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

Tribunales en la Encrucijada: Defendiendo los Derechos Digitales contra la Represión de la Encriptación en el Sur de Asia

Raquel Kroich - Internet Society: Hola, bienvenidos a todos a Encriptar una Fecha para Salvaguardar el Mañana. Comenzamos con la primera sesión del día, Tribunales en la Encrucijada, Defendiendo los Derechos Digitales contra la Represión de la Encriptación en el Sur de Asia.

Permítanme pasarle la palabra a Karthika, para que pueda comenzar la sesión de hoy.

Karthika Rajmohan - Internet Freedom Foundation: Gracias, Raquel. Hola a todos. Bienvenidos a la Cumbre del Día Global de la Encriptación 2024. Soy Karthika Rajmohan. Soy Asesora Asociada de Políticas en la Fundación para la Libertad en Internet. Somos una organización de libertades civiles con sede en Nueva Delhi que trabaja en temas de derechos digitales, y hoy seré la moderadora de la sesión.

IFF está encantada de organizar un panel como parte del GED Summit. La discusión de hoy, como mencionó Raquel, será sobre códigos en la encrucijada. Defendiendo los derechos digitales contra la represión de la encriptación en el sur de Asia. La inspiración detrás de este panel y el contexto en el que nos basamos es el creciente esfuerzo gubernamental por restringir la encriptación de extremo a extremo bajo el pretexto de la seguridad nacional y la prevención del crimen.

Estamos muy contentos de contar con un panel de oradores extremadamente calificados y estimados, que son expertos en derechos digitales de varios países del sur

de Asia. Presentaré brevemente a todos los oradores. En primer lugar, tenemos al Dr. Sanjana Hattotuwa. Es un experto en desinformación en la Fundación ICT for Peace, donde estudia los desórdenes informativos y su impacto en la democracia y la sociedad.

A continuación, tenemos a la Sra. Vrinda Bhandari. Es una abogada independiente que litiga casos de libertad de expresión y derechos digitales en India. También es asesora externa de la Fundación para la Libertad en Internet. Luego tenemos al Sr. Shahzeb Mahmood. Es un investigador senior en el Instituto Global de Tecnología, donde su trabajo se centra principalmente en la regulación de contenido en línea, la inteligencia artificial y los deepfakes.

Luego tenemos a la Sra. Farieha Aziz. Es cofundadora de Bolo Bhi, una organización de la sociedad civil orientada a la defensa, políticas y investigación en áreas de derechos digitales y responsabilidad cívica. Y por último, tenemos al Sr. Santosh Sigdel, el Director Ejecutivo de Digital Rights Nepal, una iniciativa sin fines de lucro dirigida a la protección y promoción de los derechos digitales en Nepal.

Entonces, ahora que hemos presentado a nuestros panelistas, podríamos pasar a algunas declaraciones iniciales. Tal vez los panelistas podrían comenzar dándonos un contexto sobre cuál es la situación en sus respectivos países, qué tipo de represiones han estado llevando a cabo los gobiernos contra el cifrado de extremo a extremo y qué justificaciones están utilizando para ello.

Creo que para las declaraciones iniciales, podríamos empezar con el Dr. Sanjana. Si le gustaría comenzar.

Sanjana Hattotuwa - ICT4Peace Foundation: Sí, gracias y encantado de estar aquí. Seré breve. Para aquellos de la región, Sri Lanka es una historia conocida. Acabamos de tener una elección presidencial significativa, así que no sabemos si lo que hemos visto en el pasado continuará en el futuro. Uno espera que no. Pero el contexto general del país ha sido una historia familiar para otros países del sur de Asia también, donde la autoridad estatal, la autoridad ejecutiva y la impunidad han impedido la libertad de expresión y los derechos fundamentales en el país durante décadas, mucho antes de las redes sociales, pero se ha exacerbado como consecuencia del creciente interés del estado en las comunicaciones privadas privilegiadas y el estado securitizado en particular bajo el pretexto de combatir el terrorismo, pero también en Sri Lanka, con la vista puesta en este argumento de protección de mujeres y niños, donde ha habido mucha regulación y leyes aprobadas o contempladas para ser aprobadas ostensiblemente para proteger a mujeres y niños, pero que es bastante condenatoria con respecto a los principios fundamentales.

Voy a hablar de dos. Una es una ley absolutamente draconiana, sin precedentes en la historia legislativa del país, llamada la Ley de Seguridad en Línea, que entró en vigor en enero de este año. Es una historia más larga sobre cómo surgió, pero ahora está en

nuestros libros de estatutos, y no puedo usar, debido al Código de Conducta, palabrotas en esta llamada, pero es horrible.

es antitético a todos los derechos humanos imaginables en la Constitución. Es extraterritorial, se aplica a todos. En la Tierra, por increíble que parezca, retrocede en el tiempo hasta la primera vez que usaste Internet, y es increíblemente invasivo en términos de privacidad, está bajo el control del ejecutivo.

Lo cual es un gran problema debido a la naturaleza constitucional del país y lo poderoso que es el ejecutivo. Permite que la ley acceda a cualquier dispositivo, en cualquier lugar, en cualquier momento, sobre cualquier cosa, sobre una categoría de contenido llamada contenido prohibido. Y no es algo que yo esté inventando, eso está en la ley. Eso puede significar cualquier cosa.

Así que no está muy definido. De hecho, hay cláusulas en la ley que parecen sacadas de una novela romántica, porque en la ley se dice que si dices algo que molesta los sentimientos de una comunidad, eso es un posible punto de intervención. Y he dicho que no tengo sentimientos cuando he escrito cartas de amor o cuando he recibido cartas de amor, pero es muy extraño encontrar ese tipo de lenguaje en la ley.

Entonces, la OSA puede forzar la divulgación y en realidad es bastante grave. Afecta a E2EE de manera indirecta. En un contexto donde debes entender que en Sri Lanka, al menos, somos un país muy violento y el Ministerio de Defensa, regularmente y durante décadas, ha torcido el brazo de las telecomunicaciones para obtener la información que desean, sin ningún tipo de debido proceso.

Para dejarlo muy claro, en Sri Lanka no necesitas socavar el cifrado de extremo a extremo cuando puedes presionar a las telecomunicaciones para obtener metadatos o algunos de los datos que podrías querer sobre individuos o instituciones específicas, que generalmente son activistas de derechos humanos. Terminaré diciendo que hay una segunda ley que está en etapa de borrador y no sabemos si avanzará con el nuevo presidente ejecutivo y el gobierno, las elecciones parlamentarias en un par de semanas.

No sabemos cuál es el cronograma, pero bajo esto es una forma de gobierno. Iba a ser introducida muy pronto, llamada la Ley Antiterrorista. Así que tenemos una Ley de Prevención del Terrorismo, que es draconiana, pero ahora tenemos una Ley Antiterrorista, que ostensiblemente intenta arreglar la PTA, pero en realidad es mucho peor.

Y aquí tomamos una página de India, donde, en WhatsApp, los indios en esta llamada pueden hablar sobre el caso del Tribunal Superior de Delhi con Facebook, Meta y WhatsApp, y todo el enigma sobre ellos saliendo del mercado más grande si se les obligaba a socavar su propio cifrado de extremo a extremo con WhatsApp. Pero la sección 65 del borrador propuesto del ATA de Sri Lanka es exactamente lo mismo.

Obligará a todos los intermediarios de Internet y a cualquiera, en realidad, a entregar sus claves, a entregar su información. Así que afecta al nivel de los intermediarios, al nivel de las plataformas, pero también al nivel individual. Y es, no leeré la cláusula, pero no hay nada parecido en nuestros libros de leyes.

Y mi punto ha sido, si WhatsApp y Meta quisieran salir de India debido a lo que posiblemente se les obligaría a hacer, nosotros como país somos menos que el mercado de Mumbai. Así que he alertado a la gente de que, ¿qué creen que hará Meta en Sri Lanka si esta ley se aprueba? Terminaré diciendo que no es el caso de que seamos tan malos como India o Bangladesh o Pakistán o algunos de los otros países, pero la inclinación, la preferencia política y el sesgo es socavar.

comunicaciones privilegiadas encriptadas. Y esto ahora es un punto central de enfoque para aquellos en el Ministerio de Defensa y en el gobierno, con la intención de infiltrarse en el activismo de la sociedad civil y acceder a comunicaciones privilegiadas que consideran inconvenientes porque son inconvenientes para ellos.

Entonces, el argumento se hace ostensiblemente en torno a la reducción del terrorismo, la protección de hombres y niños. Pero todos sabemos, espero, en esta llamada y en la audiencia, que el resultado final de eso es absolutamente perjudicial para los principios fundamentales. Así que ese es el contexto general de Sri Lanka tal como está hoy.

Karthika Rajmohan - Internet Freedom Foundation: Gracias por eso. Fue muy útil. Hay muchos puntos en los que me encantaría profundizar, pero llegaremos a eso más tarde. Ahora, si la señora Vrinda Bhandari pudiera comenzar con su declaración inicial.

Vrinda Bhandari - Internet Freedom Foundation: Hola. Creo que es perfecto seguir adelante, ya que ya hemos visto el contexto de Sri Lanka, así que creo que India sigue el mismo camino, y empezaré tal vez hablando sobre el desafío que ha planteado WhatsApp.

Lo que sucedió fue que en 2021, el gobierno enmendó, básicamente introdujo reglas llamadas las reglas de intermediarios, tienen un nombre muy largo, pero para nuestro propósito, las llamaré las reglas de TI de 2021. Ahora, curiosamente, esto no se hizo a través de la legislación. Se hizo mediante la emisión de una notificación por parte del gobierno.

Entonces, bajo el poder de creación de normas del gobierno, lo que sucede es que se evita el escrutinio parlamentario, se evita el debate legislativo, por lo que es más fácil aprobar cosas. Así que fue en el ejercicio de sus poderes normativos que el gobierno introdujo estas reglas de TI, que estaban en dos partes, la primera parte trataba con intermediarios y codificaba y añadía nuevas obligaciones de diligencia debida.

Y la segunda parte trataba de los editores de noticias en línea, es decir, los editores de noticias digitales y los proveedores de contenido en línea. La parte controvertida era la regla 4, subcláusula 2 de estas reglas de TI, que efectivamente requiere que estos intermediarios significativos de redes sociales, que son todos los intermediarios, WhatsApp, se incluyan fácilmente.

Entonces, si tienes más de 50 lakh de usuarios, serías clasificado como un intermediario de redes sociales significativo. Y lo que esto hizo, hubo dos partes que se incluyeron en la regla. Primero, hablaré sobre la parte que, de alguna manera, ha sido desafiada pero con la que se ha cumplido completamente. Así que esto responde a tu pregunta, Karthika, donde pensamos, ¿cuál es el argumento del gobierno?

Entonces, el argumento del gobierno, hasta cierto punto, era que todas estas plataformas de redes sociales, ninguna de ellas tiene oficinas en India, ¿verdad? Todas sus oficinas están en los EE. UU. Así que cada vez que tenemos una solicitud de aplicación de la ley, es muy difícil obtener los datos para nosotros, porque dirán que no tenemos los datos almacenados en India, los datos están sujetos a la ley de EE. UU.

Entonces, lo que hicieron estas reglas fue obligar a todos, es decir, a cualquier intermediario significativo de redes sociales, a tener un oficial de quejas residente. Que estuviera basado en India. Y lo que eso hace es que cuando cualquier empresa tiene que tener un oficial que esté basado en India y esté sujeto a la jurisdicción de las leyes indias y de los tribunales indios, fomenta el cumplimiento.

Así que ese fue el argumento del gobierno. Dijeron que necesitamos tener un mejor cumplimiento. Necesitamos tener datos, acceso a datos que se utilizan en crímenes, y por lo tanto necesitamos que todas estas empresas tengan una solicitud de quejas separada. Así que si realmente vas a Facebook, Instagram, WhatsApp, todas estas páginas, tendrán Twitter, todas tienen un oficial de resolución de quejas designado para el propósito de la ley india.

Así que el gobierno hizo eso porque dijeron que es muy difícil para nosotros obtener datos bajo el proceso MLAT, que es el proceso del Tratado de Asistencia Legal Mutua. Así que esa fue la primera parte. La parte más controvertida, y de la que hemos hablado un poco, es que la Regla 4.2 efectivamente requiere que estas empresas, que proporcionan servicios de mensajería, revelen el remitente del mensaje bajo cualquier orden, ¿verdad?

Ahora esta divulgación debe hacerse en casos de seguridad nacional, orden público, cualquier delito, material de abuso sexual infantil, etc. Y el principal desafío que planteó WhatsApp es que dijeron, miren, esto va a romper la encriptación. No podemos divulgar el origen del mensaje a menos que sepamos quién es el originador del mensaje.

y lo que también quiero señalar es que en realidad es muy raro que las plataformas tecnológicas en India, y me interesaría escuchar las experiencias de otros países, pero es bastante raro que las plataformas tecnológicas en India tomen una postura proactiva contra la ley. Por lo general, son demandados o, son, citados como demandados en contra de algún otro peticionario que desafía o la orden del gobierno.

Pero es muy raro que una plataforma de redes sociales desafíe activamente la ley. Y este fue un ejemplo interesante porque fue uno de los primeros casos. Twitter luego siguió con un desafío de bloqueo. Pero esto fue interesante porque es la primera vez que WhatsApp dijo: No podemos identificar al originador de la información.

Hacer eso romperá y deshará la encriptación. No es así como trabajamos. Una vez que creamos una puerta trasera para una persona, tenemos que crear una puerta trasera para todos. Así que la regla en realidad era muy clara. El gobierno estaba tratando de decir: miren, hemos implementado muchas salvaguardas, así que no tienen que romper la encriptación. Cualquier otro medio menos intrusivo es posible.

Las reglas también establecen, según el gobierno, que si tienes que cumplir con la identificación del primer originador, no estás obligado a divulgar el contenido de ningún mensaje, ni ninguna otra información relacionada con el primer originador o sus usuarios.

Y luego las reglas también establecen que cuando el primer originador de la información se encuentra fuera, el gobierno de la India solo se interesa en el primer originador dentro de la India. Así que ves, no solo estás rompiendo la encriptación, también tienes que romperla geográficamente. Entonces tienes que ver quién es el originador, quién es el primero en la India.

Así que creo que esto es todo en términos de antecedentes para este desafío de la Regla 4.2. Lo que diré es que, aunque esto surgió en 2021, finalmente, tres años después, el gobierno, el tribunal, el Tribunal Superior de Delhi ahora está escuchando peticiones que desafían estas reglas, y finalmente las han programado para una audiencia. Y así, esperamos que tal vez en noviembre, diciembre o a principios del próximo año, las audiencias en este caso concluyan.

así que, después de muchos años, en este punto, finalmente vamos a poder ver algunas audiencias. Así que estamos atentos a eso. Y luego, muy rápidamente, también quiero mencionar que, aparte de estas reglas, también habrá reglas de CERT. Estas son las reglas de la Agencia Centralizada de Seguridad, y tratan con los proveedores de VPN.

Y solo quería mencionar eso porque básicamente decía que todos los proveedores de VPN tienen que habilitar obligatoriamente los registros de todos los sistemas de información, todos los usuarios, los nombres, direcciones, detalles de contacto, direcciones de correo electrónico, etcétera, lo cual también fue impugnado por un proveedor de VPN separado, sistemas de proveedores de IFF en ambas peticiones.

Y eso es otra cosa que, si la gente está interesada, podemos hablar más, porque eso trata con la encriptación de una manera diferente o con la privacidad en un escenario distinto. Así que creo que eso es todo por ahora para India.

Karthika Rajmohan - Internet Freedom Foundation: Gracias. Eso fue muy útil. Mucho contexto interesante.

Esto es algo que creo que ha... como dije, jurisprudencia en varias otras jurisdicciones también. Ahora, si pudiéramos escuchar al Sr. Shahzeb Mahmood, ¿le gustaría comenzar con su declaración inicial?

Shahzeb Mahmood - Tech Global Institute: Gracias, Karthika. Me gustaría comenzar abordando algunos de los temas planteados por mis anteriores panelistas que hablaron sobre el asunto.

Entonces, la Dra. Sanjana Patatua, creo que destacó correctamente que la herencia de las leyes coloniales, los idiomas que se utilizan en esta escuela, algunas de las leyes coloniales que compartimos, se han infiltrado en el panorama legal actual que rige Internet, lo cual caracteriza en gran medida cómo se desarrollan las políticas en el sur de Asia.

La Sra. Vrinda Bhandari también mencionó que los casos en los que las empresas tecnológicas persiguen proactivamente casos son una excepción. Y mi investigación también ha demostrado, y coincido en que no es una excepción, y estos se basan predominantemente en las políticas internas de las empresas. Hablaremos más sobre esto. En lo que respecta a Bangladesh, los tribunales han tenido una participación limitada con la jurisprudencia previa.

Hay un caso de hace unos años en el que la división del tribunal superior reconoció que la recopilación rutinaria de detalles de llamadas y grabaciones de audio sin el debido proceso, sin seguir el debido proceso y su divulgación no autorizada como audio filtrado, constituye una violación de los derechos fundamentales otorgados bajo.

El artículo 43 de la Constitución. Sin embargo, la intervención judicial robusta contra la intromisión del estado en las áreas de encriptación, vigilancia y privacidad digital sigue siendo bastante mínima. Así que me gustaría señalar tres problemas que caracterizan esta falta de intervención. El primero es la vigilancia facial y la interceptación, que son llevadas a cabo rutinariamente, de manera encubierta, por el régimen recientemente derrocado, y a menudo se hacía en colaboración con el operador de telecomunicaciones, incluyendo muchas subsidiarias multinacionales.

Esto fue posible gracias a disposiciones amplias en la Ley de Regulación de Telecomunicaciones de Bangladesh y el régimen de licencias de telecomunicaciones. Y

se justificó mediante una interpretación amplia de la excepción del Artículo 43, que permite restricciones a la privacidad por motivos de seguridad nacional y orden público.

Y estos términos problemáticamente permanecen inadecuadamente definidos en Bangladesh. Sé que están bastante bien definidos en India, pero en Bangladesh todavía están relativamente indefinidos. La Corte Suprema de Bangladesh tiene el mandato de evaluar la constitucionalidad de las leyes y las acciones administrativas. Y a lo largo de los años, históricamente, han sido bastante proactivos en las reformas legales a través de fallos suamotu, ejerciendo jurisdicción extraordinaria, emitiendo directrices y tomando decisiones seminales.

Pero la relativa inercia del poder judicial frente a sus acciones. La vigilancia estatal sistémica, durante la última década, es algo que creo que no ha pasado desapercibido. El segundo tema que me gustaría abordar es el tema del cifrado, que es un tema candente en Bangladesh y un excelente estudio de caso para el contagio regional.

India promulgó las reglas de tecnología de la información en 2020-2021, introduciendo la disposición de rastreabilidad, que es esencialmente un requisito para identificar al primer originador de un mensaje compartido en servicios de mensajería u otros servicios intermediarios. Ahora, la Sra. Vrinda Bhandari lo ha cubierto bastante bien, así que no voy a entrar en detalles.

Pero es bastante, es, bastante interesante cómo surgió esto en Bangladesh. Surgió a través de un desafío constitucional, mediante, dos vías de repetición y, involucrando la regulación de contenido. Y el requisito de trazabilidad se introdujo en el primer borrador de la regulación propuesta presentada al Tribunal Superior por la Comisión Reguladora de Telecomunicaciones de Bangladesh.

A diferencia de India, sin embargo, no hay requisitos mínimos, y la disposición estaba destinada a tener alcance extraterritorial. Así que técnicamente, todos los proveedores de servicios, e incluso los no residentes, estaban sujetos a la regulación. Ahora, nosotros, junto con Internet Society y Access Now, creamos conciencia sobre cómo esto perjudicaría a periodistas, defensores de derechos y la oposición, porque en ese momento había una comprensión y conciencia limitada o nula de cómo operaban estas disposiciones.

Y desmentimos muchos mitos al respecto, sobre cómo esta es una solución ineficaz a un problema genuino. Ahora, hay dos argumentos que escuché en ese momento de los defensores de las disposiciones de trazabilidad. El primer argumento es que la trazabilidad es esencial en un país como Bangladesh, para identificar a los perpetradores de la violencia comunal.

Y dentro de la arquitectura constitucional, es tanto razonable como justificado bajo los fundamentos de seguridad nacional y orden público, con un contrapeso frente a consideraciones previas. Y dado que los intermediarios, en la mayoría de los casos,

cumplen solo cuando quieren, es natural esperar resistencia contra solicitudes excesivas.

Ese fue el primer argumento. El segundo argumento, uno que encontré más interesante, es que la trazabilidad se está replanteando como una disposición que viola la privacidad cuando en realidad no lo es, según el argumento. Los intermediarios no necesariamente tienen que romper una encriptación. Y que pueden desarrollar fácilmente puertas traseras tecnológicas que respeten los derechos para ayudar a las autoridades estatales a abordar los problemas reales que se enfrentan en Bangladesh.

el argumento era que no necesariamente tienes que romper una encriptación para hacer cumplir la provisión de rastreabilidad y llegar al primer originador del mensaje. Hay otras formas de hacerlo, tal como Google, por ejemplo, desarrolló Content ID para obtener contenido con derechos de autor. Solo tienes que invertir en tecnología para llegar a un punto donde puedas hacerlo sin romper una encriptación.

Ahora, lo que finalmente sucedió fue que, debido a que no hubo una política o solución tecnológica por parte de los defensores de la provisión de rastreabilidad, esta fue eventualmente eliminada del borrador revisado de la regulación que se presentó al tribunal. Sin embargo, nuevamente, el silencio del tribunal al abordar el tema de manera directa no ha pasado desapercibido.

Y finalmente, y muy rápidamente, el tercer tema es cómo, a lo largo de los años, muchos servicios que permiten la encriptación de extremo a extremo han sido restringidos en Bangladesh, especialmente en la última década y media. Nuevamente, la intervención judicial también ha sido insuficiente aquí. He documentado estas restricciones en un informe sobre apagones de Internet publicado por Internews y Optima, así como en artículos publicados en diarios nacionales.

En aras del tiempo, con eso, me gustaría agradecer al moderador. Por el momento, estoy feliz de responder cualquier pregunta.

Karthika Rajmohan - Internet Freedom Foundation: Muchas gracias. De nuevo, un punto interesante que nos encantaría retomar. Pero ahora, si pudiéramos escuchar a la Sra. Farieha Aziz para que dé su declaración inicial.

Farieha Aziz - Bolo Bhi: Gracias, Karthika. Estoy escuchando muchas similitudes y paralelismos con los oradores anteriores. Permítanme intentar guiarlos a través de lo que ha sucedido este año en Pakistán con respecto a lo que se ha implementado.

Entonces, este fue un año electoral, unas elecciones muy controvertidas, y la cuestión de la legitimidad y los mandatos aún persiste, y nuestros tribunales están literalmente en una encrucijada en este momento. Justo esta mañana temprano, a las 4 a. m., se

aprobó una enmienda constitucional, que pasó por ambas cámaras del parlamento sin ningún debate.

El proceso de nombramiento judicial ha sido enmendado, y esta es una enmienda controvertida nuevamente, donde se va a seleccionar a dedo a un Presidente del Tribunal Supremo, la comisión que va a nombrar jueces ahora está inclinada fuertemente a favor del actual sistema político. Así que vamos a ver cómo se desarrolla todo esto y ahora se han formado bancas constitucionales dentro del Tribunal Supremo y el Tribunal Superior y cómo va a suceder esa bifurcación.

Vamos a ver, porque la litigación era una vía, aunque a veces no se llegaba muy lejos. Pero aun así, los tribunales eran un lugar para disputar algunas de las violaciones que ocurren. Y todo eso ahora está en el aire, y veremos cómo se resuelve. Pero en febrero tuvimos las elecciones, hubo interrupciones de Internet, y luego vemos que X está bloqueado.

Primero no hubo un reconocimiento oficial por parte del gobierno, y luego se supo que había una notificación, y el ministro de información. Y finalmente, hubo básicamente casos ante varios tribunales superiores del país. En este momento, en todos los tribunales superiores del país, hay peticiones pendientes sobre la prohibición de X.

Y lo que finalmente presentaron en el tribunal fue que X ha sido prohibido por motivos de seguridad nacional. Y obviamente, relacionándolo primero con la desinformación relacionada con las elecciones, pero luego también se convirtió en un tema de terrorismo, como también dijo la Dra. Sanjana. Por ejemplo, no solo terrorismo en el contexto de lo que el gobierno se refiere como movimientos separatistas en las diferentes provincias, sino que los jefes militares también han aparecido en televisión para acuñar la frase "terrorismo digital" en relación con los partidos políticos y sus trabajadores que usan las redes sociales. Así que también está ese aspecto.

Y luego, la segunda cosa que el gobierno dijo en su presentación ante el tribunal, y esto es algo de lo que también habló la Sra. Rinder, son las reglas. Así que tenemos las reglas de redes sociales bajo la Ley de Prevención de Delitos Electrónicos, que se promulgó en 2016, la primera ley de ciberdelitos.

Y en ello, lo que se hizo fue, y tenemos, estoy seguro, marcos compartidos. El artículo 19 sobre la libertad de expresión de nuestra constitución fue literalmente copiado y pegado en esta pieza de legislación penal y se le otorgaron a la Autoridad de Telecomunicaciones, en mi opinión, nuestros poderes judiciales y legislativos para esencialmente interpretar y aplicar las excepciones que existen, y tenemos una larga lista de excepciones en el artículo 19. Tienes el derecho a la libertad de expresión, pero sujeto a la gloria del Islam, la seguridad nacional y las relaciones amistosas, y la lista sigue y sigue, para las excepciones. Y hemos visto arbitrariamente cómo la Autoridad de Telecomunicaciones ha bloqueado diferentes sitios web y luego vinieron las reglas de las redes sociales, y nuevamente, tomando prestado de India y otras jurisdicciones, y la

intención siempre fue que queríamos que estas empresas formaran oficinas y nombraran personal.

Y nuevamente, la queja con X en particular es que no cumplen con nuestras solicitudes y no han abierto oficinas según nuestro requisito. Y en Pakistán, ninguna de estas empresas tiene presencia a diferencia de otras regiones. Así que esa es la diferencia. Y nuevamente, el mismo argumento de que les enviamos solicitudes y no cumplen con ellas.

Y así se convierte en esta táctica de zanahoria y palo donde los mantendrán bloqueados hasta que se sienten a la mesa y comiencen a cumplir en cierta medida. Y esto ha sucedido con otras plataformas en el pasado. Entonces eso pasa. Y luego. También escuchamos que el Internet ha estado excesivamente lento, escuchamos que son fallas en los cables submarinos, pero también que se está instalando un llamado firewall nacional y se está utilizando de manera intercambiable con un sistema de monitoreo web o un sistema de gestión, y anteriormente se había adquirido tecnología de inspección profunda de paquetes de Sandvine. Así que esa parte también se añadió y sabes lo que se mencionó, creo, en el contexto indio también es que aquellos que están incorporados localmente, como las telecomunicaciones y los ISP, sienten que pueden hacer muy poco porque sus licencias pueden ser canceladas en cualquier momento y entonces para ellos, es como el camino de menor resistencia, y siguen cumpliendo.

Un caso judicial muy significativo recientemente fue sobre este sistema de vigilancia, el Sistema de Gestión de Interceptación Legal, como se le llamaba. Y ha estado en funcionamiento desde 2013, pero no fue hasta un caso político donde se filtraron audios de la ex Primera Dama y también del hijo de un ex Presidente del Tribunal Supremo, que llevaron el caso a los tribunales, y se llevaron a cabo las audiencias y órdenes.

Resulta que los datos de 4 millones de suscriptores a la vez están siendo pasados por un sistema centralizado, simplemente entregados. y no hay escrutinio. Y cuando el tribunal preguntó bajo qué autoridad están haciendo esto, resultó que nadie, ninguna agencia estaba autorizada. Y entonces lo que sucede es que post facto, se emite una notificación ejecutiva autorizando a la agencia de servicios inter, que es el ISI, a realizar esta vigilancia. Ahora, eso también fue impugnado, pero lo que terminó sucediendo es que la orden del Tribunal Superior fue impugnada ante la Corte Suprema, y la Corte Suprema esencialmente suspendió y restauró el régimen de vigilancia, que anteriormente había sido suspendido por el Tribunal Superior. Así que aquí también estamos viendo cómo diferentes tribunales, diferentes jueces están respondiendo a las cosas.

Las peticiones de ex BAN han estado pendientes durante meses, y las órdenes del Tribunal Superior también están siendo violadas. También estamos en el contexto del llamado firewall. Han podido interrumpir ciertas funcionalidades. Se bloqueó una señal.

Disfunción de medios en WhatsApp. Así que en datos móviles, no podemos transmitir medios de WhatsApp a menos que haya una VPN activada.

entonces, ¿qué capacidad mejorada tienen para poder hacer esto? El registro y bloqueo de VPN, por otro lado, está en marcha, la lista blanca de IPs, que se les pide a las empresas que sigan y están cumpliendo porque también han enfrentado problemas. Así que eso también está en curso en este momento.

Y, por supuesto, tenemos regulaciones. Así que, en términos de, incluso si no es el contenido de los datos a los que pueden tener acceso, los metadatos, como se mencionó, se entregan voluntariamente, y luego tienen sistemas centralizados donde pueden obtener todo eso. Así que quieren saber de dónde se originan los mensajes, quién se está comunicando con quién, incluso si no es el contenido de los datos.

Y por otro lado, en términos de acceder a los datos, hemos tenido redadas generalizadas, arrestos, detenciones ilegales, registros e incautaciones, a pesar de que la ley requiere una orden judicial, no se solicita. Luego se obliga a las personas a proporcionar contraseñas o acceso a sus teléfonos, y así es como se obtiene la información y el contenido, como los chats, con quién te estás comunicando, estableciendo esos vínculos, construyendo esos casos, a veces incluso se utilizan leyes antiterroristas en combinación con las leyes de ciberdelincuencia, y luego todo esto se admite como prueba.

en los juicios, y generalmente estos juicios no son necesariamente siempre para obtener una condena, sino como sigo diciendo, es el proceso como castigo. Una vez que has podido obtener acceso y coaccionar y hacer lo que necesitas, entonces eso es, esencialmente el objetivo se ha logrado. Así que esto es esencialmente donde estamos ahora, donde todo esto todavía, continúa desarrollándose.

Y ahora sentimos que incluso los tribunales, no sabemos qué nos deparará esta nueva estructura bajo la enmienda.

Karthika Rajmohan - Internet Freedom Foundation: Gracias por eso, Farieha, muchos puntos muy interesantes que me encantaría desarrollar. Por último, si pudiéramos tener a Santosh Sigdel, por favor, para que dé su declaración inicial.

Santosh Sigdel - Digital Rights Nepal: Gracias, Karthika. Después de escuchar a la Dra. Sanjana, Vrinda, Shahzab y Farieha, puedo concluir que tenemos una tendencia similar en todo el sur de Asia en cuanto a la regulación del espacio digital y los derechos digitales; las tácticas del gobierno también son similares.

En Nepal, hay dos formas de regulación. Una es a través de órdenes ejecutivas y acciones ejecutivas y la otra es a través de leyes y políticas. En los últimos años, el gobierno ha comenzado a proponer una serie de políticas para regular el espacio

digital. Y en un panorama más amplio, esto también se debió a que, en las últimas elecciones, hubo nuevos partidos políticos y candidatos jóvenes e independientes.

Tomaron el control de los antiguos guardias y en muchas de las, incluyendo la ciudad capital, una densidad metropolitana de, capital. había un joven que logró ser elegido como alcalde. era un rapero. así que estas personas pensaron que todo se debía a las redes sociales. no podemos controlar, no podemos estar en la carrera.

Nosotros, si no podemos controlar las redes sociales. Había una especie de, un sentimiento entre los viejos, partidos, viejos guardias, y, en el frente ejecutivo, ha habido varios casos en los que el gobierno está tratando de.

Vigilar, la comunicación, al mismo tiempo, mantener control sobre la gente. Han propuesto este Servicio de Gestión de Dispositivos de Medios, MDMS, a través de los códigos de cola.

Y al mismo tiempo, existe el Mecanismo de Monitoreo de Tráfico y Control de Fraude en Telecomunicaciones, TeraMox. También hubo corrupción durante los procesos de adquisición y se presentó una petición judicial en contra de esta propuesta en el tribunal. Finalmente, el asunto llegó al Comité Parlamentario y el Comité Parlamentario ha detenido el proceso por ahora, por lo que el TeraMox no ha sido implementado.

Y el año pasado, el gobierno adoptó la Política Nacional de Seguridad Cibernética. Hay una serie de disposiciones problemáticas en la Política Nacional de Seguridad Cibernética, incluyendo la provisión de una Puerta de Enlace Nacional de Internet. Quieren establecer una Puerta de Enlace Nacional de Internet similar a la propuesta en Camboya, donde todo el tráfico entrante al país debe pasar por el punto de control dedicado del gobierno, la red dedicada del gobierno, y todo el tráfico saliente del país también debe pasar por allí y ellos tienen acceso.

Sobre todo el tráfico de Internet.

que está en la política. No sabemos cómo van a implementarlo, pero, después de la presión de la sociedad civil y los medios, ahora lo han renombrado como una especie de política de gestión de banda ancha. ahora están. El último gobierno, ellos tenían un estudio que presentamos.

Derechos Digitales Nepal había presentado una solicitud de acceso a la información para obtener una copia de ese informe, pero no se ha publicado. Así que han constituido un estudio sobre esta política de gestión de banda ancha donde quieren, no quieren hablar de ello como una cuestión nacional, sino que quieren disfrazarlo con otro nombre técnico.

como sabrás, quieren, el mismo argumento que Brinda y otros han proporcionado, que las empresas de redes sociales no están registradas en Nepal, así que el año pasado adoptaron una directriz de redes sociales, que requería que una empresa de redes sociales se registrara en Nepal dentro de tres meses, e inmediatamente después de una semana, TikTok fue prohibido en noviembre pasado, y más de una docena de solicitudes de revisión fueron presentadas en la Corte Suprema.

Y eventualmente TikTok también se acercó al gobierno. Y la tendencia es similar. Como dije antes, TikTok estaba haciendo la diplomacia, esta negociación por la puerta trasera en lugar de desafiar la decisión. Y fueron las organizaciones de la sociedad civil y otros quienes estaban desafiando la decisión.

Desafiando esa decisión y eventualmente llegaron a un acuerdo, negociaron. Y, la organización de la sociedad civil todavía, porque los detalles de la negociación entre TikTok y el gobierno no están muy claros. Así que anteriormente TikTok había dicho que proporcionaría un sistema para marcar el contenido que el gobierno considere inapropiado y revisarán esos contenidos.

Entonces, ahora no sabemos qué. La sociedad civil sospecha de otras posibles negociaciones entre TikTok, pero se reanudó en agosto de 2024. Y, ahora TikTok ha comenzado el proceso de registro en Nepal. Así que es característico. Y después de que lo bloquearon durante un año, ahora están de vuelta en el país y han comenzado este proceso de registro.

el gobierno también ha propuesto dos nuevos proyectos de ley que tienen disposiciones muy problemáticas. Uno es un proyecto de ley sobre el uso y la regulación de las redes sociales, que nosotros, Derechos Digitales Nepal, analizamos y el año pasado proporcionamos comentarios al gobierno, al ministro. Y ahora está en el comité legislativo del gabinete, y se va a presentar en el parlamento en la próxima sesión.

Y solo hay un proyecto de ley de ciberseguridad y tecnología de la información. Y creemos que muchas de las disposiciones de la política nacional de ciberseguridad se implementarán a través de esto. Este proyecto de ley de ciberseguridad tiene muchas disposiciones problemáticas, relacionadas con la eliminación de contenido y otorgar a muchas instituciones el poder de ordenar a las empresas de redes sociales que eliminen contenido.

se ha otorgado el poder a al menos cinco agencias, por lo que si alguna de las agencias encuentra algún contenido problemático, pueden emitir la orden y si en 24 horas no se elimina el contenido, serán multados con 10,000. Hasta 10 lakhs de rupias, que son alrededor de 70,000, creo. Así que esa es la, hay muchas otras disposiciones problemáticas.

Una disposición importante es la responsabilidad de los intermediarios. Así que también hemos analizado eso. Estamos coordinando con otras organizaciones para hacer algunas enmiendas, proponer algunas enmiendas a este proyecto de ley, y también hemos estado trabajando con un miembro del parlamento. Hablando de los tribunales, como compartieron Sajab u otros, los tribunales tienen un papel mínimo, sin embargo, ha habido algunos casos en los que han desempeñado un papel muy importante.

Hace unos años, un juez en funciones de la Corte Suprema fue corrupto, y en ese momento, las agencias de investigación recopilaron más de medio millón de registros de detalles de la corte y miles de contenidos de redes sociales, mensajes de texto, SMS, y en ese momento, solicitamos al tribunal, desafiamos la decisión de las agencias de investigación, y en ese momento, la Corte Suprema emitió órdenes directas para crear leyes que regulen ese proceso, y al mismo tiempo, requirió la sanción judicial.

la aprobación del tribunal de distrito para recopilar cualquier detalle de llamadas de las compañías telefónicas. Así fue como el tribunal pudo implementar el derecho a la privacidad, un derecho a la privacidad consagrado en la constitución. Y hay, varios otros casos que también están actualmente sub judice en la Corte Suprema.

Por ejemplo, ha habido un caso relacionado con Teramox y su implicación en el derecho a la privacidad. Estamos esperando el resultado de este caso sub judice para ver cómo el tribunal defenderá el derecho a la privacidad. Estos son algunos de los escenarios generales. El último punto concluyente es que el gobierno también está intentando, porque ahora, en comparación con los medios tradicionales, los medios en línea han sido muy robustos y críticos, por lo que han propuesto estas directrices para los medios en línea.

Y ahora el gobierno ha propuesto un proyecto de ley para un consejo de medios, que también regulará los medios en línea. Muchos de los temas que hemos estado discutiendo ahora también se verán afectados porque la plataforma de redes sociales de los medios, los medios tradicionales o los medios en línea, también estarán sujetos a este proyecto de ley de redes sociales, ley de tecnología de la información.

Y el impacto también será en la libertad de prensa en los próximos días. Bueno, eso es todo por ahora, como contexto general.

Karthika Rajmohan - Internet Freedom Foundation: Muchas gracias. Hemos recibido muchos puntos muy perspicaces de todos nuestros oradores. Para resumirlo todo, creo que un hilo común que hemos notado entre todos los oradores es que hay ciertas, una lista de razones que los gobiernos parecen estar utilizando para justificar las medidas enérgicas contra el cifrado de extremo a extremo.

En primer lugar, la seguridad nacional. En segundo lugar, mantener el orden público, regular el discurso de odio y las noticias falsas. Y por último, facilitar investigaciones criminales y combatir el abuso sexual infantil.

En primer lugar, me gustaría dirigir una pregunta a la señora Vrinda y a la Dra. Sanjana, solo para que nos cuenten qué están haciendo los tribunales en su país cuando se trata de equilibrar la necesidad de tener un espacio seguro para mujeres y niños frente al derecho a la privacidad y la libertad de expresión.

¿Cuáles son los tipos de argumentos que los tribunales han estado considerando, cuáles son los tipos de actos de equilibrio que han rodeado los debates? si quieres empezar, Vrinda, señora.

Vrinda Bhandari - Internet Freedom Foundation: Sí. Disculpas, Dra. Sanjana. Tuve que irme antes, por eso pedí hablar primero. Entonces, lo que realmente es interesante es que en muchos casos, lo que sucede es que cuando el tribunal está involucrado, y creo que tal vez esta experiencia se compartirá, me interesaría saber eso. Por ejemplo, cuando hablamos de los derechos del niño, lo que a menudo sucede es que no surge en un caso específico, sino que se presenta como lo que en India llamamos litigio de interés público.

Entonces, será presentado por, digamos, alguna organización de derechos infantiles diciendo, miren, esto es un problema serio, necesitamos hacer algo. Y lo que sucede es que, como se presenta como un PIL, muchos de los intermediarios no se involucran, ¿verdad? Así que es el tribunal y el peticionario del PIL. Y entonces, el tribunal realmente no entiende cuáles son los aspectos técnicos, qué significa cuando dices, oh, todos ustedes deben dar sus datos al gobierno en todo momento. Así que, aunque tienen buenas intenciones, creo que lo que vemos a menudo, y esto ha sucedido incluso recientemente, con la Corte Suprema y otro fallo, es que emitirán directrices a varios intermediarios.

Lo cual luego se vuelve difícil de cumplir operativamente, ¿verdad? Pero como nunca han escuchado esas preocupaciones, ese es un problema. También acabo de enviar un enlace a un artículo que tuve el privilegio de escribir con Anya Kovacs, y en realidad analizamos cómo han abordado los tribunales en India las cuestiones de género y sexualidad.

¿Ha ampliado los derechos digitales o en realidad los ha contraído? Así que, he compartido esto en el chat y creo que puedes compartirlo con el panel más amplio también, con la audiencia más amplia también, pero lo que encontramos es que muchas veces, aunque bien intencionado, para proteger a las mujeres o para proteger la moralidad de las mujeres, especialmente cuando tratamos con algo obsceno, los tribunales terminan restringiendo los derechos digitales.

Y consideramos los derechos digitales de manera muy amplia en términos de libertad de expresión, privacidad, todas estas cosas. Así que eso es una cosa. Cuando se trata de seguridad nacional, desafortunadamente, en la mayoría de los casos, el gobierno, el tribunal adopta un enfoque de no intervención. Pueden, en hechos específicos, es muy difícil, así que hubo un caso de bloqueo que surgió en el Tribunal Superior de Delhi, donde había un software, que lo habían impugnado, y había sido bloqueado temporalmente en Jammu y Cachemira.

Y el tribunal dijo, oh, miren, esto es un bloqueo muy temporal, es por preocupaciones de seguridad nacional, es en Cachemira. Y luego casi se vuelve intocable, ¿verdad? ningún tribunal va a ir adelante y realmente desafiar eso. Vimos eso con los cortes de Internet también, cuando sucedió en Cachemira y lo habíamos desafiado en el tribunal y aunque obtuvimos un fallo, en realidad no hubo una implementación específica, como no hubo un fallo sobre las órdenes como tal, como sobre los hechos reales del caso, fue más un fallo sobre cómo deberían tratarse los cortes de Internet, así que lo que a menudo encontramos desafortunadamente es que cuando se trata específicamente de seguridad nacional, se vuelve muy difícil. Para los tribunales, realmente ejercer sus poderes de revisión judicial. Tienden a tener un enfoque más distante. Y lo que hemos tratado de argumentar todo el tiempo es que simplemente decir que algo es un asunto de seguridad nacional no debería ser suficiente.

Tiene que haber alguna base, porque de lo contrario es imposible para ti como peticionario, mostrar apoyo o refutar esa presunción o decir por qué es desproporcionado. Así que ha habido, creo que ahí es donde estamos enfrentando un desafío. Dicho esto, me gustaría recomendar a todos que vean, lean la reciente decisión del Tribunal Superior de Bombay, sobre otro aspecto de estas reglas de TI, y tal vez Karthika, podrías compartir el enlace al fallo, pero donde el tribunal anuló en una proporción de dos a uno.

Hubo un primer veredicto dividido, se llevó a un tercer juez y él falló a favor de los peticionarios. IFF también había asistido en eso. Y donde anularon el establecimiento de una unidad de verificación de hechos, que examinaría información falsa, engañosa o difamatoria en relación con el gobierno.

Entonces, esta era una unidad de verificación de hechos notificada por el gobierno y el tribunal la anuló. Así que fue un desarrollo realmente positivo, pero creo que en general, así es como lo manejamos. Lo siento mucho, necesito irme. Dejaré mis datos de contacto por si alguien quiere ponerse en contacto conmigo.

Me encantaría hacerlo.

Karthika Rajmohan - Internet Freedom Foundation: Muchas gracias. Un placer tenerte aquí. Dra. Sanjana, si desea agregar algo.

Sanjana Hattotuwa - ICT4Peace Foundation: Sí, lo único que puedo agregar a eso es que, como país, no estamos tan desarrollados en nuestro PIL y nuestros tribunales han estado bajo la bota del ejecutivo, de la misma manera en que constitucionalmente se ha construido la oficina del presidente ejecutivo desde 1977, que es cuando nació la constitución actual.

El presidente ejecutivo es intocable. Y quienquiera que haya ocupado ese cargo ha invadido derechos de todas las formas y maneras posibles. Y los tribunales han estado sujetos a esa autoridad, que es casi divina. Cuando hablamos del discurso del sur de Asia hoy en día, y hablamos, por ejemplo, del mandato de Modi.

Hemos tenido presidentes ejecutivos como Raj Paksa desde 2005 en adelante, pisoteando completamente. Así que el PIL ha sido bastante efectivo, pero ha tenido un costo significativo. Activistas han sido arrestados, dañados, heridos, asesinados y ejecutados extrajudicialmente. Y así, incluso embarcarse en PIL, particularmente en temas de seguridad nacional, es enormemente, es un gran obstáculo.

Así que no es fácil. Y tenemos este tipo de escenario kafkiano, que alude a lo que dijo el orador anterior, donde para averiguar cuál es el problema de seguridad nacional, no revelan cuál es el problema de seguridad nacional. Así que se convierte en un escenario un poco absurdo donde no sabes contra qué se supone que debes luchar, pero te dicen que aceptes por autoridad que es un problema de seguridad nacional.

La otra cosa que quería señalar, y de nuevo, cuando escucho los ejemplos de la India, me siento bastante triste. Una de las cosas sobre las que el departamento del Fiscal General y la Corte Suprema juzgaron con respecto a la Ley de Seguridad en Línea, que fue aprobada en el Parlamento de una manera muy inconstitucional también, así que incluso eso está en disputa.

Pero el fallo en sí fue extraordinariamente malo. Y uno de los, para decirlo simplemente, creo que es muy claro cuando lees el fallo que el tribunal no sabe, no está al tanto y no se le ha informado sobre qué constituyen los daños en línea. Así que están operando con una comprensión y noción de regulación, daños, medios y el panorama informativo muy anticuada y desfasada.

Y no parece haber ninguna maldad en la Corte Suprema, ni en la comunidad legal en general, en torno a algunos de los temas que estamos tratando en esta llamada, que es un nudo gordiano. No tienen una jurisprudencia particularmente clara, pero incluso en ese aspecto, el poder judicial de Sri Lanka y la comunidad legal no están atados.

Actualizado. Y eso está muy claro en el juicio. Así que tenemos mucho que ponernos al día en ese sentido, y eso genera miedo autocrático. El resultado neto de eso es que nuestro gobierno y nuestros presidentes ejecutivos tienen una proclividad y una propensión y una cultura de impunidad, dado que incluso la resistencia de PIL es tan débil que hacen lo que les parece adecuado, en línea con lo que otros han hablado en

otros países: regulación arbitraria, leyes arbitrarias, órdenes extra constitucionales o contra constitucionales dadas a las telecomunicaciones, metadatos a gran escala. Y terminaré diciendo que una de las cosas que consideramos un tema de frontera es la llegada de la IA generativa. Y lo que eso significará para las autoridades estatales en la recolección a gran escala de lo que hacen y luego el posterior objetivo de manera individual, institucional o específica de un tema.

de maneras que no hay jurisprudencia legal, jurisprudencia o marco regulatorio actualmente contemplado en el país. Así que eso no es solo un tema de frontera, es en realidad un tema fundamental. Creo que es un tema de primera línea, dado lo que hemos visto en el país, pero eso quizás sea una discusión diferente. Pero de la manera más simple que puedo decir es que, con respecto a la respuesta que se dio desde India, estamos en una etapa mucho más embrionaria, y argumentaría que, como consecuencia, somos más frágiles y estamos más abiertos al miedo y abuso autocrático, como consecuencia de la fragilidad y la naturaleza limitada de nuestros tribunales.

Karthika Rajmohan - Internet Freedom Foundation: Muchas gracias por eso, Dra. Sanjana. Sé que se nos está acabando el tiempo, pero me encantaría conocer rápidamente la opinión de Fareeha sobre esto también. Especialmente porque hemos estado hablando sobre la seguridad nacional, que se utiliza como justificación para la erosión del cifrado de extremo a extremo. Brinda también mencionó que es complicado para los tribunales equilibrar estos intereses.

La Dra. Sanjana también mencionó que, especialmente en tiempos de fragilidad, estos problemas se intensifican aún más. Y dado que mencionaste que en Pakistán, siendo un año electoral, se están realizando nombramientos judiciales en el camino. ¿Cómo está manejando Pakistán este debate entre la seguridad nacional y otros posibles desafíos relacionados con la privacidad, la libertad de expresión y de prensa?

Farieha Aziz - Bolo Bhi: El problema es, como señaló la Dra. Farieha, las afirmaciones infundadas de seguridad nacional. Y esperamos que los tribunales se impongan un poco más y pidan al ejecutivo que especifique qué exactamente está amenazando la seguridad nacional en el contexto de la prohibición de X. y lo han bloqueado. Los ministros están usando X a través de VPNs, que también están bloqueando y registrando.

Solo vean la hipocresía de todo esto. Y al menos cuestionen por qué y para qué propósito y a quién sirve. Así que está ese aspecto. Y nuevamente, en términos de autorizar a una agencia de inteligencia a posteriori para luego llevar a cabo vigilancia masiva, eso también, ¿cuál es el requisito? Y por otro lado, porque muchas peticiones de hábeas corpus por secuestros de ciudadanos se presentan ante los tribunales superiores.

En esos casos, nunca se proporciona el CDR. De alguna manera, las cámaras de la ciudad segura nunca funcionan. Nunca pueden rastrear a las personas que realmente

secuestraron. Ninguno de los sistemas existentes se utiliza para rastrear a los culpables. Pero por otro lado, y además de lo que está sucediendo, también tenemos tribunales que tienen una visión antagonista de las redes sociales.

Y así tuvimos al actual Presidente del Tribunal Supremo, diciendo que todos estos vlogueros que ganan dólares y están en nóminas, etc. Y porque ha habido críticas, obviamente, al Tribunal Supremo y a los jueces y a otros también. Y por otro lado, hemos pasado por esta crisis judicial donde jueces del Tribunal Superior realmente escribieron una carta y salieron a decir que, el establecimiento está controlando, se encontraron cámaras en los dormitorios de los jueces.

pasaron muchas cosas, y la Corte Suprema y el Presidente del Tribunal Supremo básicamente miraron hacia otro lado. Y así, dentro de los tribunales, también tienes algunos inclinándose en una dirección y otros en la otra. Pero los procedimientos por desacato, porque entonces tienes estas guerras de poder donde esos jueces fueron difamados.

porque estaban enfrentándose a la institución y luego también tomaron la ruta del desacato diciendo oh ahora tiene que haber recolección de datos y quiénes están haciendo tendencia con estos hashtags y de dónde se está filtrando esta información personal de los jueces y se están llevando a cabo campañas en su contra, incluyendo a los medios de comunicación principales, así que hay mucha fricción dentro del poder judicial también y ahora con el Dr.

Farieha mencionó las botas militares y eso es todo. Hemos tenido una historia judicial accidentada, pero al mismo tiempo, aquí en el Ejecutivo, hay más arraigo en términos de, tú, tú quieres una judicatura que sea independiente y que desafíe al Ejecutivo cuando los ciudadanos acuden a los tribunales contra el Ejecutivo.

Quieres que los tribunales puedan cumplir. Sin embargo, cuando eso sucede, los jueces son marginados o, por ejemplo, la orden del Tribunal Superior de Islamabad, que luego fue suspendida por la Corte Suprema, y ahora quieren simplemente reorganizar a los jueces y también todo, dentro del poder judicial. Así que en este momento, no sabemos.

Además, toda la práctica de simplemente tomar los dispositivos. Las personas son secuestradas, arrestadas, se les quitan sus dispositivos. Así que no hay protección. Incluso un proyecto de ley de protección de datos, que está en proceso, proporciona más acceso al gobierno, facilita más el acceso del gobierno a los datos en lugar de protegerlos.

Y para mí, siempre, la intención está en duda. Las narrativas son las mismas. Tenemos que proteger a los ciudadanos y también a las mujeres y los niños. Esas narrativas proteccionistas y paternalistas, pero nada de eso realmente sucede. Y bajo el disfraz de todo eso y la seguridad nacional, la intromisión del estado se afianza.

Y eso es esencialmente lo que hemos visto a través de la ley, la creación de normas dentro del poder judicial, problemas de actitud. y en este punto, honestamente, incluso los logros que hemos obtenido, pueden revertirse, dado cómo ahora se van a reestructurar los tribunales, si la jurisprudencia seguirá aplicándose, si vamos a empezar de cero, y quién va a encabezar esos tribunales constitucionales.

que obviamente creemos que serán designados a dedo para bloquear cualquier tipo de defensa y litigio basado en derechos. Y hay varios casos pendientes, pero no están avanzando. Sí.

Karthika Rajmohan - Internet Freedom Foundation: Maravilloso. Eso fue realmente interesante. Desearía que pudiéramos continuar por más tiempo, pero si pudiéramos pasar a la sesión de preguntas y respuestas. Bien, creo que nos hemos pasado del tiempo. Tendremos que cerrar el panel aquí. Lo siento mucho, Santosh y Shazeb. Tenía específicamente un par de preguntas que quería hacerles, pero nos estamos quedando sin tiempo. Así que creo que tendremos que cerrar la sesión aquí. Quiero aprovechar la oportunidad para agradecer a todos nuestros maravillosos panelistas.

Ha sido una discusión excelente, muy enriquecedora e informativa, y ha sido un placer participar en esta conversación con todos ustedes. Muchas gracias.