
## Global Encryption Day – October 21 2024 - Encrypt Today to Safeguard Tomorrow: The Encryption Summit

## ¿Cómo será la regulación de plataformas amigables con el cifrado? Perspectivas transregionales sobre la regulación de plataformas en línea y el cifrado'

**Maria Paz Canales - Global Partners Digital:** Buenas tardes, soy María Paz Canales. Soy la Jefa de Política Legal e Investigación en Global Partner Digital. Y tengo el placer, como representante de mi organización, miembro de la Coalición Global de Cifrado, de ser su moderadora hoy en esta conversación tan relevante que tenemos. Titulada '¿Cómo será la regulación de plataformas amigables con el cifrado? Perspectivas transregionales sobre la regulación de plataformas en línea y el cifrado'.

Para poner un poco en contexto esta conversación que estaba presentando con el título de la sesión, y que será compartida sustancialmente por nuestro maravilloso orador, quiero compartir unas pocas palabras al respecto. Vivimos en una era donde muchas más personas tienen acceso a la encriptación que nunca antes.

Sin embargo, también estamos viendo una gran cantidad de nuevas propuestas que lo socavarán, amenazando la privacidad y seguridad de la comunicación digital, poniendo en riesgo los derechos y el bienestar de individuos y grupos específicos. Al mismo tiempo, existen necesidades bien reconocidas de proteger mejor a los niños de daños y de garantizar la responsabilidad por los abusos de las empresas.

Sin embargo, en este contexto complejo, una respuesta regulatoria debe ser matizada y consultiva, respetando y cumpliendo con los principios de legalidad, necesidad, proporcionalidad, legitimidad y no discriminación desde nuestra perspectiva como defensores de la protección de la encriptación. Esta mesa redonda tiene la intención de reunir a estos maravillosos defensores que voy a presentar en unos minutos, provenientes del Reino Unido, Nigeria y Brasil, que han estado trabajando en la intersección de los derechos humanos y la tecnología para compartir su experiencia y conocimientos en esta discusión sobre la regulación de plataformas nacionales.

A través de esta discusión, lo que esperamos es cambiar tácticas y estrategias para participar en este debate. Y cuatro respuestas regulatorias que sean proporcionales y protectoras de la encriptación. Nuestro objetivo con esta sesión es generar aprendizajes y conclusiones que puedan ser útiles para la comunidad en general en lo que necesitan abogar en diferentes momentos, en diferentes geografías, en diferentes jurisdicciones.

Ahora pasaré a presentar a mi distinguido orador. Hoy contamos con la presencia de Adeboye Adegoke, quien es Gerente Senior de Paradigm Initiative de Nigeria. También nos acompaña Heloisa Massaro, quien es Directora de Internet Lab Brasil. Y por último, pero no menos importante, tenemos a Mark Johnson, quien es Gerente de Defensa en Big Brother Watch del Reino Unido.

Y comenzaremos la primera parte de esta discusión con un análisis profundo de la defensa en el proceso regulatorio de plataformas en línea a nivel nacional. Cada uno de estos distinguidos oradores tendrá alrededor de cuatro minutos. Tenemos cuatro minutos para compartir un poco de su introducción. Y sin más preámbulos, comenzaré contigo, Mark, pidiéndote que compartas un poco de tu experiencia considerando que el Reino Unido fue uno de los primeros países en desarrollar un sistema de seguridad en línea dedicado, en lugar de utilizar leyes existentes para abordar algunas de las preocupaciones de regulación de plataformas. ¿Puedes contarnos sobre tu participación en el proceso de elaboración de la Ley de Seguridad en Línea, a la que nos referimos, y la lucha por defender la fuerte protección de la encriptación? ¿Cómo se enmarcó la discusión y cómo respondieron Big Brother Watch y otros grupos de la sociedad civil que se coordinaron para confrontar esta propuesta a estas críticas, particularmente en el papel de la encriptación?

Muchas gracias por estar aquí, Mark. Tienes la palabra.

**Mark Johnson - Big Brother Watch:** Muchas gracias, María, y buenas tardes si es por la tarde donde te encuentras.

Sí, si no conocen Big Brother Watch, somos una organización de libertades civiles con sede en el Reino Unido. Tenemos un interés particular en la intersección entre los derechos humanos y la tecnología, y el título, obviamente, de la discusión es cómo sería una regulación de plataformas amigable con el cifrado.

No quiero ser negativo en mi perspectiva, pero desafortunadamente, según mi experiencia, tengo un buen ejemplo de cómo podría ser una mala regulación de plataformas no amigables con la encriptación con la Ley de Seguridad en Línea del Reino Unido. Para aquellos que no están familiarizados con esta ley, fue una legislación aprobada por nuestro Parlamento el año pasado, y tomó varios años en su elaboración.

La idea de una Ley de Seguridad en Línea del Reino Unido se planteó por primera vez a principios de la década de 2010, pero básicamente la forma en que funciona este tipo de regulación es que crea o designa un regulador independiente para establecer códigos de práctica, principalmente para grandes sitios de redes sociales abiertas. Y estos códigos de práctica dictan reglas sobre cómo deben moderar el contenido en sus sitios.

Las primeras versiones del borrador del proyecto de ley no mencionaban los servicios de mensajería privada. En su mayoría, los servicios de mensajería privada estaban exentos, y la idea de esta regulación era crear una forma de regular el contenido en las principales plataformas como Meta, X, y otras similares.

Por supuesto, había varias consideraciones sobre la libertad de expresión, y trabajamos en el proyecto de ley principalmente desde el principio con una perspectiva de libre expresión, pensando en cómo la moderación de contenido y las reglas al respecto podrían afectar el derecho de los usuarios a la libertad de expresión en línea. Pero mientras se desarrollaba el proyecto de ley, hubo un impulso simultáneo por parte de nuestro Ministerio del Interior aquí en el Reino Unido para insertar disposiciones en la legislación sobre los servicios de mensajería privada y, en particular, sobre los servicios de mensajería cifrada.

Y, en última instancia, la versión final del proyecto de ley incluyó disposiciones que se conocieron coloquialmente como avisos tecnológicos. En esencia, estos avisos tecnológicos eran una manera muy sutil, poco examinada y silenciosa de exigir que las plataformas utilicen tecnologías como el escaneo del lado del cliente para abordar el material de abuso infantil en sus sitios.

Esto fue a pesar de que en el Reino Unido, los cuerpos de seguridad y otras agencias ya tienen una serie de poderes para abordar ese problema, que por supuesto es una cuestión de derechos y debe tomarse muy en serio, pero ya había una variedad de poderes disponibles para muchos de nuestros cuerpos de seguridad y agencias para enfrentarlo.

Y estos poderes se insertaron a pesar de la privacidad, la precisión e incluso la compatibilidad de las tecnologías disponibles o la falta de compatibilidad con los dispositivos de los usuarios. Y así, estas disposiciones se añadieron a la legislación sin un gran escrutinio desde la perspectiva de la sociedad civil. Nos involucramos en el proceso, pero, por supuesto, este era un proyecto de ley vasto que hablaba sobre la regulación de varias partes diferentes de Internet, predominantemente plataformas de

redes sociales abiertas, pero también consideraba no solo la moderación de contenido, sino también la verificación de edad y otras disposiciones, incluyendo algunos nuevos delitos penales.

Desde la perspectiva de la sociedad civil, estamos increíblemente sobrecargados, dado que ya nos estábamos enfocando en consideraciones sobre la libertad de expresión y otros asuntos relacionados con la legislación. Nos involucramos con el gobierno en ese momento, pero desafortunadamente, el gobierno no estaba particularmente dispuesto a escucharnos, y presentamos los argumentos, tanto los argumentos de derechos.

los problemas de precisión cuando se trata de tecnologías como el escaneo del lado del cliente y también los problemas básicos sobre cómo funcionarían los procesos. Desafortunadamente, a pesar de nuestros mejores esfuerzos trabajando con parlamentarios de la oposición, finalmente no pudimos eliminar estos poderes del proyecto de ley, por lo que se convirtieron en ley el año pasado.

La buena noticia de nuestra parte, creo, es que hasta ahora el regulador que el gobierno ha designado, Ofcom, ha adoptado un enfoque bastante cauteloso, por lo que los poderes aún no se han utilizado. Y creo que es positivo que Ofcom haya sido muy cauteloso. Están muy conscientes de las consideraciones de derechos, el impacto en la privacidad y muchos de los problemas en cuestión.

La dificultad es que estamos muy a merced de Ofcom para que adopte ese enfoque. Pueden cambiar su enfoque en cualquier momento. Podrían volverse significativamente más intervencionistas. Y el marco regulatorio de la Ley de Seguridad en Línea del Reino Unido es un marco que está abierto a la influencia política por la forma en que está redactado.

Entonces, existe la posibilidad de que el gobierno pueda presionar a Ofcom para usar estos poderes y obligar a una plataforma de mensajería encriptada como WhatsApp o Signal a escanear todos los mensajes de todos los usuarios en el sitio. Y hay muy pocas formas en las que podríamos detener eso. Por supuesto, siempre existe la posibilidad, y de hecho, creo que es bastante probable que estos poderes puedan ser impugnados en un tribunal de justicia en el Reino Unido, y la organización de derechos humanos, la organización de libertad de expresión, Index on Censorship, encargó una opinión legal que decía que era probable que los poderes fueran ilegales.

De hecho, la opinión fue escrita por Matthew Ryder, quien en realidad dijo que Ofcom ahora tiene más poderes que GCHQ, nuestra agencia de espionaje digital aquí en el Reino Unido, como resultado de la ley. Es alentador en este momento que Ofcom sea cauteloso, los poderes no se han implementado. Pero existe la posibilidad de que haya un desafío legal si alguna vez se utilizan en el futuro.

Desde nuestro lado, es una situación difícil porque hemos sentado un mal precedente. Tendrá un impacto en los usuarios de todo el mundo porque si se utilizan estos

poderes, y si WhatsApp o Signal se ven obligados a comprometer la seguridad de sus usuarios al socavar el cifrado de extremo a extremo, también afectaría a personas en todo el mundo.

Así que hay un impacto en los derechos en otras partes del mundo, no solo en el Reino Unido. Y, desafortunadamente, es un mal ejemplo de regulación. Pero todavía hay oportunidades para luchar contra ello. Lo estamos examinando tanto como podemos. Y si el gobierno alguna vez piensa en presionar a Ofcom, o si Ofcom alguna vez piensa en usar esos poderes, seremos los primeros en oponernos e intentar evitar que se utilicen.

**Maria Paz Canales - Global Partners Digital:** Muchas gracias, Mark, por esas perspectivas, aunque, sí, son menos positivas de lo que quisiéramos para esta conversación, pero creo que hay aprendizajes relevantes que se sienten positivos en términos de estrategia y una oportunidad para también colaborar con una organización que trabaja en otras jurisdicciones para mostrar cuáles podrían ser las mayores consecuencias de este tipo de enfoque legislativo en otras partes del mundo. Y pasando a esa conversación, me gustaría pedirle a Boye que comparta su perspectiva sobre cuál ha sido su experiencia y la experiencia de Paradigm Initiative en participar en el proceso de redacción del proyecto de ley de protección de la salud en línea en Nigeria, cómo han estado participando en la etapa consultiva de este proyecto de ley para dar forma a este desarrollo y cómo, muchas gracias por unirse a nosotros hoy, y esperamos que este tema de la encriptación haya surgido y cómo también tal vez podría conectar con algunas de las experiencias compartidas por Mark y cómo esas podrían ser útiles o no, o diferentes en el desarrollo de la discusión en Nigeria.

Te cedo la palabra.

**Adeboye Adegoke - Paradigm Initiative:** Muy bien. Gracias, María. Creo que mucho de lo que dijo Mark también resonó conmigo. Pero creo que la principal diferencia es que en línea, el proyecto de ley de seguridad en línea del Reino Unido y el proyecto de ley de daños en línea en Nigeria, el proyecto de ley de daños en línea en Nigeria todavía está en proceso.

No tenemos una ley todavía. De hecho, ni siquiera tenemos un proyecto de ley. Todo lo que tenemos es un documento técnico que define la dirección que tomaremos. Ahora, en términos de nuestra experiencia en este tema, creo que se basa en nuestros años de trabajo abogando por la protección de los derechos digitales en Nigeria. Así que cuando el gobierno nigeriano habló sobre la creación de un comité para asesorarlo sobre cómo debería ser la protección contra daños en línea en Nigeria.

Decidieron invitarnos a la sala, pero no solo nos invitaron. También fue porque estamos tratando de crear un equilibrio en la participación, diciéndonos que ustedes han estado abogando por la protección de los derechos digitales. También han propuesto una ley sobre derechos digitales y libertad en Nigeria.

Entonces, lo que habían propuesto al principio era tener una legislación que abordara los derechos digitales y la salud en línea. La propuesta en ese momento era tener una legislación de protección de derechos digitales y salud en línea. Pero pensamos que eso era complicado para nosotros, dado que sabemos cómo ha sido este proceso.

No queríamos que los dos temas se mezclaran. Queremos que Nigeria tenga una legislación que hable sobre los derechos digitales y la libertad, mientras que también pueda abordar el tema de los daños en línea en una legislación separada. Así que, cancelamos eso. Está bien. Estamos en este comité para asegurar que haya protección digital en su esfuerzo por regular los daños en línea, pero no le den ese nombre porque una vez que le den ese nombre, será difícil para nosotros.

Entonces, la forma de regulación, por ejemplo, cuando Mark estaba dando la experiencia del Reino Unido, mencionó algo sobre cómo, en el producto final, no pudieron cambiar ciertas cosas que les hubiera gustado cambiar. Así que también sabemos que nuestro poder estaba limitado en términos de poder determinar cómo se vería el documento final.

Así que queremos poner fin a nuestra defensa de una legislación sobre derechos digitales en Nigeria, modelando un tema que busca proteger las manos en línea, dado que ya conocemos ciertos desafíos que podrían surgir en ese contexto. Así que comenzamos a trabajar como miembros del comité directivo de la iniciativa junto con muchas otras organizaciones que forman parte de ese comité.

Muchos de ellos son grupos de expertos, muchos de ellos también trabajan en los ámbitos de la tecnología y la política. Por supuesto, los problemas eran claros en términos de lo que es de suma importancia para cada uno de los interesados. Para nosotros, lo que nos interesaba era asegurarnos de que esto no se convirtiera en otra excusa para violar derechos.

Como hemos visto muchas veces en esta parte del mundo, donde las leyes que abordan el cibercrimen se convirtieron en herramientas de opresión, en herramientas para suprimir el espacio cívico o para atacar a los defensores de los derechos humanos. Así que eso siempre ha sido una prioridad. Ese proceso llevó a la publicación de un libro blanco sobre la protección en línea en Nigeria.

Y si miras ese libro blanco hoy, no parece realmente malo cuando se trata específicamente de la cuestión de la encriptación. Pero eso es porque comenzamos, comenzamos la conversación desde la protección de los derechos digitales. Pero como dije, todavía es temprano en el juego para celebrar porque lo que tenemos es un libro blanco, el libro blanco, del libro blanco vamos a tener un proyecto de ley, y también el proyecto de ley pasará por muchos procesos, los políticos lo revisarán, las diferentes agencias gubernamentales darán su opinión sobre todo eso, y muchas cosas aún pueden suceder.

Pero una cosa en la que hemos sido muy consistentes es en monitorear el proceso. No solo porque somos miembros del comité directivo, sino también porque siempre hemos monitoreado el panorama de los derechos digitales en Nigeria en general, y seremos los primeros en dar la voz de alarma cuando algo salga mal.

Entonces, una de las cosas que también hemos hecho es llevar a cabo lo que nos gusta llamar la Serie de Compromiso con la Política Digital con el Grupo de la Sociedad de Radiodifusión para informarles sobre lo que está sucediendo con ese proceso, porque esto aún no es público. No muchas personas saben que este proceso está en marcha.

Estoy seguro de que las personas en esta llamada se estarán preguntando por qué algo así está ocurriendo en Nigeria. Por supuesto, no era de conocimiento público. Pero lo que hicimos fue organizar esa serie de compromisos de política digital donde informamos a las partes interesadas, especialmente desde el ámbito de la sociedad civil, sobre lo que está sucediendo con el gobierno nigeriano.

Esto es lo que se nos ha pedido hacer. Así es como los hemos apoyado hasta ahora. Además, con respecto a la disposición preocupante del borrador del libro blanco en este momento, también hemos planteado algunas cuestiones. También, trabajando con nuestro socio, Global Partners Digital, revisamos ese libro blanco juntos. Identificamos algunos problemas y los comunicamos, diciendo que estos son asuntos que nos gustaría que se abordaran.

Hasta ahora, todo bien. Ese proceso aún está en marcha, como dije, pero es demasiado pronto para celebrar y decir, oh, este libro blanco es bueno para la encriptación o permite la encriptación. Cualquier cosa puede suceder porque hay intereses en competencia. Y tal como dijo Mark, el punto sobre quedar a merced de Ofcom también es una posibilidad de fallos en esta parte del mundo.

Hemos visto muchas leyes por aquí donde, en la letra de la ley, ni siquiera parecen preocupantes. Pero por experiencia, sabemos que en términos de implementación, lo que sucede luego depende de quién implemente la ley. Así que somos muy conscientes de esa perspectiva también. Y también estamos tratando de prevenir eso en lo que será el resultado final de este proceso.

Muchas gracias.

**Maria Paz Canales - Global Partners Digital:** Gracias, Boye. Definitivamente, creo que hay diferentes desafíos para superar esto. Algunos de ellos surgen durante el proceso de redacción de esta legislación, pero sin duda, como destacan tus comentarios y los de Mark, hay otra etapa del proceso. Preocupación en términos de la implementación y la interpretación de los poderes de la autoridad para implementar estas leyes.

Pasando a un sabor diferente en los desafíos de esta discusión, escucharemos a Heloisa, y te pediré que nos cuentes en particular sobre la experiencia de Internet Lab al involucrarse en el proceso de desarrollo del Proyecto de Ley 2630 de Brasil, cuál es el contexto del acuerdo y las preocupaciones clave relacionadas con él, especialmente en temas de cifrado, y cómo se movilizó la sociedad civil para evitar amenazas a la libertad de expresión y privacidad que surgieron en esta discusión.

Gracias por estar aquí, Heloisa, para tu charla.

**Heloisa Massaro - InternetLab:** Gracias, Maria Paz. Hola a todos. Es realmente un placer estar aquí hablando hoy. Creo que para hablar específicamente sobre los problemas que surgieron durante las discusiones del proyecto de ley 2630, es importante, creo, destacar dos contextos diferentes.

Eso influyó un poco en cómo se abordaron las aplicaciones de mensajería en los primeros borradores del proyecto de ley. Entonces, el primero es que entre 2015 y 2017, Brasil tuvo un par de casos que involucraron el bloqueo de aplicaciones de mensajería, específicamente WhatsApp. Y en ese entonces, las órdenes de bloqueo provenían de procedimientos, de procedimientos penales de los que no tenemos muchos detalles, pero el problema principal involucrado era.

Los jueces querían acceso o los fiscales querían acceso a las comunicaciones que estaban encriptadas y WhatsApp no podía proporcionar el contenido de estas comunicaciones, por lo que el juez bloqueaba la aplicación hasta que se cumpliera la orden. Así que hubo estos episodios clave relacionados con la encriptación y muchos malentendidos sobre cómo funcionaban las aplicaciones de mensajería en ese entonces.

Necesitamos recordar que en 2015 estábamos, podríamos decir, en los primeros años de uso masivo de aplicaciones de mensajería encriptada, como difundir las noticias. Y esto es lo primero. Ya habíamos tenido un par de problemas con las aplicaciones de mensajería. Y es importante destacar que Brasil es un gran usuario de aplicaciones de mensajería.

Tenemos alrededor del 99 por ciento de los usuarios de Internet que usan aplicaciones de mensajería en su vida diaria. Usan aplicaciones de mensajería todos los días. WhatsApp. Tenemos investigaciones que muestran que el 99 por ciento usa WhatsApp todos los días en su vida. Así que es un uso realmente intensivo de la aplicación y considerando que tenemos alrededor del 85 por ciento de la población conectada, es realmente mucha gente usándola.

Entonces, en 2018, durante las elecciones en Brasil, lo que sucedió fue que recibimos algunos informes de mensajes masivos en WhatsApp que violaban la ley electoral. 2018 fue el año en que Bolsonaro fue elegido y fue una elección muy marcada por la difusión de desinformación y ataques en un contexto realmente polarizado.

Ese era el escenario, y había una gran preocupación de que el canal clave para la desinformación y la polarización eran las aplicaciones de mensajería, especialmente WhatsApp. Así que cuando llegamos a 2020, después de muchos problemas relacionados con esta información y discusiones sobre noticias falsas, etc., y luego estamos en la pandemia, surge este proyecto de ley, el 2630, que se propone en el Congreso bajo el nombre de Ley de Noticias Falsas.

Y los primeros borradores eran realmente preocupantes. Hubo mucha presión por parte de la sociedad civil. Y luego, a mediados de 2020, uno de los primeros borradores fue aprobado en el CNA. En ese entonces, el borrador trataba principalmente sobre transparencia y algunos temas procedimentales, pero había un punto muy controvertido sobre la trazabilidad.

La regla básicamente decía que cada mensaje que era, no recuerdo exactamente los detalles, pero era algo así como que cada mensaje que se reenviaba a más de cinco grupos y llegaba a más de 1,000 personas en un cierto período de tiempo. La plataforma necesitaría mantener los metadatos de esta acción de reenvío.

Entonces, la idea detrás de esto era que si podías identificar un mensaje infractor, podrías, a través de estos metadatos, rastrear a la primera persona que lo envió. ¿Cuáles eran los objetivos? El objetivo principal era identificar de dónde provenía esta información. Y, pero, ¿cuáles eran los problemas con esto?

Esta regla de trazabilidad es que, en primer lugar, las plataformas, las aplicaciones no podrían identificar una vez que se envía un mensaje, si se volverá viral o no. Así que, en la práctica, necesitarían mantener los metadatos de cada mensaje hasta que se alcanzara este período de tiempo, al menos hasta que se alcanzara este período de tiempo.

Entonces, para asegurarse de que si este mensaje se volvía viral, tendrían los metadatos y era un mandato para la retención masiva de datos, y existía la posibilidad de acceder a estos datos en procedimientos penales. No había muchos requisitos para este acceso, por lo que era bastante vago cómo se podía acceder a estos datos.

Y en la práctica, había muchos riesgos, pero la norma en sí no era realmente efectiva para su objetivo, porque ignoraba completamente el hecho de que a veces las personas simplemente descargan el contenido. A veces el contenido viaja a través de plataformas. Así que tal vez el contenido estaba en Telegram y alguien lo copió y lo pegó allí.

Entonces, realmente no se podía acceder a quién fue la primera persona. La persona que lo envió y eso creó el riesgo de criminalizar al usuario al final del día. Y había un gran desafío dentro de esta regla, ya que la sociedad civil en sí misma estaba bastante dividida, no era unánime la oposición a la regla y al proyecto de ley en sí.

Y en ese entonces, había mucha presión por parte de un grupo, una coalición de organizaciones de derechos digitales de la cual formamos parte, para actuar juntos y contrarrestar estas reglas problemáticas dentro del proyecto de ley. Y nosotros, junto con muchas organizaciones que forman parte de esta coalición de derechos digitales, trabajamos produciendo tanto conocimiento como análisis de políticas y tratando de dialogar con el ponente del proyecto de ley.

Y esto fue algo realmente importante en ese momento porque el ponente en ese entonces era alguien muy abierto al diálogo con la sociedad civil. Y habíamos producido en 2020, 2021, un análisis de políticas sobre los problemas involucrados en este tipo de normas. Y al final del día, hubo muchas discusiones de ida y vuelta con este proyecto de ley, y terminó no siendo aprobado, no tanto por los problemas de privacidad en sí, sino principalmente por las tensiones políticas dentro del Congreso.

Y luego, en 2023, volvió como un proyecto de ley de regulación de plataformas. Así que el mismo proyecto de ley, el texto fue completamente reformulado y apareció como un proyecto de ley de regulación de plataformas que era más GSA y esta disposición sobre la trazabilidad fue eliminada. El proyecto de ley, pero nuevamente, el proyecto de ley no fue aprobado una vez más, también debido a cuestiones políticas.

Y ahora estamos en un escenario en el que probablemente tendremos a la Corte Suprema decidiendo sobre la constitucionalidad de la regla de responsabilidad de los intermediarios en Brasil. Esto cambiará un poco cómo se maneja la responsabilidad en Brasil e intentará agregar algunos puntos para la regulación de las plataformas. Así que este es nuestro escenario actual.

Gracias.

**Maria Paz Canales - Global Partners Digital:** Muchas gracias, Heloisa. Y creo que este es un momento perfecto de transición, tal vez para un diálogo más práctico en la siguiente sección de esta conversación, en términos de pensar en el panorama general que proporcionan estos tres diferentes ejemplos de compromiso al abordar las amenazas de cifrado que ocurren en el contexto de la regulación de plataformas.

Pero también pensando en cómo este espacio proporcionado por el trabajo conjunto en la Coalición Global de Cifrado y la oportunidad de expandir la comunidad en este evento de hoy, en torno al Día Global del Cifrado, puede ser útil para continuar este intercambio de tácticas para el compromiso y la participación nacional.

Gracias. Estrategias para defender la encriptación y quiero hacer un par de preguntas adicionales a los ponentes en esta ronda, en esta sección, pero también animo a la audiencia a compartir sus comentarios, sus preguntas, sus reacciones, pero realmente con este enfoque más estratégico en mente para que podamos aprovechar al máximo el resultado de esta sesión en términos de conclusiones.

Y empezando con Mark primero. Ya comenzaste a compartir un poco sobre cómo, a medida que la Ley de Seguridad en Línea pasa a la implementación y aplicación, hay toda esta expectativa y posible tensión en cómo las autoridades y, en particular, Ofcom interpretarán la ley y cómo interpretamos sus propias responsabilidades clave proporcionadas en la ley. ¿Cuáles son los mensajes clave que tendrás para los responsables de políticas que diseñan o implementan la regulación de seguridad en línea, considerando esta tensión que ya comenzaste a destacar en el blog anterior? Tal vez quieras expandir un poco más, pero pensando también en las intervenciones que han venido después de ti de otros colegas en otras regiones, ¿qué otras cosas consideras que podrían ser útiles en términos de tácticas y puntos focales de atención al tratar con este tema de la definición de responsabilidades de las autoridades y las cosas que se pueden hacer durante el período de implementación que ya estás comenzando a experimentar por ti mismo en la implementación de la Ley de Seguridad en Línea?

Gracias, Mark.

**Mark Johnson - Big Brother Watch:** Sí, en cuanto a las próximas fases de la implementación de la Ley de Seguridad en Línea, hemos tenido una comunicación muy buena con Ofcom, el regulador independiente, que ha sido bastante receptivo, diría yo, en términos de hablar con la sociedad civil y escuchar sus preocupaciones. Creo que cuando el proyecto de ley de seguridad en línea, antes de convertirse en ley, estaba pasando por el Parlamento.

Los debates en torno a esto no fueron exhaustivos porque había casi un consenso bipartidista de que necesitábamos algún tipo de legislación. No estábamos de acuerdo con el modelo de la Ley de Seguridad en Línea debido a todas las diferentes consideraciones de derechos, ya fuera la libertad de expresión, la privacidad u otras ramificaciones de la legislación.

Pero hubo bastante apoyo en ambas Cámaras del Parlamento. Así que el debate nunca fue tan completo como debería haber sido en el Parlamento. Y hay algunas lecciones que podemos aprender de esa experiencia y cómo podemos ser mejores como defensores e intentar impulsar un debate más amplio. Pero creo que Ofcom ha adoptado un enfoque después de que se aprobara la legislación, que es que saben que planteamos preocupaciones a lo largo del proceso, incluso si este debate no fue tan completo y exhaustivo como debería haber sido en el Parlamento.

Y han tenido una actitud receptiva, nos han escuchado y consultado, lo cual creo que es muy positivo. Además, han adoptado un enfoque cauteloso porque saben que algunos de los cambios que traerán las leyes serán bastante radicales y realmente reformularán cómo podría funcionar nuestra relación con las plataformas de redes sociales o los servicios de mensajería en el futuro.

Entonces, ellos han estado, han participado en nuestro. El plan desde la perspectiva de nuestra organización es continuar monitoreando cómo funciona el proceso tan vigilante como podamos y seguir participando. Ofcom ha realizado algunas consultas abiertas. Hemos participado en términos de lo que podríamos hacer colectivamente.

Descubrí que tener voces externas como parte del debate es de gran ayuda porque cuando nos involucrábamos con el gobierno y cuando nos involucrábamos con los políticos, incluso con los políticos de la oposición, porque la oposición en el Partido Laborista, obviamente ahora están en el gobierno, pero todo esto sucedió cuando los Conservadores estaban en nuestro gobierno en el Reino Unido, la oposición no era muy fuerte en derechos digitales, el Partido Laborista no era fuerte en derechos digitales, y la dificultad, el desafío que teníamos era que con esta legislación, todos los diferentes problemas estaban frente a nosotros, ya fuera relacionado con la libertad de expresión, la verificación de edad, las implicaciones de privacidad o la encriptación.

Y estábamos muy dispersos. También estaba el desafío de que ambos partidos querían que algo sucediera en este ámbito. Así que fue muy difícil. A menudo nos acercábamos a los mismos políticos una y otra vez, y ellos decían: "Oh, aquí está Big Brother Watch de nuevo. Siempre hacen los mismos argumentos."

Pero si logramos tener voces externas, y hacia el final del proyecto de ley, conseguimos incorporar más voces externas en la sala. Esto crea una imagen más amplia. Da más matices a los argumentos porque podemos decir que esto violará nuestros derechos de privacidad y también podemos decir que esto tendrá un impacto en periodistas o defensores de derechos humanos en otras jurisdicciones alrededor del mundo.

Realmente no, serían los mismos argumentos que estamos haciendo, mientras que si pudiéramos traer otras voces de otras jurisdicciones, de otros antecedentes, tuvimos una mesa redonda con otra organización de derechos donde tuvimos a Amnistía presente. Tuvimos una organización LGBT, varios grupos y organizaciones diferentes que representaban a personas para hablar sobre periodistas o defensores de derechos humanos en diferentes partes del mundo.

Tener otras voces en la sala fue realmente útil, así que aunque el resultado de la legislación no fue tan positivo como nos gustaría, lo que es útil es que podemos mirar hacia atrás con reflexión y decir esto es lo que podríamos haber hecho más en el futuro. Esto es lo que otras personas pueden hacer en el futuro si enfrentan amenazas similares.

Obviamente, como dije, la buena noticia es que Ofcom no ha utilizado estos poderes y están siendo muy cautelosos. Así que no es una historia terrible, pero ciertamente hay mucho que aprender de esta experiencia legislativa, que definitivamente fue menos de lo deseado.

**Maria Paz Canales - Global Partners Digital:** Gracias, Mark.

Creo que tampoco deberíamos ser tan duros con nosotros mismos. Creo que al final, aunque el resultado final tal vez no fue el que deseabas, definitivamente podría haber sido peor. No estabas llevando a cabo todos esos esfuerzos. Así que creo que tú y otros que trabajan en esto merecen crédito.

Posiblemente también la moderación en la fase de implementación que estás viendo, es también resultado de que la autoridad es consciente de cómo esto crea tensión y críticas durante la discusión del proyecto de ley. Así que creo que, tomemos también ese lado positivo en el resultado. Y pasando a Boye, de nuevo a Boye, creo que ya mencionaste en tu intervención anterior, este concepto que Mark nos trajo en términos de expandir la participación, no solo de los sospechosos habituales, sino de grupos adicionales de la sociedad civil, pero tengo curiosidad si puedes decirnos más sobre unirte a nosotros y espero que entiendas un poco más, Boye, en términos de las cosas que has visto en, por ejemplo, cómo el contexto proveniente de otras jurisdicciones de experiencias previas ha sido útil o no en la discusión que estás teniendo en Nigeria sobre el tema en línea, en Internet.

¿Y qué se puede aprender de la experiencia de los defensores en Nigeria más allá de este elemento que ya mencionaste sobre la ampliación de la participación, que también tiene puntos en común con lo que Mark estaba diciendo? Así que tienes la palabra, Boye.

**Adeboye Adegoke - Paradigm Initiative:** Muy bien. Muchas gracias, María. Es interesante porque ni siquiera creo que estaríamos teniendo esta conversación en Nigeria si no existiera la Ley de Seguridad en Línea del Reino Unido.

No porque la contemplación no existiera o no siempre estuviera presente, sino también por la reputación de usar legislaciones que buscan abordar armas, ya sea en espacios digitales o en espacios offline, como una herramienta para suprimir los espacios cívicos. Ha habido retrocesos muy significativos por parte de la sociedad civil o incluso de los ciudadanos contra el gobierno cada vez que intenta introducir cualquier legislación de esa naturaleza.

Entonces, el gobierno necesita poder señalar ejemplos de países que típicamente se considerarían buenos ejemplos para que el gobierno nigeriano pueda decir cómodamente que esto es lo que está sucediendo en otras partes del mundo. Y eso también es lo que está sucediendo en lugares que llamarías sociedades justas o democráticas.

Entonces, proporciona una especie de mayor validación para siquiera contemplar hacer esto en primer lugar. Eso te dice que tiene una influencia muy grande al observar lo que ha sucedido en Australia y en el Reino Unido. Influyó en la decisión del gobierno de ser lo suficientemente audaz como para salir sin recibir demasiada resistencia de los ciudadanos, porque el déficit de confianza es muy bajo por aquí entre el gobierno y la gente.

Y cada vez que el gobierno contempla ciertos tipos de legislación, los ciudadanos tienden a verlo desde una perspectiva negativa y todo eso. Pero luego, cuando el gobierno puede señalar ejemplos de lo que está sucediendo en el Reino Unido y Australia, que una persona promedio por aquí considera sociedades cuerdas, entonces, si está sucediendo en esas jurisdicciones, ¿por qué no podemos tener esa conversación aquí?

Así que esa es la medida en que influyó en la decisión de emprender este camino en Nigeria. Sin embargo, más allá de eso, también influye en la prueba, el contenido de la legislación propuesta. Porque lo que suele suceder es que los países que primero implementan algunas de estas leyes se convierten en un modelo para que otros lo utilicen.

Mientras hablamos, puedes ver que, incluso con el libro blanco, se hicieron referencias a la Ley de Seguridad en Línea del Reino Unido. También se hicieron referencias a la versión australiana, porque esto sirve como un modelo que estamos utilizando. Y luego intentamos contextualizar lo que vemos en esos modelos a nuestra realidad como nigerianos y africanos.

Nosotros, somos muy conscientes y muy conscientes del impacto o de cuánto lo que sucede en otros lugares impacta lo que sucede en nuestra parte del mundo. Y, incluso te interesaría, incluso argumentaría que incluso los procesos globales pero los marcos de la ONU.

Como el marco de la GDC o de la UNESCO, por ejemplo, o la regulación de plataformas, no tienen tanto impacto como los marcos nacionales de ciertos países. En muchos países africanos, incluida Nigeria, estas leyes nacionales que se han promulgado, ya sea en el Reino Unido, en la UE, en los EE. UU. o en cualquier otro lugar, tienen una gran importancia.

Influir en la forma del enfoque. Y de hecho, permítanme también contarles una narrativa muy interesante en Nigeria cuando introdujimos el proyecto de ley de Digitalistas y Libertad. Y cuando llevamos el proyecto de ley al Parlamento, una de las cosas que nos preguntaron fue que al Parlamento le encantaría ver un almacén.

Esto se ha hecho, incluso les encantaría probablemente realizar un estudio de trabajo para ver qué está sucediendo en esa tradición. Y en el momento en que redactamos el proyecto de ley sobre la libertad. No había ningún país que estuviera teniendo una conversación similar en ese momento. Lo más cercano en ese momento era el Marco Civil en Brasil, lo que luego genera una conversación sobre cómo nuestros gobiernos africanos abordan la legislación, especialmente la regulación y legislación digital.

Esa es una suposición de que tienes que esperar a que los hermanos mayores muestren la dirección antes de tomar una decisión. Esa es la reticencia a asumir un

papel de liderazgo cuando se trata de definir la dirección para la regulación de las plataformas digitales o la tecnología en general. Gracias.

**Maria Paz Canales - Global Partners Digital:** Gracias, Boye. Sí, definitivamente, es un desafío. Creo que todos pueden relacionarse, particularmente en los países de la mayoría global, al observar modelos buenos y malos y continuar en esa línea. Brasil ha sido un líder en muchas cosas relacionadas con lo digital, como acabas de mencionar, el Marco Civil.

Por eso es tan interesante tenerte aquí, Heloisa, hablando sobre la experiencia. ¿Cuáles son tus conclusiones en términos de los aprendizajes sobre las trampas y oportunidades de regular las plataformas en línea, particularmente vinculadas a la discusión sobre la encriptación? Y tal vez pueda hacer una provocación para una ronda final de comentarios un poco más tarde para cada uno de ustedes como panelistas, así que no solo para Heloisa, sino para los tres en sus comentarios finales, me gustaría que lo cubrieran.

¿Cómo sería un enfoque amigable con la encriptación en el contexto de la regulación de plataformas en línea según la experiencia que ya has tenido al abordar este tema? Un poco sobre las lecciones aprendidas en el proceso brasileño. Y luego, si quieres abordar esta pregunta más general, también sería genial y más tarde daré la palabra a Mark y Voya para que den su opinión.

A ti, Heloisa, gracias.

**Heloisa Massaro - InternetLab:** Gracias Maria Paz. Primero diría que hemos estado aprendiendo cosas desde 2020, así que son cuatro años de aprendizaje con este acuerdo que va y viene y toma muchas formas y enfoques diferentes. Pero, diría que, ante todo, una cosa que ha sido realmente central en nuestro trabajo es ofrecer diagnósticos mejores y más matizados.

Y sé que esto tiene un impacto limitado de alguna manera, pero es realmente importante tener esto para llevar a la conversación. Y por qué digo esto, lo digo porque cuando hablamos de aplicaciones de mensajería, por ejemplo, comenzamos a desarrollar investigaciones cuantitativas y cualitativas sobre cómo se utilizan las aplicaciones de mensajería en Brasil para la comunicación política.

Y una de nuestras conclusiones clave es cómo los mensajes, principalmente WhatsApp, son una plataforma realmente importante y conectan otras plataformas, pero no es el único protagonista. Muchas gracias. Además, pudimos mostrar la variedad de usos que tiene WhatsApp, así que cuando implementas una medida para, no sé, abordar algún problema con esta información que podría no ser una pregunta específica en una aplicación de mensajería, realmente estás impactando a los pequeños negocios.

Realmente estás impactando la vida diaria de las personas. Y hemos estado tratando de llevar esto al diálogo durante los últimos años. Y esto es una de las cosas que hemos encontrado realmente importante y útil porque ayuda con el análisis de políticas y desarrollamos mejores enfoques también. La otra cosa, y es que trabajar en coalición durante este proceso fue realmente importante.

Las organizaciones de derechos digitales realmente han trabajado juntas durante el proceso de regulación de plataformas, y esto ha sido realmente importante para crear, este tipo de, para tratar de abordar los desacuerdos entre nosotros en este espacio seguro antes de realmente abogar por otro enfoque.

Y esto ha sido realmente importante para este proceso. Diría que muchas de las victorias que la sociedad civil ha tenido durante este proceso fueron gracias a este trabajo en coalición. Y también pudimos aprovechar lo mejor de cada organización en esto. Tendríamos organizaciones como Internet Lab, que estarían produciendo investigaciones orientadas a hechos.

Tendrías organizaciones que estarían más en el terreno haciendo defensa en el Congreso. Así que esto fue realmente importante. Y una última lección que diría de estas cosas positivas es el diálogo con las partes interesadas. Y cuando digo diálogo con las partes interesadas, es como realmente escuchar y realmente tomar en consideración cuáles son los problemas.

que las partes interesadas están tratando de abordar o cuáles son los desafíos que enfrentan. Y esto se aplica tanto al sector privado para entender profundamente cuáles son los problemas que han surgido, como también trabajar con profesionales legales, por ejemplo. Así que realmente dialogar con fiscales, con jueces, y desarrollar este tipo de.

capacidad de escucha que realmente ayuda en este proceso también. Y en cuanto a los desafíos, añadiría dos cosas y luego concluiría. Diría que a pesar de todos estos logros que hemos tenido, no tenemos una ley que haya sido aprobada. Así que al final del día, tienes las disputas políticas que eclipsan todo y de alguna manera superan todo el trabajo que se ha realizado.

Y el poder de los medios tradicionales, especialmente en Brasil, no puede subestimarse. Los medios tradicionales fueron realmente importantes en este proceso de negociación y fueron uno de los elementos que bloquearon el proyecto de ley. Estas serían mis consideraciones finales, y en cuanto a la pregunta de Maria Paz sobre la regulación de plataformas amigables con el cifrado, no tengo la respuesta, pero añadiría algo que creo que es realmente importante tener en cuenta, que es, creo que necesitamos profundizar en la distinción entre las redes sociales y las aplicaciones de mensajería privada.

y entender que la regulación es diferente. Y cuando digo esto, también incluyo en la conversación el hecho de que a veces las aplicaciones de mensajería se convierten en plataformas de redes sociales y esto también debe tenerse en cuenta. De lo contrario, tendremos regulaciones que apuntan a atacar las características de redes sociales de las aplicaciones de mensajería y socavan la privacidad y la libertad de expresión.

Eso es todo. Gracias a todos.

**Maria Paz Canales - Global Partners Digital:** Gracias, Heloisa. Creo que, como de costumbre, nos estamos quedando sin tiempo con esta discusión tan interesante, pero me interesa escuchar tu opinión, Mark, y tu opinión, Boye, sobre esta pregunta, cómo sería un buen enfoque para ustedes. También soy consciente de que hay una pregunta adicional que se publicó en el chat y tal vez pueda intentar extender nuestro tiempo y preguntársela, incluirla en su respuesta, que está relacionada con oportunidades más específicas que ven en el horizonte en términos de trabajar juntos en cualquier propuesta legislativa o en términos de canales de implementación o desafíos en la implementación de algunas de las piezas de legislación que han estado siguiendo o cualquier otra oportunidad que vean en el horizonte en la que este trabajo de coalición global pueda ser útil en términos de servicio a otros que están comenzando a tener esta discusión.

Entonces, en las dos preguntas, tal vez. Muy rápidamente, pueden distribuir su tiempo como deseen. Mark, y luego Boye, gracias.

**Mark Johnson - Big Brother Watch:** Sí, intentaré ser breve. Sí, sobre la pregunta de cómo podría ser una buena regulación, es una pregunta muy difícil. Cuando abordamos el proyecto de ley de seguridad en línea, fuimos muy claros, no somos amigos, ni amigos cercanos ni aliados de las plataformas de redes sociales, reconocemos que hay mucho por hacer para responsabilizar a estas empresas, pero no pensamos que la Ley de Seguridad en Línea fuera necesariamente el enfoque correcto.

Preferiríamos ver una regulación que aborde los modelos de negocio de las empresas, que ponga fin al comercio masivo de datos y que considere la privacidad y la libertad de expresión como elementos centrales de cualquier tipo de regulación. Creo que, en términos de los desafíos específicos que diferentes jurisdicciones intentan abordar cuando piensan en eludir o socavar el cifrado de extremo a extremo, normalmente se trata de contenido relacionado con terrorismo, material de abuso sexual infantil y quizás desinformación, como escuchamos en el caso de Brasil. El principio debe seguir siendo que el cifrado de extremo a extremo no puede ser comprometido y que cualquier vigilancia debe basarse en sospechas razonables y ser dirigida, y que no se debe comprometer toda la plataforma.

Sé que muchas de las principales empresas de mensajería privada colaboran muy estrechamente con las fuerzas del orden en diversas jurisdicciones alrededor del

mundo. Podría haber formas de formalizar algunas de esas relaciones sin comprometer canales enteros y la privacidad de las personas que usan esos canales.

Entonces, esa es una respuesta un poco vaga, pero creo que lo más importante, obviamente, como todos en la escuela saben, es que debe haber ciertas líneas rojas que nunca deberíamos estar dispuestos a cruzar. En términos de oportunidades de colaboración, es posible que WhatsApp o Signal u otros servicios de mensajería encriptada de extremo a extremo importantes puedan fácilmente dirigirse a los reguladores del Reino Unido o al gobierno del Reino Unido y decir que están felices de no cumplir con lo que están haciendo. Y de hecho, ambas plataformas principales hablaron sobre la posibilidad de retirarse del mercado o ciertamente resistir las amenazas, la encriptación de extremo a extremo que fueron planteadas por la legislación de seguridad en línea.

Pero hay mercados más grandes o jurisdicciones más grandes para esas plataformas que están considerando la regulación en este momento, como el tipo de control de chat que se está considerando en la UE, y donde tienes 400 millones o más de usuarios, es mucho más difícil para esas plataformas individuales resistir o amenazar con retirarse.

Entonces, la probabilidad de que tengan que cambiar su producto o servicio en ese caso es significativamente mayor en comparación con un ejemplo más pequeño como el Reino Unido. Así que obviamente, para los colegas en la UE, obviamente ya no estamos en la UE, pero para los colegas que están en la UE, si es útil y podemos ayudar, y sé que las conversaciones aún están en curso en este momento, creo que estamos en una buena posición, pero si hay algo que podamos hacer y para los colegas de todo el mundo, entonces imagino que sería una jurisdicción bastante importante para hablar y ayudar.

Sí.

**Maria Paz Canales - Global Partners Digital:** Gracias, Mark. Boye, ¿cómo sería tu enfoque en esta regulación de plataformas amigable con la encriptación?

**Adeboye Adegoke - Paradigm Initiative:** Sí, creo que el debate para nosotros dentro del antiguo debate sobre privacidad y seguridad en términos de cómo podría ser una regulación de plataforma amigable con la encriptación.

Creo que lo importante es que debemos reconocer los problemas conflictivos en términos de cómo, por ejemplo, comprometer la encriptación puede tener impactos significativos en la privacidad, los derechos de privacidad de los usuarios, y también puede exponer a ciertos usuarios a riesgos. Pero tampoco debemos pasar por alto el aspecto de cómo la encriptación también puede ser mal utilizada o puede ser una herramienta para actores malintencionados.

Creo que lo importante es proporcionar salvaguardias que también aseguren que las autoridades no utilicen la encriptación como arma para lograr fines políticos. Usar, debilitar la encriptación para, para lograr fines políticos y una encriptación débil, para apuntar a ciertos individuos, probablemente debido a sus creencias políticas, creencias religiosas o su estilo de vida, o cualquier otra característica distintiva que posean.

Creo que nos guiamos por los Instrumentos Nacionales de Derechos Humanos en cuanto a cómo abordamos la limitación de derechos, como el derecho humano a comunicarse y tener comunicaciones encriptadas. Creo que limitar esos derechos debe seguir directrices muy claras. El Procedimiento de las 3 Pruebas, por ejemplo.

No creo que las autoridades deban tener un poder absoluto para acceder a las comunicaciones encriptadas, por ejemplo, lo cual, en términos prácticos y en la vida real de muchas personas, suele ser el caso, especialmente en países con instituciones débiles, y creo que eso será muy comprensible para la mayoría de los países del sur global.

La falta de instituciones fuertes ha creado un sistema en el que las autoridades, típicamente, se aprovechan de esta debilidad institucional para acosar a veces a las empresas de redes sociales o a las empresas que brindan servicios de comunicación, exigiendo acceso, exigiendo acceso trasero a la comunicación sin seguir el procedimiento, sin seguir el estado de derecho, sin ninguna justificación legítima y todo eso.

Entonces, creo que el equilibrio, lo que el equilibrio significaría para mí, es crear un sistema que respete los procedimientos, que respete el estado de derecho, que solo acomode preocupaciones legítimas, ya sea por parte de agencias de seguridad o autoridades, pero no un acceso generalizado o una prohibición generalizada de la comunicación encriptada. Tenemos que limitar cuánto poder tienen las fuerzas del orden, cuánto poder tienen las autoridades para acceder a la puerta trasera de conversaciones y comunicaciones importantes.

Tiene que ser en casos excepcionales donde esto sea necesario. No tiene que, no debería ser la norma. No debería ser la norma. Eso es básicamente lo que estoy diciendo. Y en nuestro trabajo en Nigeria también en torno a la explotación en línea, nuestro argumento ha sido crear fuertes salvaguardas, protección en términos del principio contenido en las leyes internacionales de derechos humanos para guiar los esfuerzos del gobierno en ese sentido.

Soy muy consciente del tiempo, así que voy a detenerlo aquí.

**Maria Paz Canales - Global Partners Digital:** Muchas gracias, Boye, y me has dado la clave perfecta para las conclusiones finales. Muchas gracias a todos por sus perspectivas. Espero que esto sea útil en términos de puntos de acción para las personas que siguen la conversación de hoy.

Y resumiré que algunos de los elementos clave a tener en cuenta a partir de su experiencia son esta idea de ampliar el grupo. Y creo que es importante tener este tipo de participación para contar con una comunidad más amplia que se ocupe de esto y comprenda las sutilezas de las diferentes comunidades sobre la implicación de impactar negativamente el uso de la encriptación, la idea de trabajar en coalición para moldear esta discusión en un espacio más seguro antes de entrar en otras batallas con la autoridad, la diversidad de contextos y diferentes usos y actores aquí, no solo pensando en las grandes tecnológicas, sino también en la diversidad de implementación de estas diferentes aplicaciones y el papel que juegan en la sociedad. El enfoque en el desafío, volviendo al último punto de Boye, su comentario final, desafíos, y estoy tratando de centrarme en esos desafíos y el enfoque del gobierno desde una perspectiva de derechos humanos.

Con esto, les agradezco mucho a todos ustedes y cerraré esta sesión, invitándolos a la próxima en esta muy interesante Conferencia de la Coalición del Día Global de la Encriptación. Gracias.