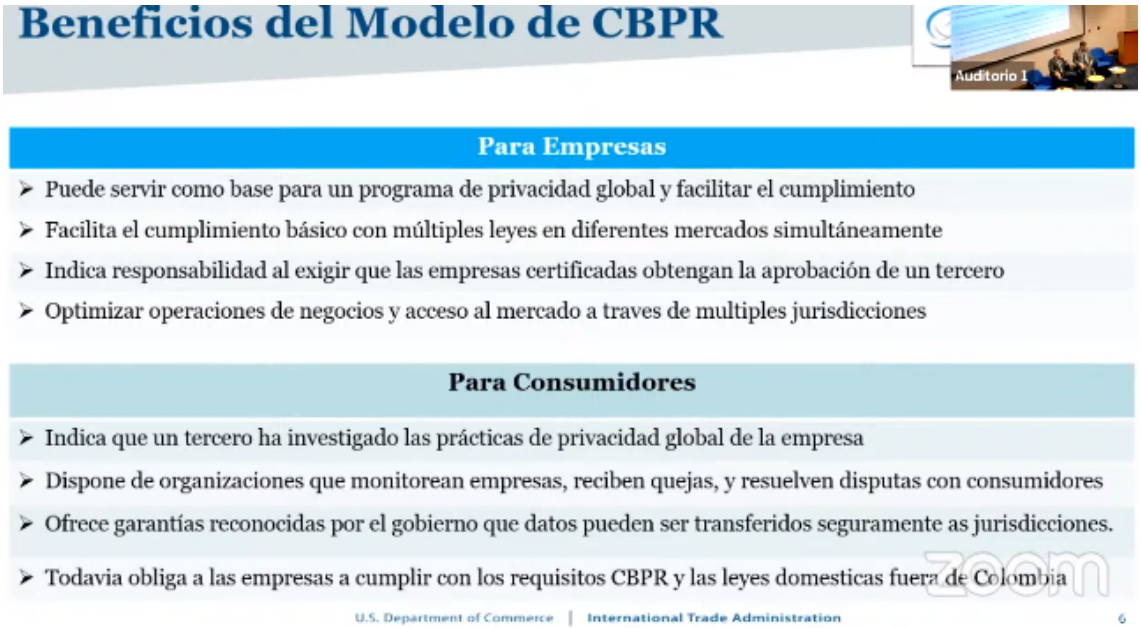
Tomado de : Presentación del Doctor Jonathan Mendoza – Secretario General de Protección de Datos del INAI de México

De esta manera, comentó que hay 3 actores principales en el sistema de CBPR, que son los (i) países/jurisdicciones, los cuales para participar su primer paso para pertenecer al sistema es designar a una autoridad para participar en el Cross-Border Privacy Enforcement Arrangement (CPEA), los (ii) Accountability

Agents, ellos tienen 3 responsabilidades de certificar empresas domésticas, deben monitorear los requisitos del programa, y deben repasar cada dos años las prácticas de privacidad de las empresas certificadas y las (iii) organizaciones certificadas, las cuales obtienen la certificación por 1 año.

Tomado de : Presentación del Doctor Jonathan Mendoza – Secretario General de Protección de Datos del INAI de México

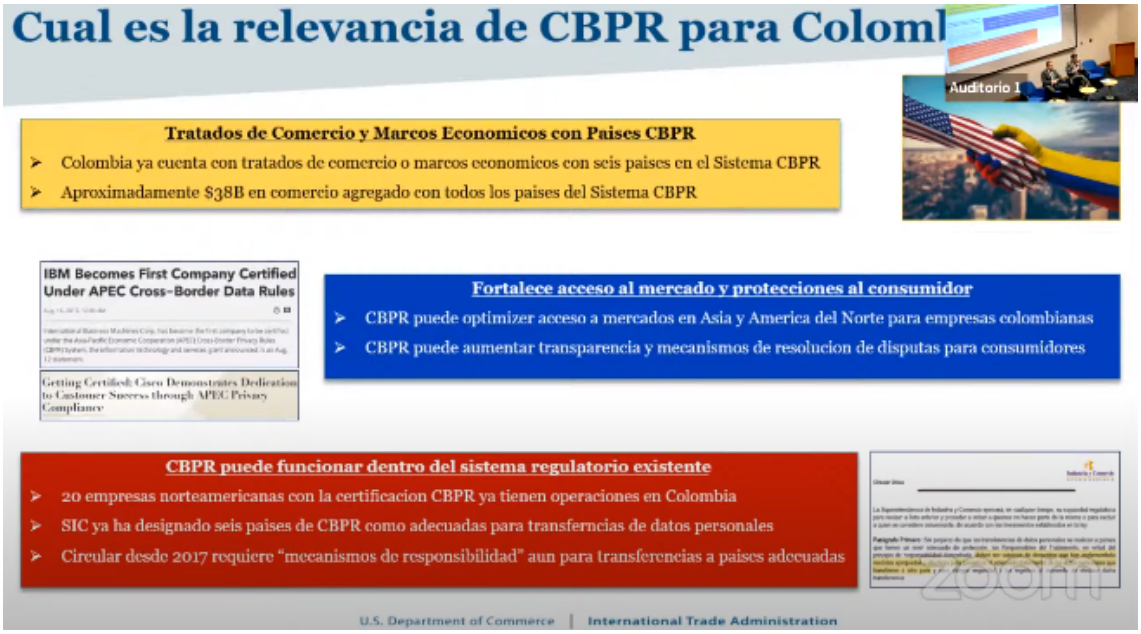
Hay muchos beneficios del modelo CBPR, como los siguientes, la certificación es muy importante para PYMES que quieren agrandar su negocio.



Tomado de : Presentación del Doctor Jonathan Mendoza – Secretario General de Protección de Datos del INAI de México

De esta manera, anunció que en abril se realizará el establecimiento del Foro Global CBPR, este foro quiere permitir que otros países participen, se pretende poner en marcha por el principio 2023 para permitir participación de países fuera de APEC, y este será administrado de forma independiente y separado de APEC.

Tomado de : Presentación del Doctor Jonathan Mendoza – Secretario General de Protección de Datos del INAI de México

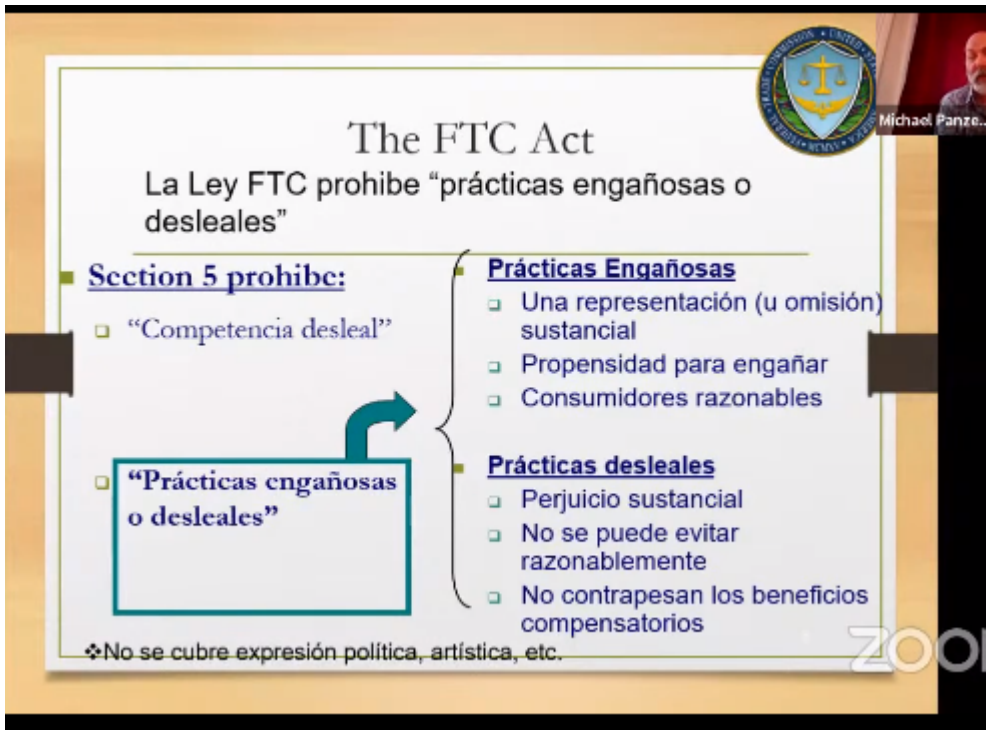


Tomado de : Presentación del Doctor Jonathan Mendoza – Secretario General de Protección de Datos del INAI de México

Intervención de Michael Panzera – Federal Trade Commission

El Doctor Panzera agradeció la invitación, y comentó respecto al tema de eficacia y eficiencia de las leyes de protección de datos, recalar la cuestión de los recursos y herramientas que tiene una agencia de protección de datos, donde los principios son importantes, pero si la agencia no tiene los recursos y las herramientas necesarias para aplicar la ley.

De esta manera, comentó los antecedentes de la FTC (Federal Trade Commision), la cual es la única agencia de protección al consumidor de jurisdicción general de los Estados Unidos, y tiene una división general dedicada a la protección de datos denominada “Division of Privacy and Identity Protection”, además de la Division of Enforcement que viola las ordenes de la corta para mirar que las empresas cumplan con estas, y la Office of Technology and Investigación (Otech) que fue creada hace 10 años para tener un equipo de técnicos para garantizar el monitorio y la vulneración de datos, estas tres divisiones trabajando juntas para garantizar la protección de datos en los Estados Unidos.

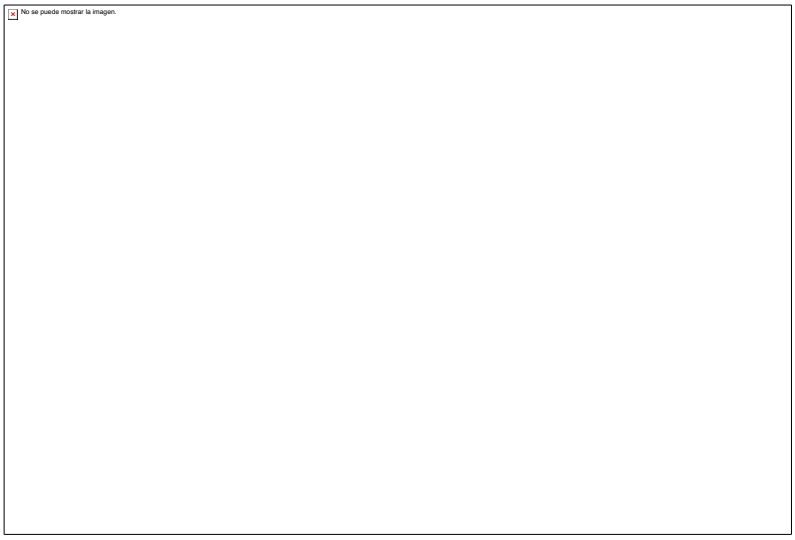


Tomado de: Presentación del Doctor Michael Panzera – Federal Trade Commission

De esta manera tienen leyes sectoriales, de niños, de datos financieros, de datos de salud y demás. En la mayoría de los casos, las partes llegan a un acuerdo que termina en órdenes de consentimiento aprobadas por el tribunal, y que tiene los siguientes aspectos:

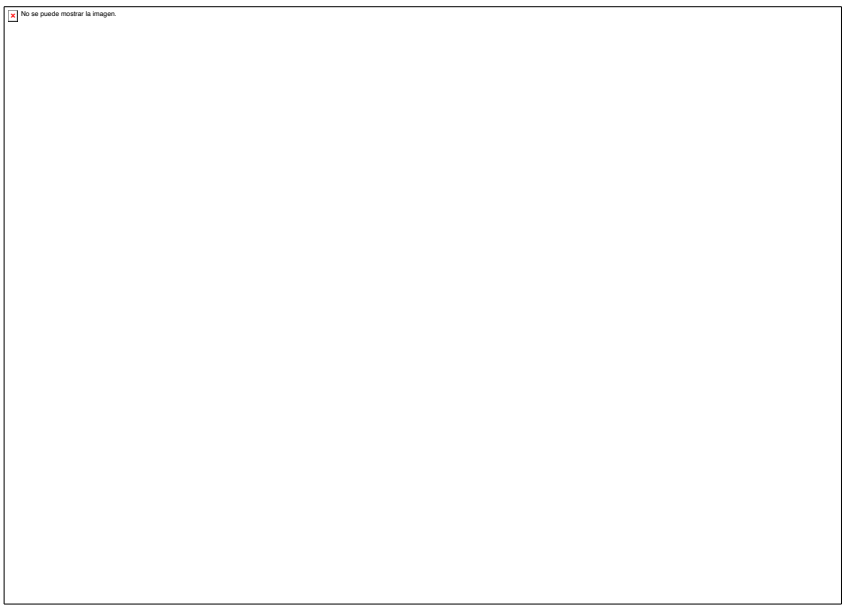
Tomado de: Presentación del Doctor Michael Panzera – Federal Trade Commission

De esta manera, explicó como aplica el sistema CBPR en los estados unidos, el cual tiene ciertos principios a los que cada país debe cumplir, entre esos el Accpuntability, que deriva consecuencias por el incumplimiento de estos.



Tomado de: Presentación del Doctor Michael Panzera – Federal Trade Commission

Cuando se otorga la certificación, se prohíbe que las empresas tergiversen sobre su participación, membresía o certificación en cualquier programa de privacidad o seguridad patrocinado por un gobierno o una organización de autorregulación o establecimiento de estándares.



Tomado de: Presentación del Doctor Michael Panzera – Federal Trade Commission

Así mismo, explicó que tienen la posibilidad de emitir cartas de advertencia a las empresas por haber afirmado en sus políticas de privacidad que son participantes en el sistema CBPR, aunque no fueran participantes verificados. En 2019, la FTC envió cartas de advertencia a varias empresas, indicándoles que deben eliminar de sus sitios las políticas de privacidad o cualquier otro documento o declaración pública que pudiera interpretarse como una afirmación de participación o involucramiento en el sistema CBPR, a menos que se demuestro que tienen sometido a la necesaria revisión y certificación.

Por lo anterior, comentó que la FTC advirtió que iniciaría acciones legales correspondientes si las empresas no responden de una manera satisfactoria, y una posible sanción. Este sistema es un mecanismo voluntario, pero es sujeto a la protección de la ley, por lo tanto, siempre hay un agente que vigile, lo cual es muy importante para mantener la seguridad a los usuarios.

11. ¿Cuál es el valor para México para ser reconocidos como país en materia de protección de datos, como miembro de APEC?

Intervención de Jonathan Mendoza – Secretario General de Protección de Datos del INAI de México

El Doctor Mendoza comentó que para México es muy importante pertenecer a la APEC y también formar parte del TE-MEC, que tiene ciertos estándares, por lo tanto, al poder participar del SBPR, junto a las 7 economías se busca una convergencia, que es lo que se apuesta a México, por lo tanto, se debe buscar una alianza en toda Latinoamérica, ya que hoy recurrimos secundariamente a las cláusulas contractuales secundarias, que terminan siendo temas que están en documentos que no abona para el tema de la Accountability y a la responsabilidad, pero de igual forma se ve mucho desarrollo en la región, donde se ven leyes muy buenas, pero estas se deben implementar sino serán leyes muertas, se debe implementar la responsabilidad demostrada, finalmente los datos no son una barrera a la economía, todos los sistemas y sus actores se deben integrar para actuar.

12. ¿Cuáles son los beneficios del CBPR y del APEC?

Intervención de Sam Schofield – Policy Advisor del International Trade Administration del US. Department of Commerce

El Doctor Schofield comentó que respecto a las diferencias del CBPR y del GDPR, el GDPR es una regulación que muchos países han tomado, pero también hay similitudes un instituto en Washington DC, hizo un estudio y determino que hay un 66% de similitudes entre los dos sistemas, la gran diferencia es que el CBPR es un puente entre las regulaciones entre los sistemas del mundo.

De esta manera, aclaró que los Estados Unidos no está luchando contra el GDPR, solo creen que el modelo de CBPR tiene más beneficios a todos los stakeholders en la economía mundial y digital, por eso una gran parte de la visión del sistema CBPR es el reconocimiento que da a cada país para establecer sus propias leyes, pero se puede propiciar para que haya menos barreras entre países, por lo que hoy se mira la posibilidad de cambiar algunos requisitos para entrar en un foro global.

13. ¿Cuáles son las posibles consecuencias de alejarse del cumplimiento de un requisito dentro del sistema CBPR?

Intervención de Michael Panzera – Federal Trade Commission

El Doctor Panzera comentó que es un sistema de flexibilidad que no obliga a un país de aplicar la ley de manera homogénea, las sanciones que aplican en cada país, son las sanciones que se dan el sistema del CBPR, por lo tanto, se podrían

aplicar este tipo de sanciones dependiendo de cada país, por lo que cada país no tiene que elegir entre el sistema CBPR o su sistema, ya que el CBPR funciona como un puente, ya que si se trata de un caso de una empresa de un país y los usuarios en otro país se puede coordinar entre los dos países.

SÉPTIMO PANEL: NUEVAS TECNOLOGÍAS Y RETOS DEL ESTADO

Moderador:

23. **Juan Camilo Medina – Legal Manager de Beat Colombia**

Panelistas:

24. **Silvana Lara - Directora de Sector Público de Microsoft**
25. **Juan Pablo Salazar - Director legal y regulatorio de RIPIO**
26. **Paula Vargas - Director, Privacy Policy & Engagement LATAM en Meta**

Intervención de Juan Camilo Medina – Legal Manager de Beat Colombia

El Doctor Medina agradeció la invitación del Departamento de Derecho de las Telecomunicaciones, y explicó que el panel tiene dos propósitos, el primero sobre tecnologías disruptivas y como los derechos dentro de estas mismas tecnologías se debe garantizar por parte del estado, como en el metaverso se debe garantizar derechos fundamentales, toda la cantidad de datos que se recolectan y como el estado debe tener un rol importante dentro de las tecnologías para garantizar los derechos de los ciudadanos, o el caso de San Francisco, Estados Unidos para detectar delincuentes, tuvieron ciertos problemas como no identificar a verdaderos infractores, por lo que se debe mirar cómo conciliar esto.

14. **¿Cómo pueden ser las empresas de tecnología ser aliadas del estado en su propósito de ser eficientes y a la vez garantizar los derechos fundamentales de los ciudadanos?**

Intervención de Juan Pablo Salazar - Director legal y regulatorio de RIPIO

El Doctor Salazar agradeció por la invitación y manifestó que cada vez más el estado físico y virtual se están imbricando en uno, y eso va a implicar el desenvolvimiento del yo digital, físico e hibrido, y cómo manejar esos datos transfronterizos, en Latinoamérica solo hay una jurisdicción amigable que es Argentina, por lo que se tiene que solucionar para buscar una transferencia fácil de los datos, se tiene que mirar como puede ser clara y rápida, teniendo en cuenta el diálogo estado y empresa.

Intervención de Paula Vargas - Director, Privacy Policy & Engagement LATAM en Meta

La Doctora Vargas agradeció a los presentes, y propuso el tema de cómo se pueden usar los datos privados para el bien común, ya que cuando los datos se comparten responsablemente pueden salvar vidas, se tiene un proyecto donde la información donde puede llenar vacíos críticos en crisis humanitarias pueden ayudar a la destinación de recursos, para guiar la ayuda humanitaria en ciertos estados, y en la pandemia fue muy importante como con la información se puede generar herramientas para el uso de los recursos.

De esta manera, comentó que se puede usar la herramienta de Facebook Meta, con su capacidad computacional, machine learning, con mapas, encuestas y demás que permiten guiar políticas públicas, con el mapa de movimiento se puede usar la privacidad diferenciada, y que puede generar un índice de riqueza para mirar donde se puede dirigir los recursos, por lo tanto, hay casos claros donde los datos pueden aportar a generar políticas públicas.

15. ¿Qué retos tiene el estado para garantizar los derechos de los usuarios por vulneraciones en el extranjero?

Intervención de Juan Pablo Salazar - Director legal y regulatorio de RIPIO

El Doctor Salazar comentó que en el caso de vulneración de datos por parte de una empresa extranjera el usuario siempre es el que pierde, por la complejidad donde esté la empresa, aquí lo que se tiene que hacer es realizar cooperaciones entre estados, para lograr la protección.

Intervención de Silvana Lara - Directora de Sector Público de Microsoft

La Doctora Lara comentó que la transformación que se está viviendo hoy fue muy acelerada en pandemia, pero no con esta misma velocidad se desarrolló una brecha de seguridad, se miran que los ramsomware actuales son antiguos, es decir, desde el 2007, por lo tanto, la seguridad se tiene que mirar como una estrategia de gestión de riesgo, y abordar la estrategia para evitar que los incidentes ocurran, y así perfilar cada usuario y los administradores, de tal manera que tenga las restricciones correspondientes, y mirar cuando se puede acceder a la información.

Por lo anterior, comentó la importancia de la prevención, ya que ya estamos en un momento de desarrollo con un gran impacto, por lo tanto, el estado debe tener un papel para ayudar con ese desarrollo.

Intervención de Juan Pablo Salazar - Director legal y regulatorio de RIPIO

El Doctor Salazar expresó que la transformación cultural y la transformación digital son muy importantes para la seguridad digital, ya que el usuario interno y externo puede generar un problema por un correo con virus o demás, por lo tanto, tenemos que generar una transformación.

Intervención de Paula Vargas - Director, Privacy Policy & Engagement LATAM en Meta

La Doctora Vargas, enfatizó en la necesidad de la necesidad de responsabilidad demostrada, y como la educación interna debe ser un punto importante dentro de la compañía, ya que todos son responsables de la información y que se requieren estos procesos internos. Además, comentó la importancia del flujo transfronterizo de datos para hacer un buen uso para maximizar los beneficios de la economía digital minimizando los riesgos.

Intervención de Silvana Lara - Directora de Sector Público de Microsoft

La Doctora Lara explicó la importancia del principio de interoperabilidad para la privacidad y de los parámetros de clasificación de la data, y a veces es diferente en cada organización el concepto de dato clasificado, por lo tanto, debe existir una directriz que muestre que información se puede compartir, y ser amplio como se aplican estas políticas sin vulnerar al usuario.

16. ¿Qué hacer con el acoso que se puede generar en el metaverso?

Intervención de Paula Vargas - Director, Privacy Policy & Engagement LATAM en Meta

La Doctora Vargas comentó sobre la importancia de la gobernabilidad del metaverso, en las conversaciones globales donde tiene que participar todos los actores, donde se debe mirar en el beneficio de la sociedad, y el fin de Meta es la transparencia de los datos, y entendiendo la privacidad dentro del producto mismo, y además mirando los diferentes tipos de datos para desarrollarlo en la práctica. Respecto, al acoso se tiene una herramienta que evita que ciertos avatares se acerquen en determinado espacio.

Intervención de Silvana Lara - Directora de Sector Público de Microsoft

La Doctora Lara explicó que la tecnología 3.0 y el Metaverso están hace mucho tiempo, que amplifican la experiencia del usuario, ya que cuando se amplifica

esto se debe amplificar la seguridad, los controles y la gestiones, y se tiene que lograr la aprobación tecnológica para aportar.

Intervención de Juan Pablo Salazar - Director legal y regulatorio de RIPIO

El Doctor Salazar comentó que el Metaverso implica acceder a servicios web 3.0 del internet con blockchain, y va a ver una evolución en los datos, y el primer escalón muestra que el usuario va a ser dueño de los datos, se habla de aplicaciones que van a permitir el uso de repositorio de esos datos, y permitirá el uso por parte de un tercero, y así poder un solo sistema de identificación y no tener tantas claves, pero tenemos que ver como se evoluciona, e invito a la investigación de esto.

17. ¿Qué estrategias están teniendo las empresas para que sea más amigable y mantener al estado informado, que sea más transparente?

Intervención de Silvana Lara - Directora de Sector Público de Microsoft

La Doctora Lara manifestó que es más un tema de educación al usuario, la capacitación debe ser continua y programática, debe ser un modelo permanente, y que la apropiación tecnológica sea de forma correcta, para identificar los modelos de control en temas de privacidad y temas de datos.

Intervención de Paula Vargas - Director, Privacy Policy & Engagement LATAM en Meta

La Doctora Vargas explicó que Meta tiene un procedimiento denominado Privacy Review donde lo que se hace es que en el desarrollo y en la creación de productos para entender cuáles son los riesgos y como se pueden mitigar antes de que se pueda aprobar el lanzamiento de un producto, se debe mirar los mecanismos internos del diseño. Meta hace poco cambió sus políticas de privacidad añadiendo herramientas de control dentro de la política misma y añadiendo transparencia, y un centro de privacidad que es la política educativa, que agrupa por temas explicaciones de cómo se hacen determinados procesos.

Intervención de Juan Pablo Salazar - Director legal y regulatorio de RIPIO

El Doctor Salazar manifestó que como abogados se debe empezar a saber a diseñar software, para que después la gente de producto no lo integre, para así facilitar la interpretación de lo que acepta cada usuario, y el doble factor de aceptación, para que el uso de los datos se realice desde la aceptación.

CONCLUSIONES

Intervención de Silvana Lara - Directora de Sector Público de Microsoft

La Doctora Lara comentó la importancia de mantener la seguridad como uno de los pilares organizacionales y de las decisiones de la empresa, e invita a elevar estas conversaciones de gestión del riesgo, y acordarse de que pueden existir todas las políticas de privacidad, pero el gran accountable de la privacidad y de la seguridad somos cada uno de nosotros, para no darnos una sorpresa, seamos consecuencias y diligentes en la información que compartimos, para mejorar la experiencia de cada individuo.

Intervención de Paula Vargas - Director, Privacy Policy & Engagement LATAM en Meta

La Doctora Vargas comentó que se debe enfatizar en el uso de los datos que cada usuario le autoriza a la empresa, de eso depende la sustentabilidad de los servicios, para Meta la privacidad es lo central en lo que hacen, por lo que invita a las personas a los links donde se puede gestionar la información, revisar las últimas opciones de privacidad y revisar si las opciones siguen siendo válidas.

Intervención de Juan Pablo Salazar - Director legal y regulatorio de RIPIO

El Doctor Salazar comentó que sobre tecnologías emergentes no están construidas todas las reglas, no hay legislación sobre inteligencia artificial en detalle, por lo que se debe aplicar los principios de todas las normas y guiarlos a la aplicación del uso tecnológico y no esperar a la normativa que llegue en 5 años.