



6to Foro de Gobernanza de Internet Colombia 06 y 07 de Noviembre del 2019

La Mesa Colombiana de Gobernanza de Internet agradece a los estudiantes voluntarios de la Universidad Externado de Colombia quienes realizaron la relatoría del evento.

Relatoría

Día 01:

Miércoles 06 de Noviembre del 2019

8:30 a.m a 9:00 a.m

Presentación del taller a cargo de la Universidad Externado de Colombia.

Ponentes:

- *Dra. Teresa Vargas. Directora del Departamento de Derecho Informático de la Universidad Externado de Colombia.*

Relatoría: **Daniel Peña**

La apertura estuvo a cargo de la doctora Teresa Vargas, Directora del Departamento de Derecho Informático de la Universidad Externado de Colombia quien manifestó un verdadero placer por el dar la bienvenida al Foro Colombiano de Gobernanza de Internet 2019, entendido como una oportunidad para que múltiples partes interesadas se reúnan en torno a la construcción de un internet más seguro, abierto y transparente.

La doctora Teresa, señaló que la Universidad Externado de Colombia acoge el Foro con gran cariño y celebra el desarrollo que ha tenido la Gobernanza de Internet a nivel local en los últimos años; lo anterior, aclaró, está plenamente demostrado por los espacios, focos de discusión, talleres y debates dispuestos, dado que son muestra de un trabajo que ha venido desarrollando la Mesa Colombiana de Gobernanza de Internet y la importancia de contar con múltiples actores que aporten a la discusión.

Posteriormente, señaló que la Universidad Externado de Colombia siempre ha sido consciente de la importancia que tiene para la educación, la apropiación de las tecnologías de información y comunicaciones y por ello ha dispuesto comprometerse por completo con el ecosistema de internet, de allí la acogida de este evento como muestra del valor que le da la universidad al conocimiento abierto y la diversidad.

La doctora Teresa Vargas manifestó que se ha hecho un gran esfuerzo entre los Departamentos de Derecho Informático, Departamento de Derecho de los Negocios, Departamento de Derecho de las Telecomunicaciones, El Observatorio de Sociedad, Gobierno y Nuevas Tecnologías y el Observatorio de Nuevas Tecnologías y Derecho Privado para acercar a la comunidad académica a la apropiación digital y el conocimiento responsable; de esta forma, señaló, se hace un énfasis en el compromiso por la educación y la formación de los futuros líderes en la gobernanza de internet.



Sobre lo anteriormente señalado, concluyó la importancia de inculcar el trabajo en equipo a las próximas generaciones porque no se puede ser egoísta con el conocimiento y menos en estos temas de actualidad, por conducto del diálogo constructivo, considero, es como se alcanza una sociedad inteligente y propositiva.

Así mismo, adjudicó a la universidad como pilar fundamental del propósito anteriormente descrito dado que es allí donde los jóvenes descubren su interés por estos temas y adquieren los conocimientos necesarios para afrontar los retos en el entorno digital.

Consecuentemente, la doctora Teresa, manifiesta aprecio por la tradición del foro local de involucrar a la academia y a los jóvenes, dado que así es como se construye los primeros pasos para que se pueda aplicar los resultados a las oportunidades y compromisos de la gobernanza de internet que también se dan a nivel regional y global.

Finalmente, invitó a todos los asistentes a disfrutar de: i) las bellas instalaciones que ofrece la Universidad Externado de Colombia, ii) la exposición sobre la desintoxicación digital, iii) los talleres dispuestos en el foro, iv) la posibilidad de hacer todas las preguntas que se les ocurran, v) la posibilidad de aprovechar para hacer *networking*, vi) los temas de cómo funciona el internet y todos los aspectos fascinantes que se encuentran relacionados.

9:00 a.m a 9:15 a.m

Introducción y presentación de la Mesa Colombiana de Gobernanza de Internet y dinámica de los talleres.

Ponente:

- **Pilar Saenz. Fundación Karisma**

Relatoría: Daniel Peña

La introducción estuvo a cargo de Pilar Saenz de la Fundación Karisma; quien agradeció a la Universidad Externado de Colombia, porque sin un lugar donde poderse reunir no es posible realizar el Foro.

Explicó que la Mesa Colombiana de Gobernanza de Internet es un espacio de múltiples partes interesadas, lo cual significa que están involucradas tanto la academia, comunidad técnica, gobierno, sociedad civil y empresas que son importantísimas en este sector; la idea es que entre todos y todas se den discusiones alrededor de cómo queremos que sea y funcione internet en el país.

Así mismo, aseguró que el Foro de Gobernanza de Internet no es un invento Colombiano, es un invento que viene desde hace mucho, desde las primeras reuniones que se hicieron sobre la *sociedad de la información* en Túnez en el año 2003 y desde ese momento se propuso el modelo de múltiples partes interesadas para abordar los problemas de internet, dado que internet no le pertenece ni a uno de los gobiernos, ni a una de las empresas, sino que es algo que pertenece a todos incluyendo la sociedad civil, academia y todos y todas pueden aportar.





Posteriormente, expuso que la historia local sobre la gobernanza de internet comienza en el año 2012 cuando .CO Internet y Colnodo con el aval del MINTIC decide realizar en el país la reunión preparatoria latinoamericana del Foro de Gobernanza de Internet y se hizo una convocatoria de personas interesadas de todo el país; a partir de ese primer encuentro con los latinoamericanos se dieron cuenta que hacía falta tener un espacio local para hacer estas discusiones, entonces desde 2012 arrancaron con mirarse a los ojos y decir: “queremos hacer algo” y en el 2013 fue que arranco propiamente la Mesa Colombiana de Gobernanza de Internet y empezó porque decidieron varios de los que habían asistido a otros eventos sobre gobernanza, a hacer el evento local, no solamente el foro sino también un espacio de discusión.

La Mesa Colombiana de Gobernanza de Internet se reúne itinerantemente cada dos meses, la sede la van cambiando dependiendo de las posibilidades de quienes asisten y han tenido 39 reuniones, un montón de reuniones, discutiendo muchas cosas, proyectos de ley, iniciativas y para organizar este foro.

Se preguntó: ¿por qué hacen un foro anualmente? porque creen que no basta solamente esta discusión que suele ser muy pequeña en la mesa, también quieren que los temas sean conocidos por muchas más personas; entonces este foro es su espacio público para hablar sobre temas de gobernanza de cara a toda la ciudadanía, por eso todos y todas están invitados, por esa razón siempre tienen *streaming*, por eso celebra que haya traducción en lenguaje de señas, porque estos medios les permite comunicarse con otros y que hagan parte de la discusión.

Aclaró que el foro se organiza por las múltiples partes interesadas y por eso pueden ver en la parte de abajo muchos logos, de gente involucrada, algunos ponen dinero porque se necesita el dinero, algunos ponen tiempo, otros ponen trabajo y otros ayudan a que tengan una agenda variada a lo largo de los dos días de foro; anteriormente el primer día se dedicó a una especie de taller largo sobre temas de gobernanza de internet, este año decidieron cambiar la dinámica del primer día y por eso lo que van a tener es una serie de talleres, los cuales se van a repetir dos veces y van a estar distribuidos en varios salones de la universidad, a saber: LINK: <https://governanzadeinternet.co/evento2019/>

Finalmente, agradeció la asistencia de los presentes e invita a propagar y difundir el vínculo de *streaming*, aunque reconoce que puede resultar difícil estar viendo en una pantalla actividades de otros que hacen desde lejos y por eso también decidieron dar becas a personas que vienen de otras regiones para que puedan asistir al evento; esta es la tercera vez que dan becas.

Extendió una cordial bienvenida a los becarios y asistentes reconociendo que esta será siempre su casa e invita a que compartan la información a sus contactos.



Taller: Cómo Funciona Internet

Karisma – ISOC Colombia

Ponente:

- **Pilar Sáenz. Fundación Karisma**

Relatoría: Catalina Riveros Manrique

El taller inició con una reflexión: las personas dan internet por hecho o por ausencia, pero pocas veces se preguntan qué se necesita para que el internet funcione.

Para iniciar, la expositora presentó un ejercicio didáctico para ser realizado tanto por los asistentes presenciales, como por los virtuales. A los primeros los dividió en tres grupos y les entregó unas imágenes laminadas. A los segundos, les presentó un link, a través del cual tendrían acceso a las mismas imágenes digitales. Acto seguido, presentó la siguiente situación:

(A) se encuentra en la oficina de Karisma ubicada en Bogotá y, por medio del computador que está conectado a la red de ETB, le envió un correo electrónico de su cuenta en Yahoo a (B). (B), se encuentra en el campus de la Universidad Externado de Colombia y recibió el correo en su cuenta de Gmail, a través de su smartphone que está conectado a la red de Claro.

A continuación indicó que las imágenes debían ser organizadas de forma tal que el mensaje del computador de (A) llegue efectivamente al celular de (B).

Los grupos y los asistentes virtuales trabajaron por quince minutos y luego, uno de aquellos, presentó sus resultados y la expositora los socializó con la audiencia, así:

Imagen 1. Computador portátil.

Imagen 2. Cable UTP. Explicó que en la actualidad, estos son innecesarios, pues las conexiones se realizan vía wifi.

Imagen 3. Router ETB

Imagen 4. Cable de fibra óptica

Imagen 5. Centro de datos de ETB. Refirió que este es el lugar en donde las compañías tienen almacenada altas cantidades de información. Por ejemplo, la denominada “nube” es realmente un centro de datos: un grupo de computadores con información almacenada.

Imagen 6. Cable de fibra óptica.

Imagen 7. Cable submarino

Imagen 8. Centro de datos de Yahoo. Preciso que en este lugar se almacenan los correos electrónicos durante el tiempo que el usuario esté activo.

Imagen 9. Centro de datos de Gmail. Identificó que acá había un error, dado que entre un centro de datos de Yahoo y el de Gmail debía haber un cable submarino, pues Google no tiene un solo servidor, sino varios y en distintos lugares.



Imagen 10. Cable de fibra óptica.

Imagen 11. Centro de datos de Claro. Explicó que, de acuerdo con las normas colombianas, las empresas de esta índole deben almacenar la información de sus usuarios -llamadas, mensajes de texto, ubicación, etc.- por cinco años.

Imagen 12. Antena de telefonía celular.

Imagen 13. Celular.

Al finalizar el ejercicio, la experta hizo tres reflexiones. La primera, que todo este proceso implica grandes cantidades de cables; la segunda, que hay muchas empresas con intereses económicos que participan en este proceso y, la tercera, que existen muchas zonas vulnerables para la información que se transmite por esta cadena.

El enfoque de la siguiente parte de la exposición giró en torno a la última reflexión y, para poner en evidencia la vulnerabilidad de la información que navega a través del proceso, presentó unas imágenes que representan las formas como se transmite la información por internet: en paquetes transparentes -acetato visible- o en paquetes cerrados -sobre de manila cerrado-, y explicó lo siguiente.

Como quiera que el internet nació en buenos términos, en un primer momento la información viajaba en paquetes transparentes: con los datos del emisor, receptor y del contenido visibles. Sin embargo, esta información era fácil de interceptar y, por tal motivo, se crearon herramientas para cifrar el contenido del paquete transparente, de extremo a extremo; es decir, hacer ilegible la información frente a terceros.

Adicionalmente, se implementaron en internet protocolos de navegación segura y anónima, para enviar y recibir información en paquetes cerrados, esto es, por medio de mecanismos a través de los cuales no son visibles los datos de emisor, receptor y del contenido.

Un ejemplo, es la información que viaja a través de un software VPN (siglas en inglés para Virtual Private Network, que traduce: red privada virtual), el que encripta toda la información de extremo a extremo y, así, la empresa que le presta el servicio de internet a una persona, solo puede saber que esa persona envió un mensaje por medio de una VPN, pero desconoce lo que hay dentro de ese paquete. Claro, la recomendación en seguridad digital es tener la garantía de que se trata de una VPN confiable.

Otro ejemplo son los nodos de TOR (siglas en inglés para The Onion Router, que traduce: el enrutador de la cebolla), a través del cual la información viaja detrás de capas o nodos. La primera es visible por la compañía prestadora del servicio de internet y contiene los datos de emisor y receptor. La segunda ya no contiene esos datos y despliega la información y de esa forma van cambiando los nodos sucesivamente, hasta llegar al punto final.

Para presentar un ejemplo cercano de esos mecanismos, expuso cómo Whatsapp utiliza un método seguro de información cifrada de extremo a extremo: cuando el mensaje sale del dispositivo del emisor y aún no ha sido recibido ni abierto por el receptor, la compañía tiene en su poder un paquete cerrado con información cifrada



que es inaccesible por terceros, incluida la misma compañía, a la que solo puede acceder el receptor.

En definitiva, concluyó que internet es un espacio para el ejercicio del derecho fundamental de las personas a expresarse libre y anónimamente; sin embargo, es menester tener claro que ninguno de los mecanismos de navegación anónima es perfecto, que existen riesgos y que, como en la realidad, es necesario preverlos y prevenirlos. En internet la seguridad es subjetiva: cada elemento es susceptible a ser vulnerado. En internet no hay nada cien por ciento seguro.

6. Sesión de preguntas y respuestas:

Las preguntas fueron presentadas a lo largo de la sesión y la preocupación central de la audiencia giró en torno a la seguridad de la información. Así:

-Pregunta: ¿qué información guarda el centro de datos de ETB?

Respuesta: los correos electrónicos de los usuarios de las cuentas locales de ETB y la información de los datos de las conexiones.

-Pregunta: ¿durante cuánto tiempo almacena la información una compañía como la ETB?

Respuesta: La ley les impone a las compañías colombianas almacenar la información por cinco años. Claro, como hay tanta información, ahí hay un tema de custodia y de migración de la información a otros centros.

-Pregunta: ¿Centro de información de la ETB maneja todos los datos de mis conexiones? ¿incluso en navegaciones privadas?

Respuesta: Si. Cuando se pone el navegador en forma anónima, el proveedor, en este caso la ETB, sabe en dónde se está navegando, pero no quedan más registros. Una cosa es la forma de navegación incógnita, en la que el proveedor va a ver los datos y otra cosa es la navegación anónima, en la que se intenta no dejar rastros de su presencia en internet.

-Pregunta: ¿por qué se necesita que la información pase por un cable submarino?

Respuesta: Porque no existe un data center de Yahoo en Colombia. Entonces, como la infraestructura no está en este territorio, debe viajar a otro país y llegar hasta donde están los servidores de la empresa. Hay compañías como Google que dona servidores especializados y que funcionan de manera local; sin embargo, por lo general las grandes compañías son extranjeras y ello implica riesgos. Por ejemplo, en Estados Unidos la información de extranjeros no tiene ninguna protección.

-Pregunta: ¿si alguien intercepta el router de mi oficina, qué información encuentra?

Respuesta: Puede tener acceso a toda la información que entra y sale de la oficina. De acuerdo con la ley de inteligencia y contrainteligencia, todas las empresas que prestan servicios de internet en Colombia deben permitir el acceso a información para las investigaciones. Los investigadores habitualmente requieren la información de manera



inmediata, así que se permite su captura y después se lleva esa información ante un juez de control de garantías. Se esperaría que la autorización fuera antes de la captura de la información, pero en Colombia es después.

Google empezó a emitir informes de transparencia de acceso a la información, cada seis meses, a través de los cuales rinden cuentas de qué países les han hecho peticiones de información de sus usuarios, informe de transparencia de Google cada seis meses.

Taller: Mecanismos de participación de Múltiples partes Interesadas – Stakeholder engagement
Ponente:
- Natalia Quevedo. Comisión de Regulación de Comunicaciones - CRC
Relatoría: *Daniel Ríos*

El taller es presentado por la ingeniera de la Comisión de regulación de Telecomunicaciones quien comienza preguntando a los asistentes: ¿Quién define el futuro de la Internet?

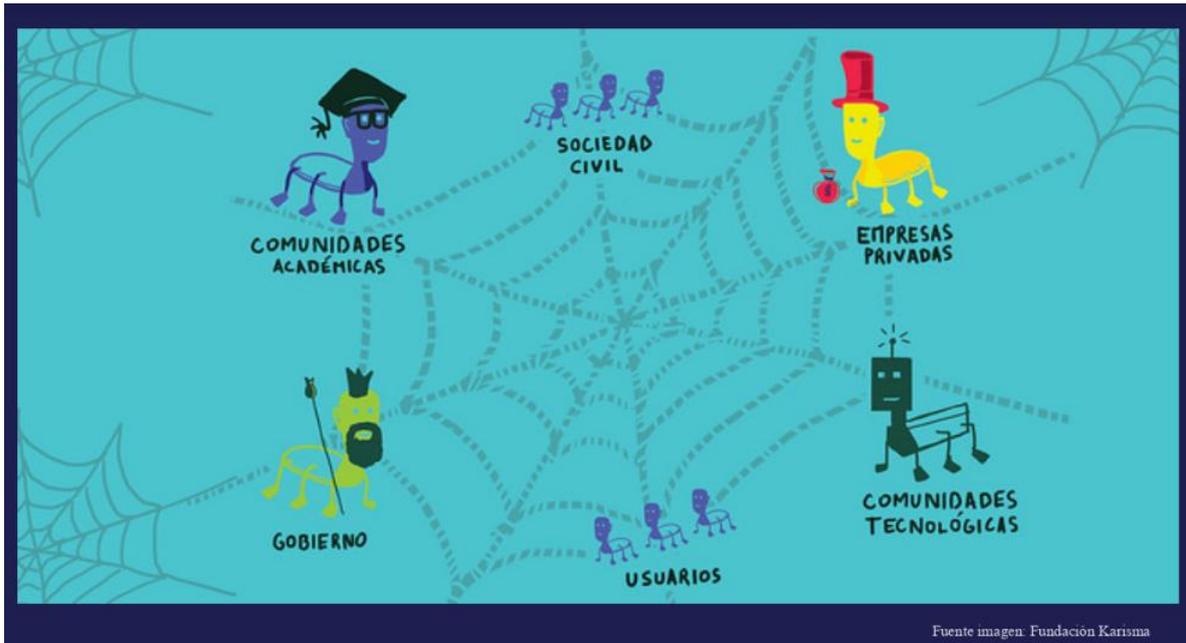
Un asistente responde: El usuario final, a medida que realizan el consumo de servicios de internet van exigiendo y pidiendo más cosas.

Otro asistente responde: Las empresas, organizaciones poderosas que establecen agendas, información y necesidades del usuario, porque es la gran debilidad o fortaleza del poder.

La ingeniera se pregunta posteriormente: ¿Quién toma las decisiones en Internet?

Un tercer asistente responde: románticamente estaría de acuerdo con que deberían ser los usuarios pero en la práctica real quien toma las decisiones es el ICANN que es la entidad a nivel internacional que administrar dominios, define parámetros técnicos y ostenta total incidencia del manejo de la internet.

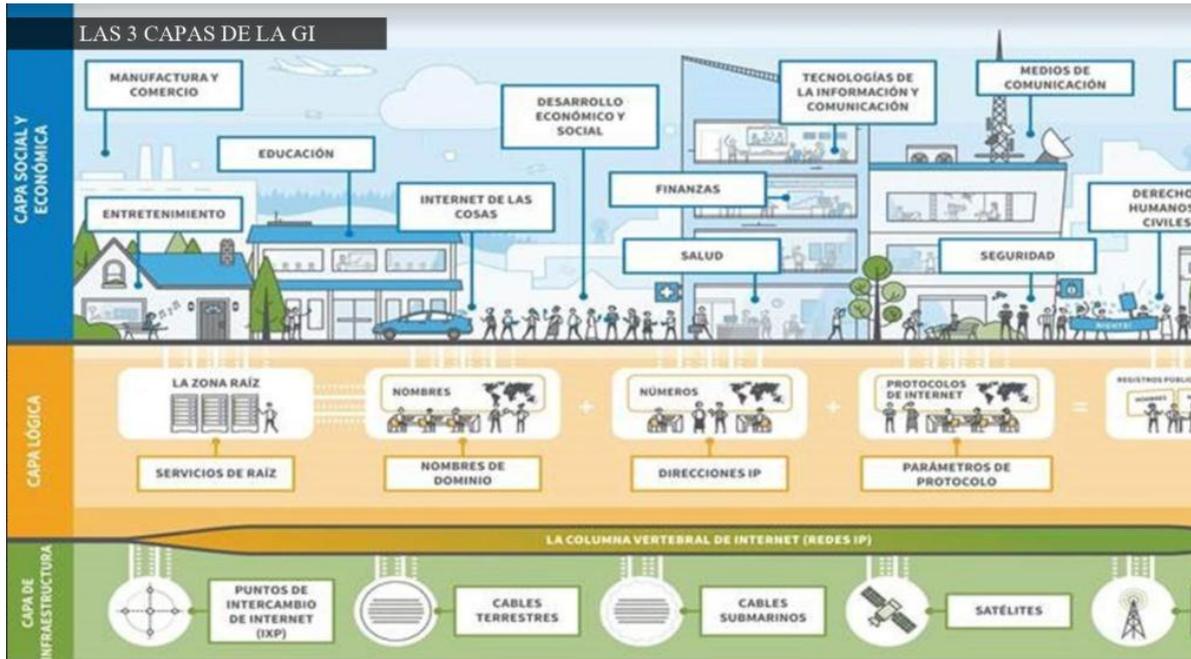
La ingeniera aclara que estas preguntas se irán abordando en el taller desde la perspectiva de la posición de la parte interesada que representa: *el gobierno*. Parte de la base que existe una diferencia entre los conceptos: gobierno y gobernanza, a saber: el primero se refiere a una estructura vertical, donde un único actor que es el Estado toma las decisiones; el segundo se refiere a una estructura horizontal y transversal, cuya participación es de múltiples actores interesados en la búsqueda de un consenso. Según la ingeniera, en la gobernanza no se toma una decisión unilateralmente por un sector, todos conversan en búsqueda de un consenso y los procesos van de abajo hacia arriba.



Un asistente increpa la anterior posición aludiendo que es una visión romántica de la gobernanza, dado que existe claras críticas a la misma, existiendo también conceptos como metagobernanza y hace referencia a que esos procesos no son tan horizontales como se cree, porque es muy distinto la posición del dueño de una empresa versus la posición de un simple usuario, no tienen en la práctica la misma relevancia, entonces hay varios niveles de influencia, entonces la gobernanza no es horizontal; por lo anterior el asistente se pregunta: ¿Cómo se puede manejar toda esa telaraña que la ingeniera muestra -en la diapositiva- porque realmente no sabe cuál es el actor que pueda defender los intereses generales o colectivos en la internet, el punto del asistente es que realmente no hay esa horizontalidad, esa idea es falsa, dado que hay desniveles y el reto es saber cómo la agenda puede establecer los intereses colectivos dentro de la internet.

Ante la anterior intervención la ingeniera responde: para eso estamos acá, justo el modelo que representamos en la Mesa Colombiana de Gobernanza de Internet es un modelo de múltiples partes interesadas donde ningún actor tiene más peso que el otro y la agenda se define por toda esta pluralidad de actores que hacen parte.

Entonces, asevera la ingeniera que la mejor definición de la gobernanza de internet viene de la conferencia mundial de la sociedad de la información del 2005 y se representa gráficamente de la siguiente manera:



Internet nace físicamente libre sin tipos de restricciones, desde el mecanismo físico comienza a permear otros tipos de niveles, sociales, culturales, políticos, etc; dado lo anterior, hay múltiples actores: está la comunidad técnica representada por ICANN el cual también es un organismo de múltiples partes interesadas, donde todos los actores hacen un consenso para la toma de decisiones En temas de buen manejo de la red está el gobierno está la sociedad civil los sectores de la sociedad civil y la comunidad académica, están las empresas no sólo las grandes empresas los desarrollos y los pequeños emprendedores también y también dentro de la comunidad técnica pueden estar actores relacionados con la investigación.

Entonces la forma de discusión, a nivel mundial este año se va a realizar el 25 de Noviembre en Berlín, también una discusión a nivel local en Bolivia que sucedió a principios de Agosto en este año y tenemos el foro local, en el que estamos reunidos, el cual se reúne cada año y se discuten todos los temas relacionados a la internet.

La gobernanza de internet se puede ver desde la perspectiva de ICANN en tres niveles: un nivel físico, un nivel lógico y un nivel de aplicación de cómo llega a la sociedad; en el nivel físico tenemos todos los medios de transmisión que hacen posible el acceso a internet; en el nivel lógico tenemos todo lo que se necesita para que internet como lo conocemos, la cual está en la nube, se pueda acceder y por ello tenemos a toda la comunidad técnica desarrollando esta labor, y por último cómo se ve reflejado esto en la sociedad en nuestra forma de cultura, en la política, como hacemos negocios, cómo nos entretenemos.

En 10 años todos estos organismos no son vinculantes pero sí son importantes, el Foro de gobernanza de internet es patrocinado y gestionado por las Naciones Unidas esto le da un gran apoyo pero no genera un carácter vinculante.



Entre las discusiones que se adelantan en este escenario se encuentran los dominios de internet, por ejemplo el debate suscitado con El dominio Amazon en el cual se preguntan si le pertenece al Amazonas o a la empresa multinacional Amazon; hasta el momento tenemos la mitad del mundo conectada aproximadamente pero para un verdadero desarrollo de la cuarta revolución industrial requerimos que todos hagan uso de internet desde su cultura y la apropiación que sea necesaria.

Otra discusión que se adelanta es que protocolo se requiere, qué requisitos se necesitan y cómo identificamos a los actores de internet. Actualmente existen las direcciones IP las cuales también merecen un debate y discusión para determinar qué es más fácil, que es más rápido y qué es mejor.

Así mismo se debate la privacidad y la seguridad, Ejemplo al salir de sus casas ustedes verifican cerrar la puerta y llevar consigo su cédula de ciudadanía. Entonces por qué no hacen lo mismo en materia digital debido a que en este seminario también se requiere una identificación y autenticación, en lo personal considera la ingeniera que la privacidad depende de cada persona y que la seguridad depende de todas las partes interesadas dado que es responsabilidad del gobierno, responsabilidad de la Industria, etcétera.

En materia de privacidad cada uno decida que presente, que publica, pero en materia de seguridad también es relevante el acompañamiento y la educación que puedan ofrecer otros actores interesados Como por ejemplo la Academia, es por publicar datos sensibles relacionados con sus familiares con niños menores de edad con datos como la dirección de la casa y otra información que pueda perjudicar a la persona, estos dilemas hacen parte de la cultura de la privacidad.

Así mismo está en discusión temas como la libertad de expresión, neutralidad de la red. Como por ejemplo lo que esté consultando nadie tiene por qué saberlo. Con la conectividad que hace referencia a las personas que aún no están conectadas al internet fomentando la posibilidad de que lo usen y se apropien de sus beneficios y lo tengan como herramienta de desarrollo personal.

Por último se trata el tema de la protección de los niños en la internet, de igual manera como el pasado 31 Octubre se protegió físicamente a los menores al momento de pedir dulces, así mismo se debe proteger a los menores en la red; hay personas que se hacen pasar por personas que no son con el fin de engañar a los niños.

Los temas que se tratarán en el Foro Global - IFG 2019 en Berlin, serán:



Así mismo, la ingeniera aclara que no solo a los asistentes al Foro les preocupa que no esté funcionando el modelo de múltiples partes interesadas, dado que no está logrando los objetivos propuestos, por lo que en Berlín también se discutirá este tema.

En el V Foro se tuvo esa discusión y por ello, una de las conclusiones era que la Mesa de Gobernanza necesita una fuente de financiación y también una mayor participación de actores y presentar en temas de legislación y empresas privadas pronunciamientos y demás; resaltó que es importante que todos participen dado que todas esas opiniones las necesita la Mesa de Gobernanza.

La ingeniera expone también que existe una gran preocupación por el tema de la inteligencia artificial dado que esta tecnología puede servir para muchas cosas pero hay problemas de seguridad y discriminación, dependiendo de cómo se configure los algoritmos, la idea es proponer un código de ética que enseñe a los algoritmos a no discriminar.

Teniendo en cuenta que los datos son el petróleo del siglo XXI, la idea es entender que algunos representan etnias o culturas que podrían ser discriminadas por los algoritmos, porque se le está enseñando a la IA todos estos parámetros que tenemos los humanos, entonces son temas que siguen en discusión.

Frente a los datos es necesario saber cómo se están manejando, dado que para ella es una mentira que la gente diga que se leyó los términos y condiciones, dado que esto está relacionado al tema de privacidad y protección de los datos, muchas veces cuando las personas no leen sus términos y condiciones están aceptando que sus datos sean monetizados para x o y cosa para acceder a una aplicación “gratuita”, pero no conocen el precio.

Posteriormente la ingeniera ofreció a todos los asistentes un test de identificación de roles dentro de las categorías de actores interesados a través de un puntaje, depende de los momentos y circunstancias presentes.



¿Quién crees que hace parte de la GI nacional?

La GI es un espacio abierto y transparente de participación de individuos, empresas y organizaciones con o sin ánimo de lucro

Mientras se desarrolla el taller la ingeniera comenta quienes pueden hacer parte de la Mesa Colombiana de Gobernanza de Internet se reúne cada dos meses en diferentes lugares y tiene una página de internet <https://governanzadeinternet.co/> a través de la cual se publica donde se realizan las reuniones.

También ella pregunta ¿quiénes deben participar?



¿Cuáles grupos crees que deben participar?

La GI es un espacio inclusivo en el cual se debe incluir la opinión y los puntos de vista de todos sin ningún peso especial por algún representante en particular. La opinión de todos es igualmente importante.



A lo cual un asistente responde que es importante tener en cuenta a las regiones y por eso valora el esfuerzo de la mesa por apoyar la presencia de personas de diferentes partes para que asistan al foro.

La ingeniera resalta que desde hace dos años se apoya a través de becas para la asistencia de personas que viene de otras regiones dado que el debate es a nivel nacional y los insumos regionales son muy importantes, dado que la cultura, la forma de abordar internet y los problemas sociales, de conectividad, acceso son muy diferentes y también por eso siempre hay la forma de conectividad remota de las reuniones.

En conclusión todos deben participar, llevar sus ideas en el stakeholder que se sientan identificados; también se pregunta ¿creen que hay ganancia por participar en la gobernanza de internet?

¿Se obtienen ganancias por la participación de espacios GI?

Los espacios de GI no tienen ninguna finalidad de lucro ni ningún interés comercial. Se valora que miembros del grupo de GI o entes externos apoyen financieramente las actividades de los espacios de GI sin que esto represente algún tipo de favorecimiento de sus puntos de vista.

A lo cual un asistente responde: que al interactuar diferentes actores el beneficio es mutuo. La ingeniera agregó que si se gana mucho en conocimiento y participación de personas que no han sido escuchadas dado que da apertura.

La ingeniera también recopila los temas tratados por la Mesa de Gobernanza de Internet desde 2012 han sido:



Wilches hizo una diferenciación muy clara entre actores organizados y sociedad civil y la importancia de esa diferencia se da en que se critica el modelo de múltiples partes interesadas en la cual no hay representación directa de la sociedad civil quién es la más afectada frente a esto temas, y específicamente se refirió a la Fundación Karisma quien los identificó como actores organizados pero no hacen parte de la sociedad civil: en ese orden de ideas pregunto ¿como legítima la Mesa Colombiana ese trabajo si no hay representación directa de la sociedad civil y teniendo en cuenta que internet es una gran herramienta que podría permitirlo de alguna manera?

La ingeniera responde que por eso se tiene esos espacios: la Comisión tiene muchos mecanismos de participación, el problema es que existen usuarios no informados que también tiene obligaciones de participación; alude que también está acompañando la mesa Colnodo, Red Papaz, dando puntos de vista de la sociedad civil en algunas temáticas. Reconoce que hace falta bastante para que los actores organizados, los no organizados y usuarios reconozcan su papel y comiencen a actuar.

¿Cómo le llegamos a usuarios no informados? a través de foros, difusión y buscando que se pongan la camisa de la gobernanza para que participen.

Todos usamos internet, todos necesitamos internet, por eso hay que llevar a través del activismo, educación un proceso que permita vincularlos.

Un asistente opina que es iluso pensar que toda la ciudadanía participe dado que también hay actores que no les interesa, y por ello la ingeniera respondió que no es tan cierto dado que lo que expuso el Director de la CRC en el anterior foro es que existen múltiples partes de la sociedad civil que ni saben que son actores y también de la comunidad técnica, estos sectores no están plenamente identificados; si perteneces a la academia, has hecho estudios, si estas en el gobierno conoces la importancia y está obligada a presentarlo, pero respecto de la comunidad técnica ellos trabajan sin tener idea de este espacio.

En la Mesa se ha identificado la necesidad de crear puentes con la sociedad civil dado que el activismo podría tener mayor eco si usa las herramientas de internet y respecto de la comunidad técnica si se agremian les falta información porque muchas veces creen que es peligroso porque le pueden robar su información.

Si se ve la internet como un derecho también debe entenderse que implica deberes, por eso se debe informar, educar, activar al deber ser.

Un asistente que viene de Pasto Nariño confesó que gracias a que estudia en Bogotá, se enteró del evento por un grupo cerrado de whatsapp vinculado a su universidad, pero lleva trabajando 7 años en internet y no sabía nada de él y nunca había escuchado el tema de gobernanza, entonces es complejo como los canales y la forma de llegar a la gente.

Otro asistente opina que respecto de la diapositiva que muestra los actores participantes de la mesa, se evidencia una brecha de la participación con el gobierno, es decir, la política pública debería estar de la mano para fomentar el internet desde

las regiones; Se habla de internet pero no de la problemática a nivel nacional de acceso, uso y tenencia de las mismas tecnologías de la información y la comunicación, que solo se fomenta desde la perspectiva nacional pero no de lo regional, local.

Frente a esta opinión, se pronuncia el señor Julián Casasbuenas G. Director Colnodo. que invita a todos los participantes que se presenten con su nombre cuando se pronuncien, para que en el *streaming* también se pueda reconocer; el tema de la participación de gobierno fue, en el pasado, muy activa por la oficina internacional de gobierno que tuvo un rol bastante relevante en el foro latinoamericano, donde Colombia jugó un papel relevante; infortunadamente en el cambio de gobierno, las personas que estaban involucradas ya no están; de hecho en el primer foro regional celebrado en Colombia tuvo un apoyo relevante del MINTIC. Desde la mesa se hace un esfuerzo para que se continúe pero hay circunstancias que lo impiden.

La ingeniera agregó que hay que aprovechar el cambio de gobierno dado que todos los asistentes son potenciales líderes de la gobernanza de internet por el hecho de estar interesados y por ello tienen una voz, por ello se pueden acercar a sus autoridades locales para comentarles sobre ello para que se incluya dentro de las agendas de política pública y por eso es importante enseñar.

Consecuentemente, la ingeniera presento el *regulatory engagement*, en los siguientes términos:



REGULATORY ENGAGEMENT

- Principios proporcionados por la OCDE a los encargados de la formulación de políticas públicas como instrumento para diseñar mejor sus estrategias de participación con las múltiples partes interesadas.



Para el caso de regulación establece la OCDE:

PRINCIPIOS DE LA OCDE

- Incorporar en la discusión la experiencia, las perspectivas y las ideas para acciones alternativas de los interesados.
- Ayudar al regulador a balancear intereses opuestos.
- Identificación de efectos no deseados.
- Evaluación de costos y beneficios.
- Identificar y facilitar las interacciones entre las regulaciones de varios actores



Estos principios de la Gobernanza de internet los establece el ecosistema de Internet que existe hoy se basa en los principios fundamentales de la propia Internet y se fortalece con la participación de una amplia gama de actores que emplean procesos abiertos, transparentes y colaborativos. La cooperación y la colaboración siguen siendo esenciales para mantener la innovación y el crecimiento de Internet.

PRINCIPIOS DE LA GI

- Participación abierta, inclusiva y transparente.
- Toma de decisiones basada en el consenso.
- Supervisión y empoderamiento colectivos
- Enfoques pragmáticos y basados en la evidencia.
- Innovación.



Posiblemente esto es lo que se requiere por parte de los asistentes el buscar maneras innovadoras de traer más personas para aportar a la mesa, en los siguientes parámetros que debe tener en cuenta cualquier ente regulador en el concepto de regulación de quinta generación basado en los siguientes ocho principios, que va de la mano de los mecanismos de participación de las múltiples partes interesadas, a saber



En Colombia, la CRC tiene en cuenta los siguientes parámetros:

LA CRC

Regulador único con independencia administrativa, técnica, patrimonial, presupuestal y con personería jurídica.

Regula redes y servicios de telecomunicaciones; servicios postales, servicio público de televisión, servicio de radiodifusión sonora, Servicio Postal Universal.

Un asistente que se presenta como Ángel Tábara, representante de un canal comunitario de Tocancipá, quien ha estado en algunas mesas de trabajo de la CRC, reconoce que actualmente esta entidad está en un periodo de transición, en la diapositiva anterior se trae a colación unos mecanismos de participación para crear las regulaciones y desde el gobierno se propone atender a ofrecer el servicio a comunidades que por rentabilidad, las grandes empresas no tienen a atender, pero va en contravía con el tema de la regulación y contravía con el tema de políticas que quieren colaborar, como un ejemplo está el tema de músculo financiero para poder



participar activamente en prestar el servicio de internet, los canales comunitarios a nivel nacional han ido desapareciendo, son empresas ESAL, donde los recursos provienen de organizaciones de comunidades organizadas que han hecho un esfuerzo muy grande para salir adelante; por ende el intentar llevar internet a las comunidades requiere un músculo financiero que estas empresas no cuentan y más aún cuando vienen los temas de regulación, ellos han estado participando activamente en esas mesas de trabajo para tratar de que en el periodo de transición puedan estar favorecidos en algunas cosas.

La ingeniera responde con una pregunta ¿has estudiado el tema del Sandbox lanzado por la CRC recientemente? es una estrategia de sandbox de conectividad, y es que ustedes pasan un proyecto donde identifican los retos y barreras regulatorias para llevar conectividad a X comunidad, con las cuales se levantan las barreras regulatorias en un ambiente controlado. Esta estrategia está publicada en la página de la CRC, la pueden consultar y a partir del otro año pueden poner el proyecto en prueba. Por ejemplo, ese tema estuvo en discusión con Colnodo para la implementación de redes comunitarias, entonces el sandbox es una buena herramienta que puede ayudar en lo que concierne a la regulación. El objetivo es demostrar que la regulación son barreras.

Otro asistente se identificó como Andrea Cortina y expuso que hay otro tema en particular frente a las cargas regulatorias que se tiene que cumplir que puede generar costos o sobrecostos dado que tiene que dar a conocer a los usuarios sus derechos, pero como está dirigido a comunidades pequeñas, la pregunta es si este tema fue verificado dado que las comunidades son muy pequeñas y los recursos no son con ánimo de lucro sino la prestación de servicio y podría desaparecer la oferta; ¿tuvo en cuenta el ente regulador esta realidad?

La ingeniera responde que sí se tuvo en cuenta, ejemplo el tema de ISP que van a prestar los servicios de internet, esta transición la contemplo la nueva ley que dio una excepción en contraprestaciones de 5 años; se puede pasar a tener un registro TIC pero se debe tener en cuenta que no es el tema que se está discutiendo ahora.

En una réplica a la respuesta la asistente presentó un ejemplo de una empresa que puede tener un músculo financiero pero no prestan adecuadamente el servicio en regiones remotas, en materia de gobernanza es importante que el usuario pueda tener representación porque hay muchas quejas por la misma razón, por lo cual se afecta la comunidad por no poder prestarse el servicio de internet y parece interesante que se quiera llegar a una conectividad total pero en el lugar remoto en condiciones paupérrimas, no se está aceptando al ciudadano para que esté presente en materia de regulación.

La ingeniera responde que ese tema se ha debatido con la Fundación Karisma donde el proyecto regulatorio los únicos representantes de la sociedad civil son Karisma y Colnodo. Ella confesó que ha estado visitando las regiones a través de la ruta del consumidor y está al tanto de primera mano de las problemáticas. Al usuario se le pide que participe pero el usuario es muy emocional con sus servicios, especialmente el de comunicaciones y se le cortó el servicio hoy pero cuando sale el tema regulatorio no le

interesa. por eso la importancia de estos escenarios donde hay puentes de comunicación.

Reconoció que hace falta más, ejemplo asociaciones de redes de usuarios de comunicaciones y estos son los escenarios y expuso las tareas y competencias del ente regulador a saber:



Así mismo, presentó el siguiente enfoque de mejora regulatoria que tiene en cuenta la CRC:



los mecanismos de participación que se pueden englobar gráficamente de la siguiente manera:

MECANISMOS DE PARTICIPACIÓN

Proyectos

Proyectos en curso | documentos en consulta pública:

- Sandbox Regulatorio para la innovación en conectividad
- Digitalización de Regimen de prestación a usuarios
- Caracterización de requerimientos de administraciones públicas de otros sectores
- Revisión Integral del Régimen de Administración de Recursos de Identificación
- Revisión del Régimen de Registro de Información Remédica
- Modernización de redes móviles en Colombia
- Revisión del Régimen de Calidad para el Servicio de Telefonía Móvil

Proyectos finalizados
Página Proyectos Finalizados



Todos los proyectos regulatorios en el plan de acción 2020 - 2021 se propone todo para que se pueda comentar, se hacen mesas de trabajo a actores, se transmiten en redes sociales y se requiere eco para que haya difusión.

El zero rating es a nivel mundial son las ofertas que dan todos los operadores de servicio móvil, ya sea virtual u operador de red, para que los usuarios accedan a algunas aplicaciones sin tener que gastar de su plan de datos.

Por lo anterior hay que diferenciar el internet que se ofrece a domicilios fijos, el cual se paga por una velocidad de acceso sin tener en cuenta la cantidad de datos gastados pero también hay un plan de datos que se ofrece en servicios móviles los cuales están determinados por una cantidad específica de capacidad.

DEFINICIÓN

- El Zero Rating (ZR), también llamado Tasa Cero, es una práctica de los operadores de datos móviles, operadores móviles virtuales y proveedores de acceso a Internet, en planes de datos limitados o con topes de consumo, en la cual no cobran a sus clientes finales por el volumen de datos usado por aplicaciones específicas.
- Los esquemas ZR abarcan acuerdos comerciales, y decisiones unilaterales del operador de la red, en los cuales cierto tráfico se exceptúa de un sistema de tarificación basado en el uso.



Existen cuatro tipos de cero rating a saber:

CUATRO FORMAS DE ZERO RATING

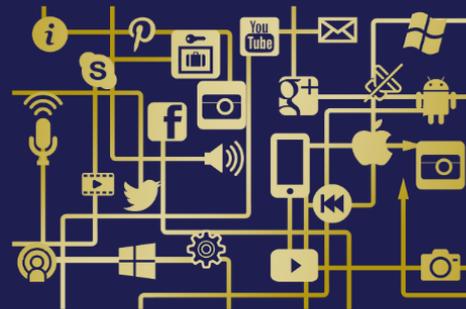
- 1. Un proveedor de acceso a Internet (ISP) puede pedir a los proveedores de aplicaciones que paguen por pertenecer a un esquema ZR.
- 2. Cuando se hace ZR a algunas aplicaciones y a otras no.
- 3. Un ISP puede incluir en un esquema ZR todas las aplicaciones dentro de una categoría de aplicaciones similares.
- 4. Un ISP que permite acceder a un conjunto de aplicaciones seleccionadas que pertenecen a diferentes categorías de aplicaciones sin que los proveedores de aplicaciones paguen por pertenecer al esquema ZR.



Por último, la importancia de este tema está relacionada con el principio de la neutralidad de la red, y por ello es un tema actual de discusión en este espacio dado que no se sabe si hay violación o no al principio.

NEUTRALIDAD DE RED

- Principios de la libre elección, la no discriminación, la transparencia y el deber de información.
- Ámbito de aplicación: a aquellos proveedores de redes y servicios de telecomunicaciones que prestan el servicio de acceso a Internet y a otros proveedores o usuarios que hagan uso de dicho acceso.
- Establecimiento de niveles de calidad de servicio relativos al acceso a Internet.
- Seguridad de redes y condiciones de bloqueo de contenidos.
- No es permitido bloquear, interferir, discriminar, ni restringir el derecho del usuario para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio lícito a través de Internet, sin el consentimiento expreso del



Resolución 3502 del 16 de diciembre de 2011



Taller: Seguridad Digital – Amenazas niñ@s adolescentes a cargo de RedPaPaz
RedPaPaz

Ponentes:

- Viviana Quintero

Relatoría: Juan Sebastián Alarcón Castillo

Que los usuarios de internet sean menores de 18 años obliga necesariamente a que cuando hablamos de gobernanza pensemos en como logramos que los entornos digitales sean entornos seguros para los niños y niñas. Ellos están accediendo cada vez más temprano a dispositivos digitales. Hoy en día según estudios desde los 13 meses de edad y esto genera unas interferencias a nivel del desarrollo cerebral, es decir, se va a desarrollar el niño o niña de una manera más lenta que cuando interactúa con el mundo real.

Este acceso temprano hace que esta proporción de usuarios que tenemos pueda ir en aumento en los próximos años, por ende, nos obliga a empezar a pensar en este tema de gobernanza.

También ocurre con los niños es que el uso que hacen de dispositivos es cada vez más privado y menos supervisado y esto está dado básicamente por “las pantallas” que nosotros tenemos en nuestro contexto digital actual las cuales son pantallas individuales, son pantallas personales, se pasó de tener un televisor gigante a tener muchas pantallitas pequeñas para que cada uno pudiese consumir el contenido que quisiera y esto hace que el contenido este menos supervisado por parte de los adultos y por ende se generen riesgos.

Debido a la incursión del internet en los hogares se ha aumentado el riesgo que ya existía, un ejemplo de ello es el tema de los retos por internet, que ya existían desde antes pero se viralizó su masificación con el acceso a internet. Se debe actuar entonces en ese poder que niños niñas y adolescentes pueden tener para enfrentar estos retos, conocerlos y tomar una perspectiva.

Otro cambio abismal de cara a la llegada del internet es el tema de la explotación sexual: por un lado empezó a naturalizar gustos que antes no eran, el gusto sexual de varias personas hacia niños y niñas no es algo que haya aparecido con internet, es algo que vino de tiempo atrás y que se mantenía muy en secreto, pero internet lo viralizó y generó el imaginario de que es algo normal que puede pasar.

Además de lo anterior, los niños y niñas que ya eran vulnerables, que vienen de contextos de pobreza o que han tenido antecedentes de salud mental, son niños que aumentan su nivel de vulnerabilidad, por ejemplo, los niños que han tenido antecedentes de conductas suicidas o antecedentes de ansiedad o depresión son niños que se enganchan más fácilmente con los retos de internet o a establecer contactos o conversaciones con desconocidos en línea.

Los factores de riesgo que se han detectado en el uso de internet respecto de niños, niñas y adolescentes son:



1. **El equipamiento temprano:** Cuando se entregan dispositivos digitales a niños y niñas que aún no cuentan con las habilidades necesarias para usarlas de forma segura se genera un riesgo.
2. **La falta de acompañamiento adulto:** Según estudios recientes cuando un niño hace un uso intensivo de pantallas, sus padres hacen casi el doble. El tiempo recomendado para que un niño entre los 0 y 12 años use un dispositivo es máximo una hora al día. Si tenemos un niño que usa 5 horas pantalla lo más probable es que sus papas usen 10 horas de pantalla y estos son niños a los que se les aumenta la posibilidad de estar solos, sin supervisión y por ende acceden a contenidos que no son aptos para ellos.
3. **Un bajo nivel de conexión con adultos de confianza:** Estos niños y estas papas que hacen un mal uso de internet no están conectados entre ellos y por ende son niños vulnerables sin una conexión de confianza con sus padres estando expuestos a por ejemplo, a hacer preguntas de sexo en internet, agredir a otros en internet, acceder a contenidos que podrían ponerlos en riesgo, etc. porque nadie les dijo que eso no se podía.

Adicionalmente UNICEF en el año 2017 apropia una categorización que fue creada por el reino unido en el año 2012 para reagrupar los riesgos digitales que enfrentan los niños y niñas en internet. Se categorizo los riesgos en tres grupos:

1. Contenidos.

- **Los relacionados con pornografía.** Pasa lo mismo que con la violencia, un niño que ve pornografía asume que es la manera normal de interactuar a nivel sexual y se reducen sus barreras naturales frente al abuso sexual. Muchas estrategias de abusadores en internet es presentarle pornografía a los niños para que ellos poco a poco vayan cediendo.
- **Los relacionados con el abuso sexual.**
- **Los relacionados con violencia y autolesión.** Un niño expuesto a violencia la empieza a ver como una forma normal o natural de interactuar y como consecuencia su forma de resolución de conflictos será una forma violenta. Con la autolesión se piensa que es un intento suicida, pero esto no necesariamente funciona así, hay casos en donde los niños hacen autolesión para liberar ansiedad.

2. Contactos.

- **El grooming.** que es cuando un adulto intenta acercarse a un niño con el fin de abusarlo o explotarlo. El grooming es la forma como se da la explotación sexual a nivel digital.
- **La sextorsión.** Es la extorsión a la que se somete una persona que ha reproducido alguna conducta de tipo sexual chantajeando a la otra persona indicando que si no quiere que ese contenido sea divulgado debe producir más contenido, pagar dinero o tener un encuentro sexual.
- **Los grupos cerrados en redes sociales o los perfiles privados.** Perfiles que los niños pueden seguir, pero los papas no pueden acompañar. En estos grupos en donde se empiezan a viralizar este tipo de contenidos.

3. Conductas.

- **El ciberacoso.** Es una agresión sistemática y repetida que se da a través de redes sociales. No es lo mismo la intimidación escolar a una



agresión donde tengo personas comentando, compartiendo, reaccionando al contenido y que puede sumar múltiples agresiones en un breve periodo de tiempo.

- **La ciber dependencia.** Se habla de adicción a los celulares, el internet, a los contenidos de redes sociales, etc.
- **El sexting.** Es tomarse fotos con contenido sexual y compartirlo con otras personas. Usualmente este sexting se hace en el marco de una relación sentimental o de amistad para posteriormente ser compartido en grupos o redes sociales.
- **La suplantación.** El acto de quitar a una persona su cargo o posición de manera fraudulenta. Un ejemplo de esto es cuando hay niños muy buenos en software y hackean el sistema de notas de su colegio.

SESIÓN DE RIESGOS

Ningún riesgo es adecuado para los niños. Entonces una de las cosas que deberíamos tener en mente es que papas y mamás son los primeros responsables, pero no son los únicos. ¿Qué es lo que los otros actores tienen que hacer para que esa labor de acompañamiento de los papas y mamás se pueda dar en circunstancias y de una forma efectiva? Se responde a esta pregunta con las siguientes ideas:

- Lo primero es aprender a analizar información, reconocer la información falsa de aquella que no lo es.** Nosotros podemos entrenar esta habilidad en los niños, pero el cerebro humano solo está preparado hacia los 13 o 14 años para poder desplegar esta habilidad de una manera adecuada. Es por esto que las redes sociales son para mayores de 13 años y esto se dice en todos los términos y condiciones.
- Lo otro es proteger su seguridad y privacidad,** nuevamente hablamos de la conciencia sobre los datos personales sobre lo privado y lo públicos viene a darse hacia los 13 años.
- Tratar bien a los demás.** Los niños necesitan saber cuándo una situación puede ser incomoda u ofensiva para otros en internet y además necesitan que los ayudemos a modelar situaciones.
- La habilidad para preguntar cuando algo los hace dudar.** Cuando nosotros generamos relaciones familiares que sobre todo tiene un corte muy autoritario los niños no preguntan porque les da miedo, se quedan callados, entonces estas relaciones deberían mirar a que “sin importar lo que hayas hecho, cuéntame siempre, puede que haya consecuencias negativas, puede que tengamos que reparar errores, pero si tú me cuentas yo te voy a ayudar” esto es lo que deberían saber los niños para que puedan confiar en adultos.
- Todo esto se da en un mejor contexto cuando no son los papas quienes están solos** cuando por ejemplo los papas cuentan con tíos, con primos, con otras personas de la familia que pueden acompañar a los niños en los contextos digitales.

TERMINOLOGÍA

Se sabe que el lenguaje es el que construye nuestra realidad. A veces nos referimos a estas situaciones de una forma incorrecta o de una forma que no es adecuada o no protege a niños niñas y adolescentes. Entonces primero los expositores comentan de



cuatro mensajes claves sobre el abuso y la explotación sexual de niños, niñas y adolescentes para luego seguir con terminología:

1. **Esto es un delito, no un negocio.** Por ninguna razón se puede justificar que sea permitido como un negocio porque las personas no son mercancías. Quienes ejercitan la explotación sexual no son empresarios, ni clientes, ni emprendedores, en realidad son proxenetas.
2. **Lo segundo es que nunca es culpa de la víctima,** como sociedad se culpa mucho a la persona menor de edad o a la niña y al niño o al joven y se dice “es que él se lo busco” o “es que para que se pone a salir de noche” o “para que tenía esa falda tan cortica en el colegio, tenía que dejársela más larga”. Una persona menor de 18 años no puede consentir su propia explotación, no puede consentir su propio abuso, entonces muy importante que las personas se lleven este mensaje, la responsabilidad de este delito siempre recae sobre quien lo comete, lo facilita y lo propicia.
3. **Las niñas, niños y adolescentes son sujetos de especial protección.** Todos estamos protegidos por unos derechos, pero ellos tienen derechos universales prevalentes e interdependientes.
4. **Este es un problema global.** Cuando hablamos de abuso y explotación sexual Colombia no es el único país trabajando en temas de protección a la niñez sino que hay toda una red global de organizaciones, de países, de personas de las sociedades civiles, de organismos internacionales, que buscan eliminar todo tipo de violencia contra los niños, niñas y adolescentes como el abuso y la explotación sexual en los entornos digitales.

Entonces, **¿Qué lenguaje es el que podemos usar y cuál es el más adecuado para referirnos a estas situaciones o problemáticas?**

A veces hablamos del pequeño del pequeñito, del menor, pero esta no es la mejor forma de referirnos. La forma preferente es el vocablo “niño, niña y adolescente” o “persona menor de 18 años” o “niñez”, pues cuando se usa otra palabra se está minimizando al niño, niña o adolescente.

En algunos medios de comunicación hemos visto que “las niñas estaban ejerciendo la prostitución infantil” entonces a las personas en el imaginario se les queda que eso se llama “ejercer la prostitución infantil” pero esa no es la forma más adecuada porque estamos dejando toda la responsabilidad en la víctima. Como ya se dijo una persona menor de 18 años no puede consentir su propia explotación, entonces usamos el término “explotación sexual y comercial de niños, niñas y adolescentes” o “niñas, niños y adolescentes explotados en la prostitución”.

Otro ejemplo es el del caso en Cartagena o en Santa Marta de “turismo sexual”, esa no es la terminología más adecuada, siempre prefieran usar “explotación sexual y comercial en niñas, niños y adolescentes en contextos de viajes y turismo”

Otro término muy común es el de “pornografía infantil” y esta no es la forma más adecuada pues la pornografía es de personas mayores de 18 años. La forma más correcta es “delito de pornografía con persona menor de 18 años” que es como está tipificado el delito en Colombia. Podemos usar también estas dos: “material de



explotación de niños, niñas y adolescentes” o “explotación sexual de niños, niñas y adolescentes en entornos digitales”.

Para terminar, a veces se usa la palabra “cliente”, “empresario”, “patrón”, esta no es la forma adecuada pues al usar estas palabras se está validando la transacción monetaria que hay en el proceso de explotación infantil.

Actualmente el mundo está trabajando en una terminología universal sobre estos temas, no solo en Colombia. A nivel mundial se está trabajando a través de las “guías de Luxemburgo” donde se hace una explicación a nivel mundial de todos estos términos y de unos términos que incluso siguen en debate hoy en día.

Para terminar a manera de conclusión:

- a. No echarle la culpa a la víctima.
- b. Es importante que si se tiene conocimiento de estos delitos no compartan esa información, no la divulguen, pues no se puede portar ni almacenar ni tener ningún tipo de imagen en nuestro celular, computadores o dispositivo de un niño, niña o adolescente con sus partes expuestas, pues esto es un delito.
- c. No justifique la conducta de los victimarios.
- d. Ningún niño, niña o adolescente se explota a sí mismo ni puede consentir su propia explotación.

Taller: Seguridad Digital – Nivel de Usuario.

Colnodo – Fundación Telefónica.

Ponentes:

- Andrea Rodríguez y Cristian Cárdenas. Colnodo
- Lorena López. Lorena López. Movistar

Relatoria: *Natalia Sofía Miranda Gómez*

Primera parte: estudio de caso.

Se conformaron dos grupos de tres y dos personas. Acto seguido, Andrea Rodríguez y Cristian Cárdenas entregaron a cada grupo un caso para estudiar, acompañado de posters donde debía calificarse el riesgo y su impacto, y se debían identificar los personajes involucrados (aliados, neutrales, opositores).

Andrea Rodríguez explicó que la seguridad digital es importante porque con el *boom* de las nuevas tecnologías cada plataforma expone datos de las personas, y hay interesados en obtenerla de manera ilegal, esperándose que este negocio ilegal llegue a compararse con las drogas psicoactivas. Así, se habla de ciberguerras, ciberseguridad, y la protección de los usuarios.

De esa forma, hoy los ciberataques son unos de los riesgos globales a los que las personas deberían prestar mayor atención, incluso los costos de ciberseguridad en USA son equivalentes a los costos que se invierten en cambio climático.

Sobre la socialización de los casos:

A. El primero versa sobre un deportista que deja su teléfono en público y le hurtan el celular, con el riesgo de jaqueo de su información personal. Los ladrones intentaron acceder a sus aplicaciones, como iCloud y demás. Al intentar bloquearlos, los ladrones le engañan para que diligencie una información con el fin de recuperar sus cuentas. El deportista nota que hay un error en la página web y no alcanza a entregar toda la información que solicitaban los ladrones.

- a. Impacto: alto impacto, pues dejó el celular a la vista pública con toda su información.
- b. Aliados activos: Pedro, el deportista.
- c. Aliados: iCloud
- d. Neutrales: Cristina, amiga de Pedro

En este caso, el grupo analizó **un riesgo físico y digital**, pues no solo se pierde el bien material (teléfono), sino también los ladrones exploraron qué podían adquirir a partir del teléfono, identificando que podían acceder a las cuentas digitales de la víctima del delito, como por ejemplo acceder a sus cuentas bancarias.

De lo anterior, Andrea Rodríguez concluyó que hoy los ladrones se interesan incluso más en la adquisición de la información que los teléfonos incluyen.

B. El segundo caso trató de una estudiante que descarga una aplicación para escuchar música gratuita y sin anuncios, la cual le solicitó permisos de acceso al almacenamiento, mensajes de texto y contactos. Luego de un tiempo, la factura de su teléfono aumenta en \$300.000, al investigar, le informan que fue gracias a unos “servicios premium” que compró por medio de esta app.

- a. El impacto es alto, pues hay alto riesgo y probabilidad de que haya:
 - i. Violación de derechos de autor
 - ii. Suplantación de identidad
 - iii. Hurto de datos personales
 - iv. Daño emergente
- b. Dentro de los actores están: SIC, titulares de derechos de autor de la música, programadores de la app inmersa, compañía de teléfono, compañeros de la estudiante, etc.

- **Phishing**

Concluidos los talleres casuísticos, Lorena López explica el *phishing* como una estafa conocida desde 1990, que continúa en uso de los ciberdelincuentes. Se trata de una táctica de ingeniería social donde se usa alguna artimaña para tomar datos personales, financieros que le interesen a la persona.

El *phishing* es explotado por el error humano: gracias a emociones del miedo, incertidumbre y demás. Ej. Un correo de la DIAN según el cual la persona no ha pagado sus impuestos, con la posibilidad de acceder a una página para conocer su deuda, y al acceder al link, los terceros tienen acceso a la información personal. Otro ejemplo que se ha visto es el uso de información falsa sobre infidelidades de la pareja.

Continúa Lorena López indicando que algunos riesgos relacionados con el *phishing* son:



- Suplantación de identidad
- Hurto de datos personales

Para evitar el *phishing*, es importante tener desconfianza de los mensajes y correos electrónicos que adquirimos. Del mismo modo, es tener presente que ninguna entidad financiera pide información por internet, así como la posibilidad de pasar el mouse sobre el contenido con el fin de conocer la URL sin dar click a ella.

En caso de duda, es mejor escribir la URL de manera completa en el buscador, sin dar click al contenido que nos llega. Así nos aseguramos de que la página a la que accedemos sea la que efectivamente pertenece a la entidad.

También es posible que contactemos directamente a la entidad para corroborar que necesitan nuestra información o se han contactado con nosotros. Muchas entidades hoy tienen “<https://>” que nos evidencia que es un sitio seguro. El https es una forma de cifrar la información que se envía. Ej. Que al enviar el formulario la información será cifrada.

- **Aplicaciones móviles.**

Lorena López explica que hay aplicaciones que solicitan permisos al momento de descargarlas en nuestro teléfono. Suelen solicitar:

- Acceso a número de teléfono
- Acceso al almacenamiento
- Acceso a los contactos
- Uso de la cámara para tomar fotografías, grabar, etc.
- Acceso a SMS para leer, escribir, modificar, etc.
- Uso del micrófono
- Conocimiento de la ubicación.
- Sensores corporales.
- Acceso al calendario para modificar, crear eventos, etc.

Al dar estos permisos hay que pensar con cabeza fría para qué necesita la aplicación tales accesos. Ej. Si no es un smartwatch, ¿para qué requiere conocer mis sensores corporales?

Segunda parte: Contexto y recomendaciones.

Andrea Rodríguez y Lorena López concluyen el taller dando los siguientes consejos sobre seguridad digital:

- Virustotal.com es un escaner nos permite conocer si el correo es malware, tiene archivos corruptos, etc.
- Descargar aplicaciones de fuentes confiables: GooglePlay, Apple Store
- Comprobar quién es el desarrollador.
- Visualizar el número de descargas. Las aplicaciones ‘originales’ tienen mayor número de descargas.
- Que solo tengamos las aplicaciones NECESARIAS en nuestro celular.
- **Sobre las contraseñas.** A partir de un video se pone de presente la importancia de no utilizar la misma contraseña para todo, ni mucho menos usar



contraseñas genéricas. Un gestor que recomiendan desde la Escuela de Seguridad Digital es Keepass.

Taller: Privacidad y Protección de datos – Exposición de Derechos de las personas usuarias

ISOC Colombia

Ponente:

- **Sarah Osma. Miembro de ISOC**

Relatoría: Yesid David Páez Porras

Para comenzar, la expositora señala la importancia de la protección de datos en el mundo contemporáneo, dada la enorme cantidad de interacciones que una persona puede tener con todo tipo de plataformas digitales en su vida cotidiana, las cuales van desde la consulta que se hace sobre el estado del tráfico a través de *Waze*, hasta la compra del almuerzo a través de *Rappi*; en este contexto, la conferencista invita a reflexionar sobre las ventajas y consecuencias de este nuevo paradigma, entre las cuales se encuentra la agilidad que le imprime a todo tipo de transacciones, haciéndolas que la adquisición de bienes y servicios sean más sencillas por un lado y por el otro, el poco control que existe por parte de los titulares de los derechos sobre la forma y los usos que se le va a dar a su información.

Sarah sostiene que la naturaleza global de los sitios de internet ha producido algunas discusiones en torno a la protección de derechos fundamentales en el espacio, saber:

1. Territorialidad: ¿Cómo determinar qué ley le aplica a un dato personal, teniendo en cuenta que, por ejemplo, la recolección del dato se podría hacer en un país (Colombia) el servidor podría estar ubicado en un segundo país (La India) y el producto o servicio ofertado lo realiza una empresa ubicada en un tercer país (algún país de la Unión Europea, por ejemplo)? ¿Cuál es la norma aplicable al tratamiento de dichos datos?; la expositora explica algunos parámetros para resolver casos como el que planteó, por ejemplo, el analizar el tipo de productos y servicios que hace necesaria la recolección del dato, así como los reglamentos de cada territorio, por ejemplo, si el producto o servicio se ofrece a un usuario que se encuentre ubicado en la Unión Europea, hace que automáticamente todo el ciclo del dato deba regirse a partir del reglamento europeo, el cual, es el más garantista.
2. Anonimidad: Adicionalmente, Sarah resalta la importancia de la *anonimidad*, y de que los usuarios conozcan los mecanismos para hacerla efectiva junto a otros derechos, por ejemplo, en casos de *injuria y calumnia*, o de *pornovenganza*, en los que el victimario podría estar resguardado en un perfil anónimo ¿Ante qué autoridad la víctima podría ejercitar sus derechos? Muchas veces, esto se convierte en un obstáculo para que la víctima puede denunciar su caso.
3. Infinidad de posibilidades para recolectar la información de una persona: la expositora resalta que, en consecuencia con el constante avance tecnológico, las posibilidades para la recolección son muy diversas, las cuales van desde la forma en que se diligencia un formulario hasta la medición del tráfico en una



página web utilizando herramientas como las *cookies*; Sarah cita el último informe sobre cibercrimen en Colombia, en el cual se evidencia que la segunda causa de cibercriminalidad es la afectación o vulneración de datos, en los cuales lamentablemente no se evidencia un avance significativo en las denuncias que se formulan al respecto.

4. Spam: se exponen varios de los mecanismos existentes, con los cuales, un usuario puede hacer saber a una empresa que no se encuentra interesado en recibir ofertas sobre los productos o servicios que ofrece, por ejemplo, la protección de la cuál gozan los titulares de los datos cuando deben hacer entrega de los mismos como requisito para acceder a un bien o servicio, en ese caso, el consentimiento del usuario se encuentra viciado y por tanto, le es vedado a la empresa hacer tratamiento de dichos datos; la expositora sostiene que hace falta mucha conciencia en los usuarios, los cuales, desconocen que tienen derecho a presentar una denuncia ante las autoridades competentes cuando se encuentren, por ejemplo, ante una cláusula abusiva o ineficiente al momento de realizar una transacción por medios electrónicos.

A continuación, Sarah reflexiona en torno al protagonismo de las distintas áreas del derecho en la protección de datos, para concluir que, pese a que se trata de proteger derechos fundamentales, este tema no es del resorte exclusivo del derecho constitucional, sino que dada la naturaleza del ciclo del dato y el valor comercial que se genera en este proceso, es transversal a varias áreas del derecho, a saber:

1. Derecho del consumo.
2. Derecho de la Competencia: hay compañías que pueden ejercer un monopolio en materia de telecomunicaciones.
3. Derecho privado y de los contratos: términos y condiciones.

En todas las etapas del comercio electrónico tienen que haber debidas garantías sobre los datos que se recolectan, las cuales deben ser proporcionales, por ejemplo, a la forma en que se recolectan, en la que se utilizan y en la que se pueden explotar los datos; la expositora explica a los participantes el problema jurídico que se genera cuando una transacción no se hace sobre un bien físico que pueda ser objeto de entrega, por lo cual plantea varias teorías, para concluir, que la mayoritaria es que se entiende perfeccionado el acuerdo cuando la persona que adquirió el servicio recibió una confirmación sobre la prestación del mismo en su correo electrónico.

A continuación, Sara expone algunos puntos importantes del comercio electrónico, que a su vez sirven como guía para saber el régimen de protección de datos aplicable para cada caso, a saber:

1. Tecnología Utilizada: existen tiendas virtuales, de subasta en línea, entre otras.
2. Partes involucradas: consumidores, empresas, gobierno, entre otros.
3. Tipo de relaciones: B2B (Business to Business), B2C (Business to Consumer), C2C (Consumer to Consumer), G2B (Government to Business), G2C (Government to Consumer), este último se puede observar, por ejemplo, cuando una persona realiza el pago de su impuesto predial a través de la página de la Secretaría Distrital de Hacienda.

4. Forma de entrega: se debe analizar el tipo de producto que se entrega, puesto que pueden ser productos objeto de entrega, o algunos que son intangibles, en el caso de las descargas por ejemplo; la inmaterialidad de un producto tiene un impacto significativa en la recolección de los casos, por ejemplo, cuando se adquiere una licencia de *Spotify* o *Deezer*, uno puede disfrutar de la música, tener ahí las canciones, pero uno no la puede sacar de la aplicación, no es como un CD que uno lo puede comprar y regalárselo a alguien.
5. Formas de pago: aquí se pueden encontrar formas de pago físicas y virtuales.

Glosario en materia de protección de datos

Sara procede a explicar un glosario con términos necesarios para entender el régimen de protección de usuarios en materia de datos personales en Colombia.

1. Dato Personal: Para la expositora un dato personal es *cualquier pedazo de información que permita hacer a alguien identificado o identificable*, por ejemplo, sí un correo tiene la terminación *uexternado.edu.co*, es posible deducir que esa persona guarda algún tipo de relación con la universidad; el contexto dentro del cual la información se mueve también es importante para valorar sí un dato es personal o no.
2. Dato privado: son propios de los intereses personales de alguien, que no necesariamente tienen que ser conocidos por nadie, por ejemplo, los hábitos del consumo; es el caso de cuando se consulta una página de internet de ropa, sí una persona ingresa allí constantemente se crea un hábito de consumo, sin embargo, dado que se trata de un dato personal, la empresa propietaria del sitio web no podría utilizar esa información sobre los hábitos de consumo del usuario para enviarle publicidad, así como tampoco podría compartirla con un tercero, para que lo pueda hacer, tendría que mediar autorización por parte del usuario.
3. Dato público: aquellos datos que pueden estar en la esfera del conocimiento, por ejemplo, el estado civil
4. Dato semiprivado: Es una especie de híbrido entre dato privado y público, es un dato que sí bien no es de naturaleza sensible, sí puede interesar no sólo a su titular sino a un grupo específico de personas.

Para el régimen de protección de datos en Colombia, es muy importante clasificar el tipo de datos, puesto que, esto permite que haya claridad respecto a las dos normas:

Ley que Regula el régimen jurídico	Temática que desarrolla
Ley 1266 de 2008	Se encarga de proteger los datos personales relacionados con la capacidad de endeudamiento o el historial crediticio de la persona
Ley 1581 de 2012	En esta ley se consigna el régimen general de protección de datos en Colombia, aplica para todos los datos, con excepción de los datos financieros o de endeudamiento

Una de las asistentes al taller, comparte su experiencia personal respecto a la protección de los datos, específicamente en materia de programas de fidelización a

través de tarjetas de puntos; ella explica que se encontraba afiliada al sistema de puntos de un almacén de cadena y que después de realizar la compra de unas botellas de vino en uno de sus almacenes, recibió en su celular un mensaje de texto, en el que le ofrecían más productos para que acompañaran las botellas de vino que había adquirido, lo cual, se configura en un caso de un mal tratamiento de datos personales; Sara resalta la importancia de que el consumidor se informe para que no sucedan ese tipo de eventos, el consumidor debe informarse, y de ser el caso, sí el tratamiento de datos no es el adecuado, abstenerse de participar en el sistema de puntos.

La expositora también resalta que el elemento más importante es el consentimiento, puesto que, hay muchas personas a las que no les molesta que se trate sus datos para ofrecerles productos y que por el contrario, lo ven como una ayuda, por esto, es fundamental que el usuario entregue un consentimiento informado al respecto; uno de los asistentes al taller, pregunta a la conferencista sobre algunas prácticas que realizan algunas empresas, las cuales consisten en solicitar datos personales innecesarios para acceder al producto o servicio o para poder disfrutar de algunos elementos como el *wi-fi*, a lo que la expositora responde que lo más importante es que las empresas o comercios le entreguen al usuario las herramientas para detener el tratamiento de datos cuando este así lo considere.

Adicionalmente, Sarah recomienda a los asistentes eliminar las cookies de sus navegadores, ya que, dada su naturaleza, permite a las distintas empresas vigilar cada uno de los movimientos que realizan los usuarios que visitan el respectivo sitio web; lo más importante, reitera, es que el usuario pueda entrar a la configuración y pueda eliminar sus cookies; también resalta la importancia de la confianza corporativa, como mecanismo de defensa y de castigo a compañías que no cumplen con la protección de datos hacia sus usuarios, y que dichas sanciones, dependen en gran medida de que el usuario conozca conceptos básicos sobre la protección de datos, entre los cuales se encuentran, los siguientes:

¿Quién es el responsable del tratamiento de datos?	El responsable es aquella persona que cuenta con la autorización del tratamiento de datos y establece como y en qué forma se a va a realizar
¿Quién es el titular de los datos?	Toda persona sobre la cual la información se esté tratando
¿Qué es tratamiento de datos?	Toda operación que se realice respecto a los datos, recolectar, almacenar información
¿Qué es una base datos?	Es cualquier conjunto de datos que se encuentre agregado de manera organizada.
¿Qué es un Metadato?	Es el envoltorio del dato; el contenido de la información que se está tratando, por ejemplo, la IP mediante la cual se envió la información o el tipo de archivo y las coordenadas en la que se tomó una foto, en otras palabras, es un dato genérico que está asociado a un dato concreto.



Una vez compartidos dichos conceptos, Sarah expone sobre los casos en que normativamente se pueden recolectar datos, a saber:

1. Cuando los titulares deciden aportarlos de manera personal
2. Cuando son requeridos para la prestación de un servicio
3. Cuando son recolectados en cumplimiento de un deber legal
4. Cuando son recopilados de manera automática
5. Cuando son obtenidos mediante el análisis y el procesamiento de los datos suministrados por el individuo

Partiendo de lo anterior, ¿De dónde viene la protección de datos? ¿Cuál es su importancia? Es un derecho fundamental que se encuentra consignado en la Constitución Política, la cual garantiza el derecho a la intimidad y al buen nombre a todas las personas, así como copiar artículo actualizar y rectificar

Estos derechos ya han sido incluso, superados por otros, por ejemplo, el de la portabilidad, el cual garantiza a todas las personas, que cuando migren de una empresa a otra puedan llevar consigo la información, y la compañía inicial no tendría por qué conservar dichos datos. Adicional a lo anterior, Sarah procede a explicar la clasificación de páginas web, las cuales, clásicamente se dividen en:

1. Páginas web simples: son aquellas que por lo general no recolectan información ni procesan datos personales.
2. Tiendas virtuales: son en las que más se recolectan y almacenan datos, ya que se hacen transacciones comerciales; allí se condensan los dos regímenes de protección de datos existentes en Colombia, a saber: los datos financieros los ampararía la ley 1266, al paso que los demás datos serían protegidos en virtud de la ley 1581;

¿Qué información sobre protección de datos debería tener una página?

1. Información sobre la compañía
2. Información legal (Mecanismos para autorizar la recolección y el tratamiento, políticas de cookies, Política de privacidad, Términos y condiciones de uso web y los mecanismos legales para ejercer dichos derechos).

Se comenta que cuando una página web no cumple con alguno de los primeros elementos que enuncian como información legal, podría estar infringiendo el régimen de protección de datos en Colombia; uno de los asistentes pregunta si la legislación colombiana exige que se cumpla con toda la información legal, incluyendo los términos y condiciones, dado que, a su juicio, muy pocas páginas cumplen con dichos requisitos; Sarah recalca que sólo sería necesario contar con los mecanismos para recolectar los datos, así como la política de privacidad, sin embargo, asevera que el hecho de que se cumplan con todos los documentos que se explicaron, más que una obligación, es un sello que demuestra que una empresa es garantista en cuanto a los datos de sus usuarios.

¿Cuál sería el estado ideal de una página web? Para Sarah, lo ideal sería una página libre de cookies, sin embargo, dado que esto sería un escenario muy improbable, la página web ideal sería aquella que se ampare en los siguientes criterios:



1. Proporcionalidad y Necesidad: las páginas no deben recolectar datos más allá de los necesarios; en este punto se debe tener especial cuidado, dado que, por ejemplo, existen aerolíneas que le solicitan a sus usuarios datos sobre la religión que profesan, un dato que aparentemente no sería necesario para celebrar el contrato, sin embargo, sí el tiquete que está comprando el usuario incluye alimentación y el vuelo proviene de un país árabe, es probable que la aerolínea requiera dicha información para saber qué alimentos no se podrían servir a un pasajero determinado.
2. Garantizar la confianza corporativa: como el caso del carrito de *Amazon*, el usuario puede agregar por error dos veces el mismo producto y antes de finalizar la transacción, el desarrollador consideró pertinente que, en estos casos, se le pregunte al usuario si desea ordenar dos unidades, prácticas como este fortalecen la confianza corporativa, que es el elemento más importante de una organización, además de ser leales con el consumidor.
3. Responsabilidad demostrada: hace referencia a las medidas que deben tomar las empresas para garantizar los derechos de ellos titulares de los datos; este criterio es de gran importancia, dado el inmenso avance de la tecnología y la imposibilidad que tiene el derecho de estar actualizándose al mismo ritmo.

La expositora aclara que la Superintendencia de Industria y Comercio, como autoridad de datos en Colombia, no puede imponer sanciones que conduzcan al pago de indemnizaciones individuales; sí un usuario busca algún tipo de retribución específica, debe hacerlo por otras vías, tales como el derecho civil o la constitucional a través de la acción de tutela; para contextualizar, Sara expone el caso de *Instagram*, la cual, es a su juicio una de las plataformas que más cláusulas abusivas imponen a sus usuarios, lo anterior, se evidenció en el caso de una cantante famosa, que quiso usar una de las fotografías que cargó a la plataforma para una campaña publicitaria, acto seguido, *Instagram* presentó una acción judicial en contra de dicha cantante por el uso de la fotografía, puesto que ella ya la había cargado previamente a la plataforma.

¿Cómo debe hacerse el tratamiento respecto a las cookies?

¿Qué son las Cookies?: *son pequeños archivos que se almacenan en el ordenador del usuario y están diseñados para contener una pequeña cantidad de datos específicos de un cliente.* Lo anterior, lamentablemente no se cumple, por cuanto, hoy en día la mayoría de las páginas web aceptan los cookies sin que exista un consentimiento previo; en esto el usuario debe ser muy cauteloso, por cuanto dicho consentimiento debe ser libre y espontáneo y es allí, donde el concepto como el de la privacidad por diseño, impiden que el usuario otorgue un consentimiento libre, por ejemplo, en los casos en que previamente la casilla en la que se aceptan los términos y condiciones ya se encuentra preseleccionada.

Uno de los asistentes al taller, agrega que el problema de las cookies puede estar en su origen, dado que, el internet inicialmente no fue diseñado para ser transaccional, y es en ese escenario, es donde nacen las cookies, como una herramienta para evitar la pérdida de información.



¿Qué deberían informar las compañías respecto a las Cookies?

1. La instalación de las cookies
2. El tiempo de almacenamiento de cada cookie
3. La cantidad de información

La expositora comparte un ejemplo de una buena política de Cookies, perteneciente a una firma de abogados española *Debrauw*: “*Debrauw.com utiliza Cookies para: adaptar el contenido de la página web a sus interés; recordar a la gente que ha agregado a tus “Mis contactos”; ofrecer la funcionalidad básica de la página web; generar estadísticas de usuarios de forma anónima para que nuestra página web sea más fácil de usar (Google Analytics); No usar o compartir sus datos con terceros para fines publicitarios*”; con este ejemplo Sarah explica que es posible hacer una buena política de datos.

La base para construir una buena política se encuentra en un adecuado tratamiento, el cual, debe cumplir con las siguientes condiciones:

1. El responsable del tratamiento debe conservar copia de la autorización de los titulares. Este requerimiento encuentra su excepción cuando la información es requerida por parte de una entidad pública en desarrollo de sus funciones, en los casos de urgencia médica o sanitaria, para el tratamiento de información autorizado por la ley para fines estadísticos o científicos, con datos relacionados con el registro civil, entre otros.
2. Contar con una política de tratamiento de información personal que debe estar disponible para los ciudadanos: la obligación incluye hacer conocible la política a los usuarios;
3. *Contar con un aviso de privacidad:* este debe contar con el nombre del responsable, la finalidad de la recolección, y en caso de que se haga una recolección de datos sensible (estos, entendidos como aquellos que pueden conducir a la discriminación y requieren de medidas de seguridad más altas para su tratamiento), la persona tiene la facultad de no autorizar el tratamiento de estos.

¿Qué requisitos debe tener una política de privacidad?

1. Nombre
2. Razón social
3. Dirección
4. Correo electrónico
5. En que consiste el tratamiento
6. Ver e informar cuales son los derechos que le asisten al titular.
7. El área competente para la atención de quejas o reclamos relativa a la protección de datos
8. Procedimiento para que los titulares conozcan sus derechos
9. Última fecha de actualización

Uno de los asistentes comparte un caso que conoció respecto a una entidad pública, cuya política de privacidad sólo consistía en remitir al usuario a la ley 1581 de 2012; la expositora asevera que allí no existiría una política de privacidad, pero que



lamentablemente, al tratarse de una entidad pública, la Superintendencia de Industria y Comercio no tendría competencia y sólo podría dar ordenar o exhortar a que se corrijan dichas prácticas, la facultad de sancionar la tendría la Procuraduría General de la Nación.





6to Foro de Gobernanza de Internet Colombia 06 y 07 de Noviembre del 2019

Relatoría

Día 02:
Jueves 07 de Noviembre del 2019

8:30 a.m – 9:00 a.m

Mensajes de Bienvenida, Dra. Adriana Zapata. Decana de la Facultad de Derecho, Universidad Externado de Colombia.

Ponentes:

- Dra. Zoila Vargas Mesa, Directora Ejecutiva de la Comisión de Regulación de Comunicaciones (CRC)
- Dra. Adriana Zapata. Decana de la Facultad de Derecho, Universidad Externado de Colombia

Relatoría: Daniel Peñaranda Rodríguez

Las palabras de bienvenida estuvieron a cargo de la doctora Adriana Zapata, quien en un principio relata cómo en 1886 nace la Universidad Externado de Colombia en respuesta al absolutismo y a la supresión de la libertad de enseñanza. En posterior instancia la doctora enlaza los principios fundantes de la casa de estudios con los promulgados por la gobernanza, pues como señala: “se defiende el acceso a la educación, la libertad de expresión y apertura”.

También indica que la red es un instrumento para efectivizar los derechos, pero que aún hay un gran camino por recorrer para conectar a los desconectados, destacando así la importancia de estos foros para superar las brechas digitales. Entonces es por esta misma razón que señala el papel que deben tener las universidades en la formación sobre tecnología en las carreras universitarias, porque el impacto de internet permea todos los sectores de la sociedad, incluso el derecho. Campo este que tiene vocación de servir al debate sobre diversos aspectos relevantes en lo que respecta a la gobernanza de internet, tema que desde los últimos años supone el mayor desafío para las ciencias jurídicas.

Posteriormente, se realizó la presentación Mesa Colombiana de Gobernanza de Internet, a cargo de la doctora Zoila Vargas refiriendo los diversos actores que la conforman. Seguido de esto relata cómo se gesta la Mesa durante la quinta versión del Foro Latinoamericano De Gobernanza de Internet en 2012, tiempo desde el cual se han adherido diversos actores para tratar temas de aprovechamiento de internet para reducir la pobreza, neutralidad en la red, ciberseguridad, entre otros.

Ya refiriéndose al sexto Foro colombiano de Gobernanza de Internet, indica que los talleres realizados durante su celebración tienen por objeto comprender los temas que atienden a la gobernanza. Además de que el foro abordará temas de suma relevancia y que se hallan en línea con el dialogo sostenido a nivel mundial en lo que hace a la gobernanza de internet.

Por último, hace especial mención en el papel de la Comisión de Regulación de Comunicaciones, en continuar participando en la Mesa colombiana de Gobernanza de Internet para aportar y construir el futuro de internet en el país.



Posteriormente se tuvieron las palabras de Markus Kummer. Presidente del Comité Ejecutivo de la Internet Governance Forum Support Association (IGFSA) quien presentó la IGFA, entidad sin ánimo de lucro fundada en 2014, que promueve las reuniones de Gobernanza de Internet a nivel nacional, regional y el Foro Global. Markus se refirió a la importancia de las iniciativas tanto regionales como nacionales donde se llevan a cabo discusiones sobre internet como en el foro en el que estamos en este momento que alimentan la Asociación que busca promover el intercambio y la colaboración entre estas iniciativas en torno a la Gobernanza de Internet.

Los aportes realizados por la IGFSA al Foro de Gobernanza de Internet en Colombia en los últimos años a permitido otorgar becas con las cuales algunos de los participantes de región han podido asistir al Foro. La IGFA identifica nuevas fuentes de financiamiento y facilita el financiamiento de las reuniones de internet y de eventos que se hacen tanto a nivel regional como nacional. Igualmente hacen contribuciones al fondo fiduciario administrativo administrado por Naciones Unidas. Markus manifiesta que es interesante ver como desde la Asociación crear estos apoyos ha hecho que cada vez más foros locales nacionales regionales surgen alrededor del mundo. Por ejemplo en 2015 hubo 15 foros nacionales y 8 regionales y para el 2017 esta cifra se incrementó a 28 nacionales y se mantuvieron 8 regionales. Ese incremento hace que hayan muchas más personas que están interesadas en estos temas participen.

Finalmente Markus manifiesta que espera que se dé una buena discusión en el Foro Colombiano entre los que estemos participando y espera que podamos vernos de nuevo en Berlín donde va hacer el Foro de Gobernanza Internet global este año a finales de este mes de Noviembre.

9:30 a.m – 11:00 a.m

**Acciones en Gobernanza de Internet para conectar a los no conectados
.CO, Colnodo y CRC.**

Ponentes:

- Martha Liliana Suárez, Presidenta en Dynamic Spectrum Alliance - DSA. Empresa Privada.
- Julián Casasbuenas G. Director Colnodo. Sociedad Civil.
- Miguel Felipe Anzola, Director General de la ANE. Gobierno.
- Jean-Marie Chenou, Universidad de los Andes. Academia

Moderador: Carlos Lugo Silva- Comisionado sesión de Comunicaciones

Relatoría: *Daniel Ríos Sarmiento*

El acceso a Internet continua siendo una limitante para cerca de la mitad de la población colombiana que aún no está conectada o está subconectada. A nivel global existen propuestas para conectar a los no conectados. Este panel busca explorar las alternativas y estrategias para llegar a estas poblaciones para que puedan disfrutar de los beneficios que trae Internet respondiendo a ¿Qué acciones y herramientas deben utilizarse para acelerar esta tarea?; ¿Qué programas o tecnologías se están utilizando en el mundo para este fin?; ¿Qué aspectos son facilitadores para conectar los no conectados?



Carlos Lugo Silva - Comisionado sesión de Comunicaciones: Primero hace una presentación de todos los panelistas y propone una reflexión inicial sobre el hacer parte de la mesa de gobernanza de internet bajo el modelo múltiples partes interesadas es un gran reto dado que el presente es un momento de inflexión e histórico que implica que las decisiones y acciones que se deben tomar los distintos agentes de este modelo va a ser fundamental para el futuro de la Internet y para el cumplimiento de los objetivos del desarrollo sostenible dado que al final de esta cuarta revolución industrial implica a todos y no solo a una parte de los ciudadanos del mundo y en foros como este se está viendo el avance de la tecnología, la modernización de redes, ya estamos en el wifi 6 que implica hiperconectividad, entonces existen ciudadanos que se enfrentan a retos a nivel social dado la proyección de la ciudadanía digital que ya no es solo usar bien la tecnología sino también conocer sus derechos, responsabilidades, leyes vitales de los derechos de autor porque ya el ciudadano no es sólo consumidor, también produce contenidos permanentemente y ahora lo va a hacer de una manera mucho más exponencial gracias a la hiperconectividad.

El estado y las instituciones reguladoras y el modelo de múltiples partes interesadas están tomando decisiones para garantizar la llamada transformación digital, pero hay una realidad que no es solo en Colombia sino en el mundo y es que haciendo cuentas gruesas la mitad del mundo no está conectada o no están conectados al internet productivo de banda ancha que permite hablar de medicina, salud, comercio electrónico, etc, esto no ha llegado a todos los rincones lo que quiere decir que la gran revolución no ha llegado a todos los rincones de la sociedad. Hay una gran preocupación y un gran reto en la toma de decisiones sobre la gobernanza de internet y por esto este panel para identificar los retos que se presentan.

Pregunta para Dr. Miguel Felipe, teniendo en cuenta las cifras que hablan aproximadamente de un 40%, cerca de la mitad de los colombianos no tienen acceso a internet: ¿Desde la visión de la ANE, qué está pasando, qué está haciendo el gobierno para poder solventar y cerrar esa brecha de conectividad que aún existe?

Miguel Felipe Anzola, Director General de la ANE: Agradeciendo la invitación, declara que hay una preocupación muy grande por logra que todos los colombianos puedan acceder a la conectividad de banda ancha, la conectividad pero también la apropiación; desde el punto de vista de conectividad, la primera gran apuesta del gobierno es poder hacer una asignación del espectro a través de una subasta que permita contar con el espectro asignado el próximo año y además que se desarrolle la ampliación de las redes de tal forma que logre cumplir con la asignación de un gran margen de espectro que a comparación con el ya asignado, lo que se propone subastar es considerablemente más amplio, alrededor de dos o tres veces más de lo que se tiene actualmente asignado. Dado lo anterior la expectativa es poder cumplir con el propósito de poder dar cobertura a todo el país.

Como se conoce por todos respecto de la ley lo que propone es que todos los colombianos podamos tener acceso muy rápidamente a los servicios, dado que el mayor valor para el ciudadano es poder contar con el servicio ya, todos sabemos que es espectro es un bien no almacenable que si no lo asigno no produce nada y no se recupera de ninguna manera un resultado si se tiene guardado, por eso la mejor opción que hay es asignar ese espectro a la brevedad para que los operadores puedan ofrecer esos servicios.



Así mismo propone recordar que también que en Colombia se trabaja bajo la premisa que hay varias opciones, el gobierno está abierto a asignar frecuencias para los diferentes tipos de redes que se tienen, hay casos de lugares en Colombia en donde muy difícilmente llega la cobertura de las redes comerciales por lo cual se puede hablar de redes comunitarias que permiten ofrecer cobertura en condiciones particulares a la población de lugares de difícil acceso.

Para el caso particular de fomento a la cobertura de los lugares de difícil acceso, la ley ofrece unas condiciones que favorece e incentiva el despliegue de infraestructura con carácter comunitario, teniendo en cuenta que es el MINTIC quien ofrece el espectro electromagnético, y es la ANE el órgano asesor que ofrece estudios técnicos en esta materia; es por esto que la política pública está dispuesta a favorecer el despliegue de infraestructura para atender a estas necesidades particulares.

Ejemplo de lo anterior se encuentra en los enlaces del Blackhold, los enlaces de conectividad los cuales cada una de las estaciones de servicio a lo largo y ancho del país promueve que se puedan usar el espectro en condiciones económicas favorables para el sujeto que aún no está conectado.

En resumen el director de la ANE reconoce que el gobierno está adelantando diferentes acciones para favorecer la conectividad del país y la ANE está dispuesta a poder trabajar con los interesados en el desarrollo de nuevas propuestas y nuevas iniciativas; así mismo expuso una estrategia muy importante. Ejemplo de ello es el uso de la infraestructura de televisión que lleva más de cincuenta años consolidándose y ofreciéndose como servicio en todo el país, entonces existe la oportunidad de utilizarla también para las frecuencias para servicio de conectividad convirtiéndose en una solución excelente para lograr alcance y cobertura en lugares remotos.

Carlos Lugo Silva- Comisionado sesión de Comunicaciones: Aprovecha antes de dar paso a la siguiente pregunta para agregar sobre las acciones que adelanta el Estado para mejorar la conectividad a través de la ley 1978 de 2019 propone tener una regulación autónoma y transparente para fomentar la conectividad y se lanzó a través de el sandbox regulatorio en temas de calidad, temas de usuario, lo que se propone es que se experimente durante los próximos dos años iniciativas innovadoras que permitan aplicar soluciones de conectividad sin tener que aplicar la carga regulatoria requerida en casos normales para fomentar la ampliación de cobertura.

Pregunta para Ingeniera Martha Liliana Suárez, ¿qué está pasando en el mundo? ¿Qué iniciativas están aplicando en el mundo entero para afrontar el reto de conectar a los no conectados?

Martha Liliana Suárez, Presidenta en Dynamic Spectrum Alliance: Comenzó agradeciendo por la invitación y respondió que el reto de conectar a los no conectados también implica a las industrias a las cuales ella representa, y lo afronta este sector promoviendo usos dinámicos de la tecnología.

Carlos Lugo Silva- Comisionado sesión de Comunicaciones: Pregunta para Julián Casabuenas G. Director Colnodo, ¿Cómo ha sido la experiencia de implementar proyectos pilotos para conectar a los no conectados? ¿Cuáles han sido esos aspectos claves para tener en cuenta en este tipo de proyectos?



Julián Casasbuenas G. Director Colnodo: comenzó agradeciendo la invitación y expuso la experiencia de poder trabajar con organizaciones internacionales para implementar estrategias de fomentar que las mismas comunidades sean las que logren lo requerido para que conectarse a través de redes comunitarias y ha sido un proceso donde se han visto experiencias en Cataluña, México, Argentina, y se puede ver que se resuelven de manera práctica el acceso de cada población y se puede implementar en Colombia sobre todo en poblaciones que están ubicadas en zonas rurales.

Al respecto de Colombia ha expuesto múltiples escenarios en diferentes foros la implementación de las redes comunitarias y a lo largo de reuniones y trabajos en conjuntos han identificado aspectos facilitadores para la implementación de estos proyectos.

En México, por ejemplo, destacó que la implementación de las redes comunitarias han aumentado considerablemente la calidad de vida de estas poblaciones con un componente importante de apropiación de tecnologías.

Evidenció la necesidad de facilitar el acceso a la fibra óptica ya desplegada y a la interconexión entre diferentes proveedores para compartir infraestructura, dados que las redes comunitarias se pueden beneficiar y se ven en el caso de Colombia en Buenos Aires Cauca y Casanare; en estos pilotos descubrieron que es más costoso conectar a Buenos Aires Cauca que a Casanare debido a que el despliegue de redes debe ser mayor porque no hay mercado en la zona consolidado que haya desplegado fibra óptica.

Un aporte crítico a la ley es que si bien es un claro beneficio promover las redes comunitarias, estas no están plenamente definidas en la norma, lo cual genera que no se aclare en qué momento se puede implementar las facilidades regulatorias del carácter comunitario.

Carlos Lugo Silva- Comisionado sesión de Comunicaciones: Pregunta a Jean-Marie Chenou ¿Por qué resulta relevante en este modelo de múltiples partes interesadas discutir estos temas y cuáles deberían ser los retos para conectar a los no conectados?

Jean-Marie Chenou, Universidad de los Andes: Comenzó agradeciendo la invitación y propuso contextualizar lo hablado hasta el momento, haciendo una salvedad sobre el cambio de perspectiva de la palabra conectados, paso de un mero concepto técnico a un concepto político y económico; lo cual demuestra que el acceso debe ser un pilar de políticas públicas y se amplía su alcance dado que implica escenarios de aplicación de derechos y capacidades empresariales y económicos, tanto como una necesidad como una oportunidad de desarrollo.

Desde la perspectiva académica, la responsabilidad del acceso no los vincula pero si la fundamentación de estudio del proceso de desarrollo; lo ideal es afrontar debates políticos, económicos y sociales de los impactos de los aspectos involucrados con el fin de proponer soluciones desde las alianzas de cada uno de los aportes de los múltiples partes interesadas.



Carlos Lugo Silva - Comisionado sesión de Comunicaciones: Pregunta para Dr. Miguel Felipe ¿Qué se proyecta a futuro en Colombia sobre la conectividad de no conectados y demás debates relacionados?

Miguel Felipe Anzola, Director General de la ANE: Sobre el reto de conectar a los no conectados, se proyecta a futuro que se afronte el reto de los datos masivos, se debe tener una baraja de posibilidades que ofrecen soluciones a las experiencias de desarrollo social.

Actualmente hay muchas zonas rurales conectadas gracias a la ardua aplicación de políticas públicas, pero se trabaja para seguir ampliando la cobertura a través de las redes comunitarias y el gobierno tiene las competencias regulatorias para el fomento pero también evidencia que debe florecer el mercado e industria relacionada.

Uno de los retos que afronta el gobierno es cuando se asigna el espectro a los operadores en lugares donde no se use, el cómo lograr que sea rentable a través de cualquier tecnología implementada.

Ejemplo la tecnología de wifi floreció debido a que los costos de implementación bajaron y permitió al mercado tener condiciones favorables para cobertura, este ecosistema está en proceso de construcción y por ende queda mucho trabajo pendiente para llegar a cumplir este propósito.

Carlos Lugo Silva - Comisionado sesión de Comunicaciones: Pregunta para Ingeniera Martha Liliana Suárez, ¿Cómo hacer para aunar esfuerzos para organizar los diferentes sectores para desarrollar todas estas iniciativas que le falta para crecimiento exponencial?

Martha Liliana Suárez, Presidenta en Dynamic Spectrum Alliance: Es fundamental que se promueva el acceso a todos los sectores interesados para que el usuario logre tener alternativas para acceder a los servicios de conectividad.

El reto es aclarar definiciones técnicas que hasta para los expertos llega a ser problemático, ejemplo cómo definir el 5G, y la mejor forma de aclarar el tema es con ejemplos de casos de uso: ya no es solo un operador móvil, también es vincula a otros sectores, cambia paradigma de seguridad, cambia el paradigma de infraestructura, quienes jalonan el 5G son las industrias y no los operadores.

Se debe afrontar que a futuro se va tener nuevos tipos de actores y nuevos tipos de redes.

Carlos Lugo Silva- Comisionado sesión de Comunicaciones: Pregunta para Julián Casasbuenas G., ¿Desde la experiencia de Buenos Aires Cauca que se evidencia y que retos encuentra para el fomento de otros proyectos?

Julián Casasbuenas G. Director Colnodo: resaltó que el proyecto aún está en proceso de implementación, este proyecto comenzó con la iniciativa de aplicar redes comunitarias inspirados con casos como el de México, y se puso en marcha a través de una licencia experimental en la cual se logró un consenso con la ANE y se puso poner de acuerdo para iniciar el proceso.



El modelo comenzó en abril de 2019 y termina en el próximo año y el convenio propone determinar la viabilidad técnica, jurídica, económica y social de implementación de redes sociales comunitarias en las poblaciones con el fin de documentar el piloto en memorias que busca superar dificultades, actualmente no hay un permiso para el uso del espectro en la zona no hay acceso a redes móviles comerciales.

Hasta ahora hay varios retos: que va a pasar al demostrar el funcionamiento del modelo en Colombia, el acceso a internet para implementar, mantener estable la red, mantenimiento, otro reto es cómo afrontar las caídas de luz de la energía eléctrica de la zona.

El piloto es un proceso que busca que la misma comunidad se organice e identifique sus propias necesidades, con un enfoque de género capacitando a las mujeres locales.

Carlos Lugo Silva- Comisionado sesión de Comunicaciones: Pregunta a Jean-Marie Chenou, ¿Desde la visión de las universidades como parte integral de la triada con empresas y gobierno, cómo afrontar los retos de conectar a los no conectados?

Jean-Marie Chenou, Universidad de los Andes: El papel de la universidad es, a su parecer de carácter híbrido, con iniciativas de participación desde las ciencias sociales a través de acompañamiento para ofrecer capacitaciones a los diferentes actores a través de la educación.

La Investigación, abstracta de los modelos de gobernanza respecto de la implementación de cómo se afrontan los proyectos o retos en términos políticos de los diferentes actores, abarcando los impactos en la sociedad global y local.

CONCLUSIONES: propuestas por Carlos Lugo Silva- Comisionado sesión de Comunicaciones

1. El considera que la subasta del espectro es necesaria para que pueda desarrollarse os objetivos de política pública en materia de conectividad.
2. El espectro no es lo único que se debe tener en cuenta en materia de transformación digital de cerrar la brecha de los no conectados
3. Incentivar el desarrollo de otros mercados
4. Desarrollar políticas pública para el fomento de las redes comunitarias
5. Regulación flexible mejora el acceso remoto a internet.
6. Pregunta ¿que tipo de internet se quiere ofrecer a Colombia?
7. Que espacios de la Mesa de gobernanza de internet sea abierto a todos
8. El rol de la academia es crucial para la educación relacionada con la transformación digital

11:30 a.m – 1:00 p.m

Libertad de expresión y bloqueo de contenidos en línea

Telefónica, Karisma y Google

Moderadora: *Carolina Botero Cabrera, Directora de la Fundación Karisma*

Ponentes:

- *Diego Armando Acosta González. Docente Investigador del Departamento de Propiedad Intelectual de la Universidad Externado de Colombia.*
- *Emilio Santofimio. Gerente de Gestión Legal, Telecomunicaciones y Competencia. Telefónica Movistar.*
- *Gabriel Recalde. Gerente de Políticas Públicas y Relaciones con Gobierno para América Central y el Caribe en Google.*
- *Andrés Vélez, Asesor Legal. RedPaPaz.*
- *Carlos Humberto Ruíz, Subdirector de Vigilancia y Control de Telecomunicaciones del Ministerio de Tecnologías de la Información y Comunicaciones*

Relatoria: *Laura González Rozo*

La moderadora inicia el panel indicando que el tema de la libertad de expresión y bloqueo de contenidos en línea es un asunto muy importante que nos afecta a todos como usuarios y usuarias de internet. Además, señala que la idea de la sesión es que se genere una discusión amplia sobre los aspectos técnicos y jurídicos que suponen los bloqueos en internet.

Posteriormente, Botero hace referencia a la promesa de internet de ser una herramienta de democratización del conocimiento, en donde cualquier persona tiene la capacidad de interactuar con los demás, pues, pese a que hay una serie de barreras de acceso a este servicio, una vez se está dentro del mismo hay una promesa de creación de una sociedad más democrática donde todos pueden participar. Indica que, aunque esta idea se ha venido resquebrajando de varias maneras, es importante saber que internet sigue siendo un instrumento que potencializa y permite la libertad de expresión, entendiendo por esta no solo la capacidad que tiene un individuo de expresar lo que piensa, sino también de encontrar la información que le permita aprender y formarse.

Es preciso indicar que un punto importante al hablar de bloqueos, es pensar por qué existen estos, pues hay que entender que internet no es más que el reflejo de la sociedad, por eso para hablar de este tema se puede comparar el internet con un cuchillo: el cuchillo, así como sirve para cortar el pan en la casa, también sirve para matar a alguien, y así funciona internet, pues potencia lo bueno, pero también lo malo.

Entre más personas usan internet, hay un despliegue cada vez mayor de esa maldad o la parte que nos gusta menos de esta red, que tiene que ver con contenidos violentos, material de abuso sexual infantil y, en general, contenidos ilegales; temas que preocupan a los Estados, personas, grupos y familias, quienes quieren saber cómo controlar que ese material no se distribuya. En este punto, uno de los problemas que surge es que no todo es ilegal ni todo lo que parece serlo lo es efectivamente, o muchas veces el uso que se da a determinadas cosas puede cambiar la legalidad del material. Al respecto hay algunos ejemplos: la propiedad intelectual es una de las



cosas que más preocupan en internet, sin embargo, se puede utilizar la foto de figuras públicas para hablar de ellas y esto constituye una excepción al derecho de autor - aunque haya una obra protegida- por el uso que se está dando. Por ello, definir cuándo es o no ilegal el contenido en ese caso, requiere más que el solo uso de una obra protegida, se necesita de contexto, definición de intención, entre otros elementos.

Algo similar ocurre con el material violento, por ejemplo, en el caso reciente de Ecuador, a las comunidades indígenas que protestaban, en redes sociales les bloquearon su contenido por considerarlo violento, entonces no es fácil determinar esa línea de ilegalidad. Sin embargo, se ha llegado a una serie de acuerdos a nivel internacional, como en el caso del material de abuso sexual infantil, donde mundialmente se reconoce que este tipo de contenido no debe circular, y se han tomado medidas para que esto no suceda. Extender ese privilegio a otros contenidos puede ser peligroso y es un tema importante para discutir.

Otro asunto a analizar es cómo se hacen los bloqueos y quién los hace, y ahí adquiere relevancia el rol de los intermediarios, que son las personas o empresas que permiten hacer lo que hacemos en internet, de estos hay varios tipos: intermediarios de infraestructura, los que ofrecen alojamiento, las redes sociales, entre otros, y esa diferencia es importante ya que su rol cambia, pues la forma en la que hacen las cosas varía y, por tanto, también la responsabilidad que tienen.

Por otra parte, es importante hablar del concepto de la neutralidad en la red, pues este recuerda que los intermediarios no deben filtrar ni bloquear el contenido, sino que deben permanecer neutrales y permitir que este fluya. No obstante, esto tiene sus matices: restricciones por motivo de tráfico, órdenes del Estado en el sentido de controlar un determinado material, entre otras, pues esto obliga a que el intermediario deje de ser neutral frente a ese contenido.

Preguntas dirigidas a los Panelistas:

1. Se pregunta al panelista Emilio Santofimio ¿cuál es el rol de Telefónica como ISP en el proceso de bloqueo de contenidos en Colombia?

Responde Santofimio que el papel es el de una ISP y, en ese sentido, Telefónica cumple con el marco legal y constitucional vigente, por lo que respeta los derechos de los usuarios y la libertad de expresión, y agrega el panelista que por ser una empresa que provee servicios en un marco de vigilancia y control, debe acatar las órdenes que imponen las autoridades jurisdiccionales o administrativas, como las relacionadas con temas de contenido de abuso sexual infantil, juegos legales de suerte y azar, y el contenido que se defina como ilícito por parte de estos agentes, que lleva a generar bloqueos adicionales a los que están expresamente establecidos en la normativa.

Por ello, indica que Telefónica siempre ha defendido la neutralidad de la red, pues es fundamental que se dé un flujo de información y esta sea bloqueada solo si esta es ilícita, entre otras razones, porque al ser vigilados, tienen visitas permanentes de las autoridades sectoriales en las que se verifican esos bloqueos, de cara a los sistemas de la compañía.



Por último, señala en panelista que la empresa en este tema es muy transparente, y por ello en su Centro de Privacidad y de Seguridad, tiene una forma mediante la cual cualquiera puede verificar las políticas de protección de datos de la compañía en su página web. Adicionalmente, indica que como el MinTIC envía periódicamente unos listados que se actualizan donde se relacionan los contenidos determinados como ilícitos, hay una persona dedicada en la empresa a este tema, para que los usuarios no puedan acceder a ese material (en caso de intentar hacerlo, se les redirige a un sitio web donde aparece un aviso en el que se dice que ese contenido ha sido bloqueado por una orden administrativa o judicial).

2. Se pregunta a Gabriel Recalde ¿cuál es la tensión que sufre un intermediario a la hora de remover contenidos generados por usuarios que puedan ser ilegales?

Los intermediarios son los actores o empresas que proveen servicios de intermediación entre quienes generan contenido y quienes quieren acceder al mismo; hay varios tipos: intermediarios de acceso a internet, los que proveen alojamiento, quienes proveen servicios de indexación de contenido como buscadores, o quienes alojan contenido y permiten la comunicación entre personas como en el caso de las redes sociales.

El crecimiento de internet en los últimos 20 años se ha dado gracias a estos intermediarios, porque son quienes han permitido convertir internet en la herramienta de comunicación más poderosa de la historia, y han posibilitado el ejercicio del derecho fundamental a la libre expresión, punto donde vemos que surge la primera tensión, al intentar definir si ésta tiene límites cuando se enfrenta con otros derechos y ahí se da la dificultad de las plataformas para definir estos temas. Hay algunos asuntos donde la respuesta es clara, como en asuntos de material de abuso sexual infantil, pues hay un consenso que indica que es un material ilegal y no deseable y, por tanto, cuando las plataformas tecnológicas lo detectan, lo remueven inmediatamente y trabajan con las autoridades para dar lugar a las respectivas investigaciones. Incluso desde la industria, se han dado soluciones tecnológicas que permiten identificar automáticamente cuando un contenido identificado previamente se vuelve a subir, para que se elimine de manera inmediata.

Pero cuando se habla de otros tipos de contenidos como políticos o violentos, los límites no son tan claros y entran otras variables, como el contexto y la cultura, que hacen que verificar ese contenido pueda ser más complicado.

3. Se pregunta a Carlos Humberto Ruíz ¿cuáles son los problemas que actualmente justifican regulaciones de bloqueos de contenidos en Colombia y cuál es el rol de las autoridades de control?

Actualmente, la ley establece el principio de neutralidad en la red, por lo que, en principio, no hay restricción para el acceso a contenido por parte de los usuarios. Asimismo, estipula que las empresas que ofrecen paquetes para acceder a internet pueden diseñar soluciones a la medida, lo cual no se entiende como una restricción, y dispone que lo único que en principio tiene la posibilidad de ser bloqueado es lo que tiene que ver con material de abuso sexual infantil, por ello, las empresas que proveen



este servicio, tienen la obligación de llevar a cabo el bloqueo de las URL que tienen ese tipo de contenido.

En la práctica, el Ministerio, para constatar el cumplimiento de esas obligaciones por parte de las empresas, hace unas visitas de verificación periódicamente, y corrobora que esté restringido el acceso al listado que hace la DIJIN con el apoyo de algunas ONG que participan en este tema, el cual es de conocimiento únicamente de las empresas que proveen este servicio, para evitar que todo el mundo lo conozca y cambie las direcciones. Se verifica que se esté cumpliendo ese bloqueo, y en caso de no ser así, a los proveedores de internet se les inician procesos administrativos de sanción.

En ese contexto, para responder la pregunta, considera el ponente que hay que velar por la protección de los derechos de los niños, de los menores de edad, la protección de otros derechos como el buen nombre, la libertad de empresa, y todo esto teniendo en cuenta que el motivo principal del bloqueo es evitar que el acceso a internet se utilice para fines que afecten esos derechos de las personas.

El rol de las autoridades en cuanto a la vigilancia y control en este tema, es verificar que las órdenes que se den, bien sea en la ley o por las autoridades que tienen facultades jurisdiccionales, en efecto se cumplan por quienes tienen la obligación de hacerlo.

Es preciso tener en cuenta las particularidades del sector TIC, que implican, por un lado, la red, los cacharros, los que proveen el acceso, los que tienen la infraestructura, y por otro lado, el contenido. En ese sentido, tenemos claras las reglas en el primer escenario, pero respecto al segundo vale la pena profundizar más.

4. Se pregunta a Andrés Vélez ¿cuál es el rol de la sociedad civil en el proceso de bloqueo y, particularmente, en el tema de material de abuso sexual infantil? ¿Este proceso incluye alguna evaluación y mitigación de riesgos, como por ejemplo evitar censura?

Es pertinente, en primer lugar, señalar que a lo largo de la historia no hubo conciencia de los derechos de los niños y adolescentes, ni mayores disposiciones con medidas para protegerlos, y sólo hasta después de la segunda guerra mundial, nació la concepción de los niños y adolescentes como el centro del quehacer público y de la sociedad y, en esa medida, Colombia cumpliendo con ese compromiso, con la Constitución del 91 los puso en el centro, imponiendo una serie de obligaciones sobre los diferentes actores de la sociedad (Estado, la familia y la sociedad civil).

En particular, el ponente hace referencia al rol que ha tenido Red PaPaz como una organización de la sociedad civil que desde hace más de 7 años ha tenido el liderazgo con otras organizaciones, para crear una línea de reporte que cumpla con las funciones asignadas al MinTIC a través de la Ley 679 de 2001, esto es, una línea de reporte de las conductas abominables que pueden ser difundidas en internet.



A RedPapaz le parece importante la generación de una mesa donde se busquen puntos de encuentro con los diferentes actores relevantes en la lucha contra ese flagelo, poniendo de presente que el material de abuso sexual infantil es ante todo es una representación de una persona real menor de 18 años que está siendo víctima de las peores ofensas contra su integridad, constituyendo un delito que trasciende las fronteras. En esa medida, RedPapaz ha creado un esquema y protocolos dentro de los cuales recibe reportes que pueden llegar de ciudadanos colombianos o de personas que están en el territorio, a través de la aplicación, de la página web o de plataformas a las que tienen acceso donde se reporta que determinado contenido es material de abuso sexual infantil. Inmediatamente se tiene conocimiento de ello, RedPaPaz hace una validación, para ello, tiene un equipo capacitado que puede determinar si el material es de ese tipo, y una vez se hace lo constata, se comunica a la DIJIN para que active su protocolo y alimente su listado.

Ahora bien, frente a la segunda pregunta, hay que decir que de los 19.000 URL bloqueados, el 96% corresponden a este tipo de contenido, y para definir si se debe hacer una evaluación para determinar si están siendo muy invasivos, conviene revisar con los actores cuáles son los mecanismos más adecuados para hacer frente a esta problemática.

5. Se pregunta a Diego Acosta: tomando como ejemplo los derechos de autor ¿cuáles son los retos que representa en internet la tensión entre proteger el derecho de autor y la libertad de expresión?

En primer lugar, hay que decir que tanto el derecho de autor como la libertad de expresión son considerados bienes de extrema importancia para los ordenamientos jurídicos a nivel mundial, considerados como derechos humanos y fundamentales.

Puede acontecer que a estos dos derechos o bienes se les vea como incompatibles, sin embargo, dadas estas categorías de derechos humanos y derechos fundamentales, una manera adecuada de mirarlos es desde el punto de vista de la compatibilidad, por lo que deben hacerse esfuerzos tendientes a eso y buscar que ambos puedan mantenerse en el entorno jurídico de un país. En ese sentido, si bien ambos tienen objetivos o fines específicos para proteger, también es necesario ver que los dos tienen un fin en común, y entonces si con la libertad de expresión se busca promover la cultura y el acceso al conocimiento, aunque el derecho de autor pueda verse en algunos casos como un obstáculo para ese fin, otra perspectiva determinaría que en la medida en la que se creen incentivos para la creación de contenidos artísticos y culturales, podría generarse más material de ese tipo para que la libertad de expresión pueda florecer.

Ahora bien, en el tema de la remoción de contenidos de internet, podemos hacer las siguientes precisiones: puede haber casos en los que al eliminar material se dé una censura a la libertad de expresión si no se toman las medidas adecuadas.



Cabe hacer una especial mención a la nueva Directiva europea de derechos de autor (que debe ser transpuesta por su naturaleza jurídica en el orden interno de cada uno de los estados miembros, y por ello no está aun plenamente en vigor), que fija un nuevo estándar para los proveedores de servicios de internet que, en términos generales, señala que aquellos prestadores de servicios que estén almacenando contenidos cargados por sus usuarios y los pongan a disposición de terceros o del público en general, están incurriendo en un acto de comunicación al público y, por esto, se les otorga una responsabilidad por estar inmiscuyéndose desde la óptica del derecho de autor. Esto es contrario a lo que acontecía antes, en donde el solo almacenamiento de contenidos no daba lugar a responsabilidad por derechos de autor. En ese sentido, estos prestadores de servicios van a tener que adoptar una postura más proactiva en comparación con el estado de cosas anterior, y van a tener que tener autorización para poder almacenar contenidos, lo que constituye una carga superior para ellos, aunada al hecho de tener que garantizar la indisponibilidad de contenidos ilícitos, que puede traducirse en tener que implementar tecnologías de filtros de contenidos, lo cual puede generar grandes cargas para los prestadores de servicios y puede llevar a censura, porque estas tecnologías no son totalmente confiables en el estado de tecnología actual, y a su vez, puede afectar la libertad de empresa por ser un tema oneroso para los prestadores de servicios.

Ronda general de pregunta a los panelistas:

La moderadora del debate indica que una de las cosas que más preocupa a las organizaciones de la sociedad civil al hablar de estos temas, es que se den efectivas afectaciones a la libertad de expresión. Por ello, señala que, en la siguiente ronda de preguntas, los panelistas pueden elegir responder una de las siguientes preguntas: ¿Cómo evitar posible censura? ¿Cuáles son ejemplos concretos sobre problemas que afectan a las personas con libertad de expresión, que esté vinculado con limitaciones técnicas?

Para guiar el enfoque de los interrogantes, Botero da un contexto general: en el caso del material de abuso sexual infantil, por ejemplo, en un reciente foro comentaron que en una ocasión, en uno de los listados que llegaba del Ministerio, una de las URL incluidas correspondía al Partido Polo Democrático. Por ello indica la moderadora que puede ser fácil dar una orden y generar un efecto que no es el esperado, que es justamente una de las críticas que ha realizado la Fundación Karisma frente a la metodología de selección de ese contenido de abuso sexual infantil, esto es, que no hay ningún mecanismo de reporte y corrección de un error, como ocurrió en ese caso. Opina Carolina Botero que si bien el sistema que se ha creado para estos asuntos de material infantil ha tenido un desarrollo amplio, hoy en Colombia se bloquea por juegos ilegales con un mecanismo es más sencillo y expedito que el del primer caso, entonces, si estamos generando esos sistemas ¿cómo hacer para que tengan estándares de protección de derechos? ¿Cómo evitar la censura?

1. Emilio Santofimio señala que Telefónica ya ha abordado el tema en múltiples oportunidades, por ejemplo, hace unos años publicaron un Manifiesto Digital que luego relanzaron, en donde propusieron una carta de derechos digitales para los usuarios,



pues es importante analizar el tema de la proporcionalidad de medidas como el bloqueo y ver qué tanto se requieren, pues afectan otro tipo de derechos que son de suma importancia para los ciudadanos. En ese sentido, Telefónica ha establecido que debe no solo propiciar la neutralidad de la red, sino también la neutralidad digital, de manera tal que se permita a los usuarios siempre acceder al contenido de manera transversal y sin limitaciones.

Adicionalmente, teniendo en cuenta esa ponderación de derechos, la empresa considera que ese tipo de medidas –los bloqueos- deben ser siempre una última ratio, es decir, no deben darse fácilmente porque son más los riesgos que se pueden generar, sin que ello quiera decir que, por ejemplo, en temas como abuso sexual de menores, no sean importantes. Pero también se ha visto que en el país actualmente hay una proliferación de autoridades que quieren tener facultades de bloqueo, o que hay autoridades jurisdiccionales o administrativas que en uso de medidas cautelares innominadas establecidas en el CGP, empiezan a tomar decisiones para bloquear contenidos, y esto es peligroso, porque, por la misma naturaleza de las medidas, estas se dan cuando no hay solución definitiva del pleito, y en consecuencia, puede darse un bloqueo de dos años y decidir después que esa medida fue un error.

En cuanto a la segunda pregunta referida al tipo de errores o problemas identificados en estos bloqueos, se han encontrado falencias en la efectividad de los listados, citando un caso, si se bloquea una dirección y si se crea otra similar, ya el contenido no estará bloqueado, y esa situación se da de manera recurrente. Por eso Telefónica cree que el bloqueo debe ir al foco: ¿dónde se están generando ese tipo de contenidos? Para que el bloqueo sea eficaz y efectivo.

Por último, esta empresa considera que hay un riesgo muy importante que es que se puede llegar a ordenar por parte de un juez de la república un bloqueo y este puede afectar un sitio que tiene otro tipo de contenidos que son legítimos o legales, entonces la medida resulta desproporcionada, porque por un contenido que podía bloquearse de otra manera, se estaría restringiendo toda una página que tiene material de naturaleza lícita, y eso podría eventualmente generar más afectación de derechos que garantía de lo que se pretendía proteger.

2. Carlos Humberto Ruíz opina que, como autoridad de vigilancia y control, tienen la obligación de hacer cumplir lo que esté vigente. Por otra parte, opinando como ciudadano, expresa que probablemente haya mejores maneras de hacer las cosas, pero que por ahora lo que hay es una lista de URL relacionadas con material de abuso sexual infantil, que son enlaces deben bloquear los ISP y como Dirección verifican que así sea.

Ahora bien, si bloquear la dirección no es suficiente, como decían otros panelistas, porque se puede cambiar el dominio y seguir compartiendo el contenido, el contraargumento de eso es que el 96% del contenido que consumimos en internet está fuera del país, luego es poco lo que se puede hacer desde aquí, y eso en caso de poder hacer algo, porque como se dijo, si bien en cuanto a la infraestructura y cacharros hay condiciones definidas, la dirección no ejerce vigilancia y control en el



sector de las TIC sobre el contenido de lo que viaja en las redes, solo lo hace en lo relativo a las obligaciones que se tienen por ejemplo en temas de acceso e interconexión, en cuanto a protección del usuario y demás, por eso considera Ruiz que ahí hay retos importantes para asumir.

3. Gabriel Recalde indica que frente a la pregunta de qué se puede hacer para evitar la censura, tomando los ejemplos internacionales, está la idea del puerto seguro, que consiste en decir que los intermediarios de internet no deben ser legalmente responsables por el contenido generado por los usuarios en la medida en la que cumplan ciertas condiciones, que son: 1) que no hayan sido los autores del contenido, es decir, que hayan funcionado solo como medio transmisor del contenido y no como sus editores o generadores, 2) que una vez se les notifique que un contenido es ilegal, procedan a removerlo, aunque se debate en este punto cuándo una notificación es válida y qué autoridad es la que está en capacidad de hacer esto.

Este principio es apoyado porque provee las guías jurídicas y evita temas de censura en casos de intermediarios, dando seguridad jurídica frente a la responsabilidad por estos temas. Varias legislaciones lo han adoptado, como la estadounidense, la brasileña, la panameña, entre otras. En el caso colombiano, si bien no hay una legislación propia que materialice ese principio, sí ha habido fallos judiciales que apuntan en esa dirección.

4. Diego Acosta indicó frente a la pregunta referida al tema de las tecnologías de filtro y cómo estas se pueden implementar con motivo de la entrada en vigor de la Directiva europea que, en primer lugar, el texto de la norma no hace mención explícita de una obligación de usar estas tecnologías, lo que sucede es que dadas las prerrogativas allí establecidas -como garantizar la indisponibilidad de contenidos que hayan sido específicamente definidos por sus titulares de derechos-, muchos dicen la manera de lograrlas es por medio de su uso, tema que se contrapone con lo que el mismo Tribunal Europeo ha establecido en su jurisprudencia, que por un lado ha indicado que el hecho de imponer a un prestador de servicios de internet la carga de establecer una tecnología de filtro, equivale a una obligación de monitoreo que bajo el sistema existente está prohibido porque impone una carga excesivamente onerosa para estos prestadores -lo que va contra la libertad de empresa-; y que por otro lado, bajo el estado actual de desarrollo tecnológico estas tecnologías, no es un mecanismo totalmente fiable dado el alto número de datos que manejan los prestadores de servicio, por lo que sería muy fácil que se incurriera en el error de que se evite la carga de contenidos que son autorizados o se suban contenidos ilícitos.

5. Andrés Vélez hace referencia al reconocimiento de la importancia del internet dentro de la sociedad, del principio de neutralidad como elemento para asegurar el libre tráfico de ideas y de la importancia de garantizar la libertad de expresión en el sistema democrático. Sin embargo, expresa que es necesario hacer unas precisiones: en primer lugar, indica que hay ciertos eventos que constituyen excepciones a esos principios, el caso específico del material de abuso sexual infantil es uno de ellos, pues ahí hay un acuerdo internacional (pese a eventualmente haber discrepancias sobre el rango de edad, que en el caso colombiano es claro que el material es delito y ofensivo



para todo menor de 18), así, si bien es límite a la libertad de expresión, es un fenómeno que merece un tratamiento específico, y en nuestro país tenemos las normas para adelantar los bloqueos correspondientes.

Los bloqueos son una medida importante impiden que personas accedan a los contenidos, y si bien hay otros mecanismos para hacer trampa a eso, es una forma de prevención de acceso porque el solo material supone una ofensa y una forma de afectar derechos de esta población sujeta a especial protección constitucional. Por ello, debe haber protocolos de desmote que sean efectivos y debemos estar en capacidad de cumplirlos como país.

En Colombia, se está bloqueando el contenido y al mismo tiempo se está informando a las autoridades de origen en el lugar donde se encuentra alojado ese material, para adelantar los trámites correspondientes. Por último, hay que decir que se tienen compromisos internacionales en esta materia, y hay que recordar que estos tienen un estatus específico por tratarse de este tipo de conductas.

Carlos Humberto Ruíz interviene en este punto, para resaltar que hay una diferencia entre lo que se entiende por mayoría de edad: indicó que en Colombia que son los 18 años, pese que a otros establecen que es de los 16, luego el país es más protector en ese sentido. Señaló también que una cosa es perseguir al que provee el acceso a internet que, en algunos casos, en palabras coloquiales es el que menos velas tiene en este entierro, y otra cosa es el delito en sí mismo, para lo que hay autoridades en el país encargadas de investigar y sancionar esas conductas.

Así, las empresas que proveen el acceso a internet en el marco de la legalidad deben ser diligentes en cuanto al cumplimiento de las normas, y de no serlo, tienen consecuencias, pero otro tema es evaluar la culpabilidad de una persona. El Ministerio en sus funciones hace especial énfasis en la prevención, en este momento está realizando una campaña para que las empresas sepan cuáles son las obligaciones que tienen que cumplir según la Ley 679 de 2001, en temas de bloqueo, obligación de información a sus usuarios, entre otros puntos, para incrementar el nivel de cumplimiento de estas normas.

Preguntas de la audiencia:

Se realizó una ronda general de preguntas, donde los asistentes al Foro plantearon los siguientes interrogantes:

1. En cuanto a la responsabilidad por el contenido, este es de quien lo emite y de quien lo crea, pero también existen ciertas responsabilidades indirectas, por ejemplo, en el caso de abuso sexual, los proveedores de servicio deben tener una responsabilidad demostrada frente a qué se está haciendo para prevenir esta situación y cómo ayudan en la investigación. Entonces la pregunta dirigida a los operadores es: ¿qué hacen para evitar que estas situaciones se den o para ayudar a la justicia?
2. Es claro que el derecho a la libertad de expresión no es absoluto y tiene limitaciones como el abuso sexual infantil u otro tipo de contenidos, donde en el caso concreto se



determina cuál es el derecho que prima. La pregunta es: ¿de qué otra forma se puede garantizar el derecho a la libertad de expresión cuando está involucrado otro tipo de actor como un funcionario de gobierno? Por ejemplo, en que un funcionario público que bloquee a un usuario de Twitter por sus comentarios ¿qué instrumentos jurídicos y técnicos (como verificación de perfiles) podría haber para evitar este tipo de prácticas?

3. Pregunta dirigida a Carlos Ruíz: en una emisora comunitaria hicieron una denuncia anónima, eso no es prohibido, pero puede dañar la imagen de una emisora ¿qué debe hacerse ahí?

4. Para ISOC, el bloqueo debe ser la última medida y debe ser proporcional, para no violar los derechos a la libertad de expresión y de información. Internet no es solo la IP, hay otros actores como quienes alojan el contenido, donde debe atacarse inicialmente. Una vez se hace el bloqueo, se genera una falsa sensación de seguridad, como si el delito no se fuera a volver a cometer. El único consenso internacional que hay es sobre pornografía infantil, pero cada vez los países realizan más bloqueos, en el congreso se está tramitando una ley de seguridad ciudadana que propone de bloqueos preventivos en caso de suspensión en un proceso jurídico, eso es peligroso y se insiste en que esta debe ser la última medida, por eso se invita a reflexionar al respecto.

Respuestas de los panelistas:

1. Emilio Santofimio indicó que este es un fenómeno de *multistakeholders*, donde la responsabilidad puede estar varios agentes y, aunque se entiende que la función de vigilancia y control es la de cumplir la ley, y si bien hay un principio de territorialidad de las normas, que la responsabilidad recaiga exclusivamente sobre el ISP porque tiene una autoridad de control parece excesivo y no es lo ideal.

Frente a la primera pregunta, indica que Telefónica como compañía ha participado activamente en la protección de los derechos de los menores, tienen una Fundación que además trabaja constantemente en políticas de protección de menores para enseñarlos a desarrollar sus derechos de forma debida en el mundo digital y a realizar una apropiación de este de la mejor forma, mediante un uso responsable. Adicionalmente, indica que la compañía tiene unas políticas de seguridad donde se relacionan cuáles son las condiciones de bloqueo y eso está a disposición del público, y señala que hay una normativa que lleva siempre a generar un cumplimiento adicional que es verificado por las autoridades de vigilancia y control, y que cada que llega una orden judicial esta es acatada, pues hay una dirección en la empresa dedicada únicamente a eso.

Un punto adicional se relaciona con los proyectos de ley, porque ahora, como se mencionó, gran parte de las autoridades quieren tener la facultad de bloquear contenido -lo cual es excesivo-, partiendo de la premisa de que es lo más sencillo, aunque en realidad eso genera una falsa sensación de seguridad que no ataca la fuente del delito.



2. Gabriel Recalde indica que Google no permite material sexual infantil, por lo que proactivamente cada vez que se identifica que alguien está compartiendo este tipo de contenido a través de sus plataformas, se remueve y se copia a las autoridades para hacer las investigaciones pertinentes, además de eso, como compañía trabajan en soluciones técnicas y tecnológicas para que eso no se pueda subir, y tienen un programa educativo para prevenir que haya víctimas de ese delito.

3. La moderadora señala que es preciso observar cómo en el caso del material de abuso sexual infantil hay un consenso al respecto y una respuesta rápida que no se da en casos como el de abuso a mujeres que, solo por no ser menores de 18 años, puede ser un proceso más complicado. Indica que no siempre la solución debe ser bloquear y resalta la importancia de iniciativas de las ONG como Karisma, que tiene un proyecto con organizaciones de otros países llamado Acoso Online, donde se ha intentado revisar la legislación que existe en otros Estados para atacar estos casos, porque a veces está la falsa idea de que hay que salir a legislar y no siempre es cierto, muchas veces existen herramientas del ordenamiento jurídico ya existente que pueden usarse, y es un reto en el que deben trabajar jueces y abogados.

En cuanto a la pregunta relacionada con Twitter, Botero precisa que se han dado varias decisiones al respecto en diferentes jurisdicciones, referidas a que un político no puede bloquear a los usuarios por ser figuras públicas, no obstante, en Colombia no hay decisiones en ese sentido todavía. Personalmente, cree que puede ser una determinación exagerada y que podría darse una decisión en ese sentido solo si la persona únicamente usa su cuenta de Twitter para efectos relacionados con su cargo (y no como una cuenta personal) y si no hay otra vía para llegar a esa información.

4. Carlos Humberto Ruíz señala que la definición del bloqueo de las URL relacionadas con abuso sexual infantil tiene su fuente en la ley. Indica, por otra parte, que en lo que tiene que ver con el incumplimiento de las obligaciones legales o reglamentarias y regulatorias a cargo de los vigilados cuando hay procesos administrativos de investigación, se garantiza siempre el debido proceso y hay etapas donde los investigados tienen la posibilidad de probar su inocencia.

En el caso de las denuncias anónimas, cualquier situación que sea puesta de presente por un ciudadano, sea a título personal, de empresa o de manera anónima, debe ser tratada por la autoridad de vigilancia y control encargada.

2:30 p.m – 4:00 p.m

Retos del trabajo en la Era Digital

Universidad El Rosario

Panelistas:

- Ramón Alfredo Aguilar. Asesor de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT). Gobierno.
- Mery Laura Perdomo Ospina. Miembro del equipo asesor de la Red Global ILAW, asesora sindical y de trabajadores.
- Sonia García. Asesora en la Alcaldía Mayor de Bogotá para la implementación del plan distrital de Teletrabajo en Bogotá y Subdirectora en DH Innovación Digital
- Iván Daniel Jaramillo. Profesor de carrera académica de la Universidad del Rosario. Academia.

Relatoría: *Luis Miguel Guevara*

Para esta sesión los panelistas invitados fueron Iván Jaramillo (Profesor de la U Rosario), Ramón Aguilar (Abogado), Sonia García (Fundadora de Teleworker) y Mery Perdomo (abogada de la central de trabajadores), a ellos se les envió antes del foro unas preguntas con respecto al tema de trabajos que ofrecen plataformas tecnológicas, ellos según su experiencia responden las preguntas que estaban preparadas y las que el público les hace según lo expuesto, las opiniones de los panelistas eran variadas y esto ayudó a que la información fuera más completa para tener una visión más amplia.

1. Cuando se habla actividades como la de Uber y Rappi se habla de servicios electrónicos de intermediación o actividad de transporte de personas o de bienes, ¿Cuáles son las consecuencias de llamarlo de una manera o de otra?

Mery abrió el debate aclarando que el trabajo digital varía mucho dependiendo la plataforma, y que independientemente sea la plataforma que sea, presta un servicio, con un trabajador que utiliza la app para ganar dinero para él y para la plataforma, el cómo se nombra pasaría a un segundo plano teniendo en cuenta que la persona y la plataforma constituyen una relación de trabajo.

Sonia se mostró alejada a esta respuesta, afirmando que la persona que utiliza la plataforma es una persona independiente que hace uso de la plataforma para darle cumplimiento a ese servicio que el usuario solicita, y que la relación de dependencia no se da ya que no hay un contrato inicial, sino que es un intermediario que ayuda al trabajador a comunicarse con los usuarios.

Ramón añadió que hay muchas plataformas y muchos oficios que se prestan a través de estas, la implicaciones que tiene el llamarlo de una forma u otra es que cada sector tiene su regulación, la tecnología no se puede regular ya que esta siempre cambia, la regulación se le debe hacer al usuario que utiliza la plataforma.

Ivan dijo basándose en un fallo de la unión europea donde reconocen a Uber como un servicio de transporte y no como un intermediario, que el tema es de carácter global, el reto nuestro es garantizar los derechos de la persona que se encuentra realizando el modelo de trabajo digital, “El trabajo no es una mercancía” añadió.



2. ¿En su criterio los trabajadores de Uber y Rappi son trabajadores en el sentido jurídico del término? ¿Qué implicaciones prácticas conlleva considerarlos trabajadores y en caso negativo con qué término podríamos referirnos a ellos?

Sonia se denomina trabajador al que tiene un trabajo como empleado, pero también al que es independiente porque está recibiendo remuneración por estar ocupado en una actividad, por lo cual lo que se quiere es trabajar con ellos para que puedan tener un acceso a las prestaciones sociales y así formalizar la forma de trabajo con el trabajador.

Ramón la constitución garantiza la protección del trabajo en todas sus modalidades y que hay libertad de escoger la profesión u oficio, en base a eso en este caso no existe una sola modalidad de trabajo y tienen la facilidad de cambiar de plataforma, el enfoque según el código sustantivo del trabajo es la protección del trabajador y esto se representa en la seguridad social que le brinda el estado con sus leyes para que se cumpla, el código sustantivo es muy exigente para categorizar la figura del trabajador, señaló que la prestación personal de servicio, remuneración y subordinación hacen parte de la categorización, donde la subordinación juega un papel importante ya que tiene que durar durante toda la prestación del servicio, así que en este caso los trabajadores que prestan el servicio son independientes ya que pueden escoger la plataforma, el horario, si quiere aceptar el servicio.

Iván afirmó que Uber en este caso tiene un control del servicio y del trabajador porque hace por medio de preguntas y acciones al usuario un control del trabajador que presta el servicio, así que no se puede llamar independiente al que tiene una subordinación directa mientras presta el servicio, además si no cumple, el despido se efectúa con bloqueo en la aplicación lo que dejaría al trabajador indefenso

Mery según el código sustantivo del trabajo es obsoleto en estas nuevas formas de trabajo, así que define que el trabajador no siempre debe tener un contrato de trabajo, los criterios son relativos para poder considerar a una persona como trabajador, pero lo que es claro es que en este caso los trabajadores hacen parte de una plataforma que es la que les ofrece el empleo y por lo tanto ellos deben garantizar el bienestar de sus trabajadores.

3. Todos están de acuerdo que el trabajador merece un mínimo de dignidad, ¿dependiendo de su posición como garantizarían ese mínimo de dignidad?

Ramón El trabajador pone las herramientas de trabajo, en este caso al ser independiente paga más prestaciones sociales y por ende la regulación afectaría el bolsillo de esa persona que presta el servicio y no beneficiaría al trabajador, lo ideal sería adaptar las leyes al modelo de trabajo para que se garantice sus prestaciones sociales.

Iván complementó diciendo que según una encuesta realizada por unos estudiantes el 85% del ingreso que ganan los trabajadores de plataforma es su única fuente de ingreso, y que en este orden de ideas el despido con un clic viola toda la teoría contra el despido que se ha hablado, hay que buscar una forma de encuadramiento que permita el trabajo decente.



Mery denomina a los trabajadores como precariado, esto ya que no tienen todavía ninguna prestación social, añade que las garantías se las tiene que dar el estado, y las plataformas que están ganando dinero por medio del trabajo de estas personas.

Sonia van surgiendo oportunidades laborales gracias a estas plataformas y la idea es que se ajuste la legislación para que haya equilibrio dentro de lo justo si hay ganancias de por medio.

Preguntas o intervenciones de la audiencia

¿Cómo se puede comparar el trabajo de un trabajador de Uber que puede elegir el día que trabaja a un profesor que tiene que cumplir un horario?

Iván Por supuesto no es igual pero se evidencia que en la plataforma hay un control del servicio que obliga al trabajador a cumplir con ciertos parámetros.

Mery no estoy de acuerdo que el trabajo tenga que ser explícitamente 8 horas, sino que puede existir el modelo de trabajo en el cual el trabajador pueda opinar con respecto a sus derechos para que se pueda autorregular sus derechos.

4. ¿Cómo se puede hacer una política pública con una cifra de 300 personas si Uber tiene más de 80 mil conductores?

Iván No pretende ser el parámetro de medición ya que es una encuesta hecha por estudiantes, es un aporte académico para poder caracterizar de a poco para darle derechos al trabajador, la intención era tener un primer paso de datos para poder avanzar en cómo se puede hacer para limitar la jornada en este contexto.

¿En el caso de que se regule los derechos (Prestaciones sociales) de las personas como se hace si trabajan en varias plataformas?

Mery un trabajador puede tener varios contratos de trabajo concurrentes, coexistencia de trabajo y contribuir al modelo de trabajo de cada uno.

4:30 p.m – 6:00 p.m

¿Es necesaria una reforma a la Ley de Protección de Datos Personales?

Youth Observatory y Capítulo de ISOC Colombia

Moderador: Felipe Tovar. Profesor de la Universidad Externado y del Rosario.

Ponentes:

- Doctora Sol Beatriz Calle D´Aleman: Docente e Investigadora del Departamento de Derecho Informático de la Universidad Externado de Colombia.
- Doctor Daniel Castaño: Abogado de la Universidad Externado de Colombia. Magister en Derecho (LLM) y Doctor en Derecho (JSD) por la University of California – Berkeley
- Ingeniero Julián Gómez Pineda: Ingeniero Eléctrico y Físico de la Universidad de Los Andes, Socio fundador de Tachyon Consultores S.A.S, especializada en el sector de Telecomunicaciones

Relatoría: *Laura Victoria Ramos Guevara*

Felipe Tovar, como moderador, dio la bienvenida a los panelistas y agradeció su participación. Explicó que la metodología del panel fue diseñada de manera diferente a la anterior, ya que se propuso la pregunta general del título del panel (¿Es necesaria una reforma a la Ley de Protección de Datos Personales?) y cada experto expone su respuesta según su postura para, posteriormente, realizar un debate y concluir con preguntas del público.

Posteriormente procedió a presentar los como expertos en Temas de Protección de Datos Personales Doctora Sol Beatriz Calle D´Aleman; Doctor Daniel Castaño y Julián Gómez Pineda.

Como moderador, Felipe Tovar, afirmó que los organizadores propusieron un tema actual: La protección de los Datos Personales, estamos en el mundo de la tecnología y el acceso infinito a Internet, lo que ocurre en el mundo puede tener presencia en la red de redes. La omnipresencia del internet en la vida, genera unos retos importantes para los derechos: Privacidad, buen nombre, Derecho a la información, constitucionalmente protegidos en el país.

Dichos derechos, han tenido un desarrollo legal, jurisprudencial y doctrinario que los han nutrido y protegido en los últimos años. Sin embargo, es importante que en Foros académicos, como en presente, se analice: ¿Cuáles han sido los avances de esa regulación para proteger los Derechos de Datos personales? y evaluar si se está en un punto en dónde se requiere una mejora o, por el contrario, se está a la altura de las mejores legislaciones.

Actualmente, la Comunidad Económica Europea, reformuló su política en temas de Protección a los Datos Personales y por ejemplo, por parte de éste foro, podría examinarse si de alguna manera, nuestra legislación está a la altura o deben hacerse modificaciones correspondientes para llegar a su nivel.

La tecnología cada día genera nuevos retos como en el Internet de las cosas, que genera información a gran escala, sobre datos que habrá preguntarse si son



personales o no, y si están protegidos por la legislación. El Blockchain, nueva tecnología que aparentemente va a “arrollar” a todos los abogados desplazándolos de su trabajo, generando un reto en materia laboral. En fin, hay una serie de avances tecnológicos que se deben incorporar a la sociedad ya que necesariamente ayudan a mejorar la calidad de vida de las personas.

Debe existir el principio de confiabilidad en la red de Internet, además, una legitimidad que garantice la protección a los Derechos dentro de ese entorno. Por eso se realizó la invitación a estos tres panelistas para que aborden diferentes campos: Técnico, jurídico y política pública.

Se le otorgó la palabra al Ingeniero Julián Gómez, quien afirmó que los datos se están convirtiendo en una enorme creación en la economía, la revista *The Economist* en la edición del 6 de mayo del 2017 dijo: “El recurso más valioso del mundo, ya no es el petróleo sino los Datos Personales”. Hay que observar dentro de las 10 compañías más valiosas del mundo, hay 7 que se fundamentan en los datos (Amazon, Microsoft, Alphabet, Apple, Facebook, y Alibabá), construidos a partir de la información que la gente le otorga a las plataformas, son unos mecanismos importantes de creación de valor que parten desde la generación de los datos por personas, dispositivos y en el futuro por el internet de las cosas.

Si hay millones de dispositivos enviando información, y esta se puede asociar con las personas, es un volumen inmenso de datos que va a ser utilizado por alguien con un propósito económico, esa generación de información pasa por redes interconectadas, convirtiéndose en conocimiento almacenado en bases de datos que se pueden visualizar y estar distribuidas en cualquier parte del mundo y a partir de ese almacenamiento se pueden generar productos, aplicaciones, servicios o cualquier actividad de inteligencia artificial.

A partir de lo anterior, la inteligencia artificial aprende según los datos otorgados por los usuarios, esos algoritmos generan también un valor agregado para las ciudades, la educación, para la modernización de los servicios públicos, redes eléctricas, servicios financieros y creación de dinero digital. Es positivo, porque genera la creación de empresas, por otro lado, esta gran base de datos debe pertenecerle a sus titulares: las personas, es el centro de lo que se tiene que reconocer en cualquier sistema de protección de datos personales.

Es importante exigirle transparencia a las empresas y gobiernos respecto a la información que tienen y cómo la usan; en el caso del segundo es crítico, por ejemplo: China implementó el reconocimiento facial para hacer transacciones diarias, pero además, ha permitido reconocer emociones, preferencias sexuales de las personas, esto lo realiza mediante la implementación de millones de cámaras, instalándolas en regiones de China alejadas (Tibet).

Las leyes de protección de Datos Personales, se conecta directamente con la ciberseguridad ya que si las empresas o gobiernos se han encargado de hacer el



tratamiento de datos personales, no están obligados a revelar la brecha de información que tienen, y por lo tanto, los propietarios de los datos no saben su destinación o si en realidad se protegen.

Los principios de neutralidad en la red y la posibilidad que tienen las personas, en un escenario de Internet abierto, de acceder a la información que deseen y para que no haya un tráfico de datos diferenciado de los proveedores de servicios o que sea discriminatorio.

El moderador cedió la palabra a la Doctora Sol Beatríz Calle D´Aleman que presentó algunos aspectos de una posible reforma a la legislación colombiana en materia de Protección de Datos. Afirmó que escuchando la intervención del Ingeniero Julián, pensó en la película “1984” de George Orwell, en dónde planteaba el Big Brother, ese Gran Hermano que es el Estado, capaz de invadir y controlar los pensamientos de los ciudadanos. Justamente el Internet de las cosas nos plantea a lo largo de los años, son premoniciones que puede que se hagan realidad, ya no en cabeza del Gran Hermano, sino el “pequeño Gran Hermano” en el que el individuo se ha convertido.

Desde la perspectiva anterior, se van a encontrar unas normas de protección de datos personales que van a responder a lo que la Corte desde hace muchos años ha identificado como el poder informático, es decir, el poder y la capacidad de la tecnología de invadir otros derechos (como el derecho fundamental a la intimidad, habeas data y protección a los datos personales).

¿Es conveniente hacer una reforma a estas normas?, la Doctora plantea otra pregunta: ¿sobre qué se haría esa reforma? Hay una vía principal que plantea: Si las normas estatutarias que plantean Derechos Fundamentales son efectivas si se realizan diferentes reformas.

El país ha presentado proyectos de ley que reforman lo anterior (Ley 1266 de Habeas Data Financiero, Norma General de Protección de Datos 1581). Cuando se habla de la reforma en la norma estatutaria se habla si se tratan de asuntos que tienen que ver con la política – Estado en relación con la norma, al mismo tiempo pensar, si las reformas que se plantean, tienen que ver con la conducta de los vigilados dentro del Estado; lo anterior da paso a dos respuestas diferentes:

1. Ley 1581, reforma proyecto de ley 089 del 2017 y hay aspectos de Ley que la Doctora afirma, que requieren una reforma ya que la ley no las provee, quizá el más importante y lo intentó la Superintendencia de Industria y Comercio dos veces: ampliar la facultad de la autoridad de control de poder intervenir empresas, que, sin estar en territorio colombiano, tratasen datos de residentes colombianos, a través de internet o cualquier otro medio. Este aspecto necesita ser reformado en Colombia, es aspecto legal que no se tiene.
2. Aplicación de la Ley colombiana en virtud de un contrato, para que las autoridades puedan investigar y llegar a terceros, pero el contrato es una ley



para las partes, surge la pregunta: ¿Si el mismo contrato lo contempla, será un acuerdo privado que podría desconocerse por la autoridad?, la Doctora cree que no.

La garantía de tratamiento por defecto, el diseño de la privacidad, principio de responsabilidad demostrada, principio de proporcionalidad se puede encontrar en el proyecto de ley anteriormente mencionado son temas nuevos en el GDPR.

Si evaluamos temas como la evaluación del impacto de la privacidad, la pregunta que surge es: ¿Por qué tendrían que reformar una norma Estatutaria, para que nuestras empresas o instituciones públicas o privadas cumplan con un asunto que hace parte de su vigencia? ¿Por qué a emprendedores que desarrollan las nuevas Apps, tienen que tener en el diseño de su producto una política de ciberseguridad? ¿No se le podría exigir responsabilidad civil a estos desarrolladores por la seguridad de sus plataformas o producto defectuoso?

La Ley 1266 del año 2008 de Habeas Data Financiero, causa curiosidad este proyecto de ley porque propone enderezar algunas malas prácticas en el Sector financiero, porque cuando la norma quería, por ejemplo, que se requería un tiempo previo para poder notificar el reporte en mora de un ciudadano, las entidades entendieron que solamente bastaba con enviar el extracto del aviso mes a mes del reporte en mora si no está al día con su obligación; entonces se tuvo que presentar éste proyecto de ley, con todos los cambios legislativos, que afirma que no es una comunicación previa, es una notificación, y tiene que seguir los mismo parámetros que la notificación judicial.

El tema del reporte de la información negativa, muchos gremios financieros, afirman que el proyecto de ley dice que las obligaciones que ascienden al 20% de 1 SMMLV, no se puede reportar al ciudadano en mora, ya que hay unos reportados en centrales de riesgo 15 años porque debían sumas muy pequeñas. Lo que dice el sector es que lo anterior no es viable porque no se sanciona a estas personas y pueden seguir debiendo sumas pequeñas.

Además, el tema de que los ciudadanos consultan de manera reiterada en las bases de datos crediticias, bajan el score que tienen los bancos. El proyecto de ley dice que lo anterior no tiene mucho sentido porque de allí no se puede establecer un rasgo de comportamiento crediticio. Cuando se analizan estas reformas de normas estatutarias hay temas gruesos de políticas de Estado como la facultad de la Superintendencia para poner vigilar a los terceros (en el escenario anterior), vienen a enderezar prácticas empresariales. Pero, ¿Será necesario reformar normas de carácter estatutario para que las empresas y el gobierno tengan responsabilidad social y empresarial?

La Guía de Responsabilidad Demostrada, la jurisprudencia de la Corte y lo existente en materia de Protección de Datos, muchos de estos temas existen en la legislación colombiana, otro asunto, es que la voluntad política de la autoridad de control, de



aplicarlo efectivamente y la otra de que este sea un asunto de respeto por el derecho de las personas y ser competitivo en el siglo XXI.

Dichas entidades deben comprender que los usuarios deben tener la propiedad y la capacidad de disponer sobre sus datos personales, incluso de monetizarlos si así lo desean, es decir, la importancia de disponer libremente sobre su derecho.

El Moderador sede la palabra al Doctor Daniel Castaño, quien indicó que se habla de una necesidad de hablar sobre una reforma a la Ley de Protección de datos o a la Gobernanza de los datos (hablando de manera global) pero, ¿para qué? ¿Realmente tenemos que reformar? ¿Lo que tenemos hoy en día es suficiente para permitir la innovación y al mismo tiempo, defender los Derechos Fundamentales de los usuarios?

Por lo anterior, el doctor Castaño, dividió su presentación en tres partes:

1. Retos que imponen las nuevas tecnologías enfocado en la inteligencia artificial.

El principal reto de la inteligencia artificial es entender lo que el ser humano piensa y hacer que haga cosas que de otra forma, no haría. Si se traduce eso en temas éticos, el reto está sobre la autonomía de la persona, ya que hay millones de equipos que rodean a las personas en cada momento de su día y algoritmos con la capacidad de descifrar los pensamientos y direccionar nuestras acciones.

¿Realmente con la reforma a la Ley de Protección de Datos, podrán prevenir que los gigantes de la tecnología y los gobiernos, tengan la capacidad de hackear a las personas? El doctor afirma que no, ya que aunque las personas tengan información sobre el tratamiento de sus datos igual lo otorgan para hacer otras cosas que en otro escenario, no harían.

2. ¿La regulación actual es suficiente para los retos que propone la inteligencia artificial? Se puede apoyar en el GDPR en materia al Derecho, por ejemplo, a tener una explicación sobre la decisión de una máquina automatizada, pero esto. ¿Impediría que los gigantes empresarios o los gobiernos dejen de realizar dichas prácticas? No, ya que son temas muy sensibles, basta con un consentimiento ambiguo del usuario. Esto puede hacernos reflexionar sobre si esa nueva regulación, va a ser eficiente y si tiene un costo – beneficio, además si realmente los incentivos para hacer viable las normas son menores que los costos.
3. ¿Qué puede hacerse para producir una regulación que sea eficiente en costo – beneficio, que tenga un impacto y prevenga e impida esa habilidad que tienen los gigantes tecnológicos y los Gobiernos de hackear a los usuarios?

Hay que entender la tecnología, porque hay posturas de ciertos grupos que están a favor de la reforma, por ejemplo, en materia de Inteligencia artificial, afirman que se tiene que regular los metadatos de la inteligencia artificial, pero en realidad no se conoce este concepto o no se sabe cómo explicarlo ¿Cómo se puede regular algo así?



Además, es necesario explicar por qué esta tecnología es beneficiosa para la sociedad e identificar modelos de riesgos para establecer en que dilema regulatorio nos posicionamos y plantear soluciones.

El doctor plantea su temor por la expedición del CONPES y su ley de Inteligencia Artificial para Colombia, en términos de competitividad, puede ser un riesgo para la innovación. Hay que buscar el camino regulatorio: leyes estatales, auto-regulación o mecanismos de co-regulación y en medio de la identificación de esa estrategia regulatoria para que cumpla los fines perseguidos y promueva las buenas prácticas, con el objetivo principal de cumplir la ética digital.

En conclusión hay que tener en cuenta que no tenemos que tener esa cultura de regular todos los aspectos nuevos, puede tomarse el GDPR, pero de manera acorde e interpretarlo según nuestra realidad.

Posteriormente, el moderador puso en la mesa el tema institucional, dijo que no es muy clara la necesidad de una reforma, por lo menos, no en los términos que se ha venido proponiendo, ya que es más superficial que de fondo. Preguntó a los panelistas: ¿Sea con la norma actual o con una reforma más de fondo sobre alguno de los temas que propuso la Doctora Sol, se debe hacer una reforma institucional de nuestro sistema? Hay países que han creado figuras independientes, autónomas y especializadas que trabajan sobre las bases de datos, es viable la creación que se encargue y tenga la capacidad de enfrentar estos problemas con la normativa actual o con una legislación modificada?

La Doctora Sol afirmó que una cosa es la regulación de la tecnología y otra cosa es la regulación de los derechos. Cuando se habla de la protección de datos y de la privacidad, se habla de la regulación de los derechos que va existir siempre. Pero si se habla de la institucionalidad que requiere hoy mayores potestades como la instauración de una autoridad de control de defender a los ciudadanos, ya que si la tecnología, realmente va a ser tan arrolladora, el Estado, en esa lógica puede desaparecer.

Otro asunto es, que se plantee la regulación de la tecnología, pero imposible regularlo por los avances diarios. Lo que se puede regular son los efectos que tiene la tecnología sobre los derechos de las personas, ya que finalmente, es la posibilidad de que el Estado garantice que el usuario conozca los riesgos de la inteligencia artificial en el tratamiento de la información y la penetración de la intimidad o de negarse a otorgar los datos.

El aspecto institucional que se requiere es que el Estado sea el Baluarte de la defensa de los derechos y quien lo garantiza, es además, la capacidad de que puedan tomar cartas en el asunto sobre las actuaciones de los gigantes de Internet y los gobiernos.

El Doctor Daniel Castaño, afirmó que cree que debe haber una consonancia de los efectos jurídicos de la tecnología y la tecnología, ese balance lo ha encontrado el



GDPR con base en la ambigüedad del lenguaje y su manera de interpretarla. Además, realizó una crítica sobre la organización del Sector TIC ya que sus funciones están regadas en varias instituciones, ya que hay un Ministerio que sanciona y crea política limitada y una SIC que tiene unas súper competencias y le han agregado otras por medio de diferentes leyes; por eso, es necesario pensar en una autoridad política independiente, ya que el que gobierna nos datos, gobernará de manera general. Por lo tanto no tiene que tener una tendencia política sino técnica.

El Ingeniero Julián Gómez Pineda, coincidió que el tema relevante es la protección de los derechos, dijo que lo que se requiere es proteger a los consumidores de redes y servicios de comunicaciones y tecnologías de la información y comunicaciones, en un ambiente de economía digital, en dónde la protección de los datos personales es un elemento importante pero no el único, ya que se tiene que garantizar su titularidad, privacidad y protección. Que se autorice y limite el uso de los tratamientos de los datos personales y su circulación. Y por otro lado, es importante la protección de los datos de los usuarios y garantizar los derechos básicos, sin entrar a regular la tecnología, pero garantizando mecanismos que protejan la información.

Por otro lado, el surgimiento de la Inteligencia Artificial es un tema delicado porque tiene sesgo, ya que es creado por lo humanos y su aprendizaje es basado en lo anterior, por lo tanto tiende a equivocarse. Estos sistemas no son objetivos.

Es necesario aplicar también, el principio de extraterritorialidad en materia de bases de datos, ya que la gran mayoría no se encuentran administrados en el territorio nacional, entonces si no construimos una legislación más global, no tendremos el espacio de aplicación ya que si no se da, puede llegar a un tema complicado del cierre de Internet para que los países garanticen realmente la protección de los datos de sus ciudadanos,

Por último, hay que resaltar que está en juego más que la protección de los consumidores, los principios de libertad, por eso es que hay que limitar a las grandes compañías y al Estado para que no usen la tecnología para controlar la vida personal de sus ciudadanos (Caso China).

El Moderador da la palabra a las preguntas de los asistentes:

Asistente: Afirmó que estamos en una era de hiperconexión en dónde existe una gran cantidad de datos, incluso en dispositivos domésticos ¿Sería adecuado hablar de una regulación para este tipo de dispositivos personales, incluso teléfonos móviles?

La Doctora Sol, respondió que ya existe, incluso la norma de protección de datos, aunque excluye las bases de datos que llaman “de carácter doméstico”, establece que si tienen uso estrictamente personal o doméstico, tienen un principio de seguridad para la protección de estos datos, pero el mundo va a tal avance, que cree que tiene que existir una fomentación de cultura de la seguridad de los datos para que la gente



tenga más consciencia del uso que se le da. Hay cierto aspecto cultural de educación que debe ser el eje central, además de la ética.

El Doctor Daniel responde profundizando en el tema de la educación, afirmando que es incluso más efectiva que la imposición de leyes. La Unión Europea en los lineamientos que sacó en Junio pasado sobre “Política pública en materia de Inteligencia Artificial” tiene un capítulo dedicado a esto e invita a la creación de una guía sobre esta materia para enseñarlas en las aulas escolares.

El moderador, hizo énfasis en que uno de los patrocinadores del Foro es RedPaPaz, una fundación que busca precisamente concientizar a los padres de ciertos riesgos y está de acuerdo con los panelistas al informar que los datos personales van más allá del individuo e involucra a todos quienes lo rodean.

Asistente: Introdujo que hay unas Cámaras de Comercio con bases de datos en los que los comerciantes han puesto, de manera voluntaria, sus datos personales quedando en el Registro de Comerciantes. La Cámara de Comercio, posteriormente, comercializa esa base de datos ya que la considera pública. Ella envió un Derecho de Petición en dónde afirmaba que la finalidad del dato es para el conocimiento de la calidad de comerciante ante la Cámara, pero para la comercialización es necesario que se solicite la autorización del dato del titular aunque sea de carácter público,

La Doctora Sol respondió en primer lugar, que el Dato Público no existe, la base de datos no tiene una vocación pública, sigue siendo de carácter personal, desde esa perspectiva, tiene que cumplir con toda la norma de Protección de Datos. En segundo Lugar, afirmó que lo que se les permite a las Cámaras de Comercio no es vender el Dato, ya que si es un dato que el Estado incluye en una base datos con una vocación Pública para publicitar la condición de un comerciante, pues en efecto, el dato no se puede vender. Lo que permite el cobro de un dinero, es el valor agregado es el servicio de organización de la información para una consulta más fácil, pero la compraventa no es aplicable a las bases de datos. Se entenderían como contratos de licencia de uso de información de los comerciantes.

El Ingeniero Julián responde sobre el tema de propiedad intelectual, sobre la forma en cómo se estructuró la base de datos de los correos electrónicos y se hace por medio de licencia de protección de datos.

Asistente: La regulación en otras regiones o países, la protección de datos es contundente y da las herramientas a las instituciones u organismos que manejan la protección de datos, de implementar herramientas efectivas para proteger los derechos de los usuarios y de los consumidores de la tecnología de la información, diferente a la realidad colombiana. Ya que la regulación vigente no está aplicando estas herramientas que permiten la normatividad de los usuarios, entonces: ¿Cómo se deberían implementar herramientas, sin cambiar la normatividad, para proteger a los usuarios?



Pregunta técnica: ¿Cómo, desde la perspectiva de los abogados, se podría en Colombia tratarse el tema de libre circulación de datos personales?

El Doctor Daniel respondió conforme a la regulación de la implementación que es una política pública y coordinación de recursos en conformidad con los fines que la misma estipula. Si existen las leyes, hay que construirla entre todos y fomentar las buenas prácticas.

El ingeniero Julián añade que hay que obligar a los que hacen el tratamiento de datos a que si hay una brecha de seguridad, informe a la autoridad competente y al dueño de los datos, ya que hay muchos casos en que hay vulneraciones y no se hace el respectivo aviso, ese tratamiento de datos se puede hacer desde Colombia o desde otro país, se puede hacer un mejor tratamiento de datos de manera específica, lo anterior necesita una autorización de los propietarios de los datos personales.

El moderador complementa afirmando que en la legislación colombiana hay un tema parecido en dónde se autoriza a ciertos países que se supone que tienen unos estándares de protección.



6:00 p.m – 6:30 p.m

Cierre del Evento

Palabras a Cargo de:

- **Doctora Adriana Castro.** Directora del Departamento de Derecho de los Negocios de la Facultad de Derecho de la Universidad Externado de Colombia.

Relatoría: Laura Victoria Ramos

Al finalizar el evento, la Doctora Adriana agradeció a los expertos, panelistas, asistentes y becarios. Expuso que la transmisión del *streaming* de los talleres del día miércoles contaron con 476 visualizaciones y el día jueves, a medio día, 857 visualizaciones. Quiso resaltar y celebrar dichas cifras porque significa que las discusiones obtenidas en ese espacio han llegado a muchas más personas.

Afirmó que las estadísticas finales y detalladas, se expondrán cuando se publique las relatorías oficiales del evento en la página de la Mesa Colombiana de Gobernanza de Internet (governanzadeinternet.co). Lo conversado en el evento, se presentará como resultado en el 6° Foro de Gobernanza de Internet en el Foro Global que se realizará del 25 al 29 de Noviembre del 2019 en Berlín, Alemania. En particular en dos sesiones:

1. Sesión principal de las iniciativas Regionales y Nacionales de Gobernanza de Internet, titulado: “Las tecnologías emergentes y sus interfaces con inclusión, seguridad y Derechos Humanos”.
2. Sesión alterna, denominada sección de acceso, titulada: “Para lograr un acceso significativo, inclusión de grupos vulnerables y desarrollo de capacidad digital”.

Adicionalmente, se llevarán las discusiones realizadas en este evento al Foro Regional de América Latina y el Caribe, que se celebrará en Santiago de Chile en el 2020.

Reconoció que al cierre del 6° Foro, se contó con 404 suscriptores a la lista de la Mesa Colombiana de Gobernanza de Internet. Lo que permite la vinculación de más personas y actores, para que efectivamente continúe dando lugar al debate y las discusiones.

Invitó a los asistentes a seguir participando en espacios como estos, en la página web (governanzadeinternet.co), en dónde se dará continuidad a las citaciones para las reuniones bimensuales, encontrarán también, las actas de las reuniones anteriores y las discusiones.

Celebró la participación de nuevos actores a través de los becados por el Foro, que provienen de Regiones como: Atlántico, Cesar, Nariño, Boyacá, Córdoba y Huila.

A modo de cierre del evento, extendió un especial agradecimiento a los voluntarios relatores, grupo integrado por algunos de los Becarios al Foro y estudiantes de la



Universidad Externado de Colombia, miembros del Semillero de Derecho Informático y Nuevas Tecnologías, miembros del Observatorio de Nuevas Tecnologías y Derecho Privado, Monitores de la Línea de Investigación de Comercio Electrónico; de su gestión, dará como resultado la relatoría del evento que será publicada en la página Web.

Realizó un agradecimiento especial a los intérpretes de señas, que hicieron una labor invaluable, al personal de *Streaming* y a todo el personal de la Universidad que facilitaron la logística del evento.

Extendió un especial reconocimiento a los organizadores que facilitaron la realización del Foro, Capítulo ISOC Colombia, .Co Internet, Comisión de Regulación de Comunicaciones - CRC, Colnodo, Fundación Karisma, Google Colombia, Internet Governance Support Association, Movistar Telefónica Colombia, Observatorio de la Juventud, Red PaPaz, Universidad del Rosario y la Universidad Externado de Colombia.

Extendió un agradecimiento a los conferencistas, panelistas, moderadores y todos los asistentes por su activa participación. Invitó a todos, a modo de cierre, a un coctel para celebrar los logros anunciados en el discurso plasmado.

Estadísticas del Evento

Número de participantes.

Total inscritos: **231**.

Total becados: **9**,

Departamentos de becados:

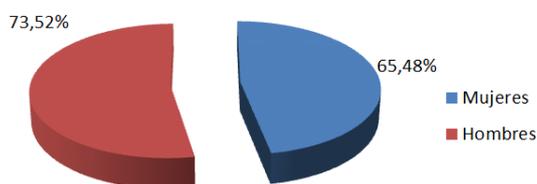
- Atlántico
- Boyacá
- Cesar
- Córdoba
- Huila
- Nariño

Talleres, Noviembre 6 de 2019:

Total presenciales: 138

Total por streaming: 476

Total: 614

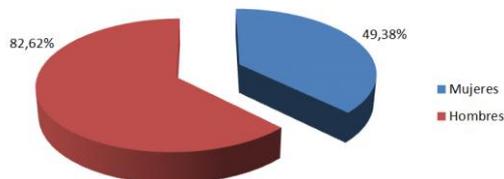


Foro, Noviembre 7 de 2019:

Total presenciales: 131

Total por streaming: 455

Total: 586



Participación por sectores:

Academia	86	37,23%
Comunidad Técnica	3	1,30%
Empresa Privada	39	16,88%
Gobierno	27	11,69%
Independiente	14	6,06%
Medios de Comunicación	7	3,03%
Organismo Internacional	1	0,43%
Sociedad Civil	45	19,48%
Otros	9	3,90%

