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

Les tribunaux à la croisée des chemins : défendre les droits numériques contre la répression de l'encryption en Asie du Sud

Raquel Kroich - Internet Society: Bonjour, bienvenue à tous à "Chiffrer une Date pour Protéger Demain". Nous commençons avec la première session de la journée, "Les Tribunaux à la Croisée des Chemins : Défendre les Droits Numériques contre la Répression du Chiffrement en Asie du Sud".

Je vais passer la parole à Karthika, pour qu'elle puisse commencer la session d'aujourd'hui.

Karthika Rajmohan - Internet Freedom Foundation: Merci, Raquel. Bonjour à tous. Bienvenue au Sommet de la Journée Mondiale du Chiffrement 2024. Je suis Karthika Rajmohan. Je suis conseillère juridique associée à la Fondation pour la Liberté sur Internet. Nous sommes une organisation de défense des libertés civiles basée à New Delhi, travaillant sur les questions de droits numériques, et je vais modérer la session d'aujourd'hui.

L'IFF est ravi d'organiser un panel dans le cadre du Sommet GED. La discussion d'aujourd'hui, comme l'a mentionné Raquel, portera sur les codes à la croisée des chemins. Défendre les droits numériques contre les répressions sur le chiffrement en Asie du Sud. L'inspiration derrière ce panel et le contexte sur lequel nous nous appuyons sont les efforts croissants des gouvernements pour restreindre le chiffrement de bout en bout sous le prétexte de la sécurité nationale et de la prévention du crime.

Nous sommes très heureux d'avoir un panel de conférenciers extrêmement qualifiés et estimés, experts en droits numériques provenant de divers pays d'Asie du Sud. Je vais brièvement présenter tous les intervenants. Tout d'abord, nous avons le Dr Sanjana Hattotuwa. Il est expert en désinformation à la Fondation ICT for Peace, où il étudie les désordres informationnels et leur impact sur la démocratie et la société.

Ensuite, nous avons Mme Vrinda Bhandari. Elle est une avocate indépendante qui plaide pour la liberté d'expression et les droits numériques en Inde. Elle est également conseillère auprès de l'Internet Freedom Foundation. Ensuite, nous avons M. Shahzeb Mahmood. Il est chercheur principal à l'Institut Tech Global, où son travail se concentre principalement sur la régulation des contenus en ligne, l'IA et les deepfakes.

Ensuite, nous avons Mme Farieha Aziz. Elle est cofondatrice de Bolo Bhi, une organisation de la société civile axée sur la défense, la politique et la recherche dans les domaines des droits numériques et de la responsabilité civique. Et enfin, nous avons M. Santosh Sigdel, le directeur exécutif de Digital Rights Nepal, une initiative à but non lucratif dédiée à la protection et à la promotion des droits numériques au Népal.

Maintenant que nous avons présenté nos panélistes, nous pourrions peut-être passer à quelques déclarations liminaires. Peut-être que les panélistes pourraient commencer par nous donner un contexte sur la situation dans leurs pays respectifs, quels types de répressions les gouvernements ont menées contre le chiffrement de bout en bout, et les types de justifications qui sont utilisées à cet égard.

Je pense que pour les déclarations d'ouverture, nous pourrions peut-être commencer avec le Dr. Sanjana. Si vous voulez bien commencer.

Sanjana Hattotuwa - ICT4Peace Foundation: Oui, merci et heureux d'être ici. Je vais faire court. Pour ceux de la région, le Sri Lanka est une histoire bien connue. Nous venons d'avoir une élection présidentielle conséquente, donc nous ne savons pas si ce que nous avons vu dans le passé se poursuivra à l'avenir. On espère que non. Mais le contexte général du pays est une histoire familière pour d'autres pays d'Asie du Sud également, où l'autorité de l'État, l'autorité exécutive et l'impunité ont entravé la liberté d'expression et les droits fondamentaux dans le pays pendant des décennies, bien avant les réseaux sociaux, mais cela a été exacerbé par l'intérêt croissant de l'État pour les communications privées privilégiées et l'État sécuritaire en particulier sous le prétexte de lutter contre le terrorisme, mais aussi au Sri Lanka, avec l'argument de la protection des femmes et des enfants, où il y a eu beaucoup de régulations et de lois adoptées ou envisagées pour prétendument protéger les femmes et les enfants, mais qui sont assez accablantes en ce qui concerne les principes fondamentaux.

Je vais juste en mentionner deux. L'une est une loi absolument draconienne, sans précédent dans l'histoire législative du pays, appelée la Loi sur la sécurité en ligne, qui est entrée en vigueur en janvier de cette année. C'est une longue histoire sur la façon dont elle a vu le jour, mais maintenant elle fait partie de nos textes de loi, et c'est, je ne

peux pas utiliser, à cause du Code de conduite, des jurons lors de cet appel, mais c'est horrible.

C'est antithétique à tous les droits humains imaginables dans la Constitution. C'est extraterritorial, cela s'applique à tout le monde. Sur Terre, aussi incroyable que cela puisse paraître, cela remonte au premier moment où vous auriez utilisé Internet, et c'est incroyablement intrusif pour la vie privée, c'est sous l'autorité de l'exécutif.

Ce qui pose un gros problème en raison de la nature constitutionnelle du pays et de la puissance de l'exécutif. Cela permet à la loi de s'introduire dans n'importe quel appareil, n'importe où, à tout moment, sur n'importe quoi, sur une catégorie de contenu appelée contenu interdit. Et ce n'est pas moi qui l'invente, c'est dans la loi. Cela peut signifier n'importe quoi.

Donc, ce n'est pas très clair. En fait, il y a des clauses dans la loi qui se lisent comme un roman d'amour, car il est dit que si vous dites quelque chose qui blesse les sentiments d'une communauté, cela peut être un point d'intervention possible. Et j'ai dit que je n'avais pas de sentiments quand j'écrivais des lettres d'amour ou quand j'en recevais, mais c'est très étrange de trouver ce genre de langage dans une loi.

Donc, l'OSA peut forcer la divulgation et c'est en fait vraiment assez grave. Cela impacte indirectement le chiffrement de bout en bout. Dans un contexte où vous devez comprendre qu'au Sri Lanka, du moins, nous sommes un pays très violent et le ministère de la Défense, régulièrement et depuis des décennies, a, sans aucun processus légal, tordu le bras des opérateurs télécoms pour obtenir les informations qu'ils veulent.

Pour être très clair, il n'est pas nécessaire au Sri Lanka de saper le chiffrement de bout en bout (E2EE) quand on peut en fait tordre le bras des opérateurs télécoms pour obtenir des métadonnées ou certaines données que l'on pourrait vouloir sur des individus ou des institutions ciblés, qui sont généralement des militants des droits de l'homme. Je terminerai en disant qu'il y a une deuxième loi qui est au stade de projet et nous ne savons pas si elle va être adoptée avec le nouveau président exécutif et le gouvernement, les élections parlementaires ayant lieu dans quelques semaines.

Nous ne connaissons pas le calendrier, mais c'est une forme de gouvernement. Elle allait être introduite très bientôt, appelée la Loi contre le terrorisme. Nous avons donc une Loi de prévention du terrorisme, qui est draconienne, mais maintenant nous avons une Loi contre le terrorisme, qui prétend ostensiblement corriger la LPT, mais qui est en réalité bien pire.

Et ici, nous prenons une page de l'Inde, où, sur WhatsApp, les Indiens sur cet appel peuvent parler de l'affaire de la Haute Cour de Delhi avec Facebook, Meta et WhatsApp, et tout le dilemme concernant leur possible départ du plus grand marché s'ils étaient contraints de compromettre leur propre chiffrement de bout en bout avec WhatsApp.

Mais l'article 65 du projet de loi proposé de l'ATA du Sri Lanka est exactement la même chose.

Cela obligera tous les intermédiaires Internet et, en réalité, n'importe qui, à remettre leurs clés, à divulguer leurs informations. Donc, cela touche le niveau des intermédiaires, le niveau des plateformes, mais aussi le niveau individuel. Et c'est, je ne vais pas lire la clause, mais il n'y a rien de semblable dans nos livres de lois.

Et mon point de vue a été que, si WhatsApp et Meta voulaient quitter l'Inde en raison de ce qu'ils étaient peut-être contraints de faire, nous, en tant que pays, sommes moins que le marché de Mumbai. J'ai donc alerté les gens en leur demandant ce que Meta ferait au Sri Lanka si cette loi voyait le jour. Je terminerai en disant que nous ne sommes pas aussi mauvais que l'Inde, le Bangladesh ou le Pakistan ou certains autres pays, mais la propension, la préférence politique et le biais sont de saper.

communications privilégiées cryptées. Et cela devient maintenant un point central pour ceux du ministère de la Défense et du gouvernement, dans le but de s'immiscer dans l'activisme de la société civile et d'accéder aux communications privilégiées qu'ils jugent gênantes parce qu'elles sont gênantes pour eux.

Donc, l'argument est fait autour de la prétendue lutte contre le terrorisme, la protection des hommes et des enfants. Mais nous savons tous, j'espère, sur cet appel et dans l'audience, que le résultat final est absolument préjudiciable aux principes fondamentaux. Voilà donc le contexte général du Sri Lanka tel qu'il se présente aujourd'hui.

Karthika Rajmohan - Internet Freedom Foundation: Merci pour cela. C'était très utile. Il y a beaucoup de points sur lesquels j'aimerais approfondir, mais nous y reviendrons plus tard. Maintenant, si Mme Vrinda Bhandari pouvait commencer sa déclaration d'ouverture.

Vrinda Bhandari - Internet Freedom Foundation: Bonjour. Je pense que c'est parfait de continuer, étant donné que nous avons déjà vu le contexte du Sri Lanka, donc je pense que l'Inde suit, et je vais peut-être commencer par parler du défi, qui a été lancé par WhatsApp.

Ce qui s'est passé, c'est qu'en 2021, le gouvernement a amendé, en gros, introduit des règles appelées les règles des intermédiaires, elles ont un nom très long, mais pour notre propos, je vais les appeler les règles IT de 2021. Maintenant, ce qui est intéressant, c'est que cela n'a pas été fait par le biais d'une législation. Cela a été fait par le gouvernement en émettant une notification.

Donc, en vertu du pouvoir réglementaire du gouvernement, ce qui se passe, c'est que vous évitez le contrôle parlementaire, vous évitez le débat législatif, donc il est plus

facile de faire passer des choses. C'est donc dans l'exercice de ses pouvoirs réglementaires que le gouvernement a introduit ces règles informatiques, qui étaient en deux parties. La première partie traitait des intermédiaires et codifiait et ajoutait de nouvelles obligations de diligence raisonnable.

Et la deuxième partie concernait les éditeurs de nouvelles en ligne, donc les éditeurs de nouvelles numériques, et les fournisseurs de contenu en ligne. La partie controversée était la règle 4 sous-clause 2 de ces règles informatiques, qui exige effectivement que ces intermédiaires de médias sociaux significatifs, ce qui inclut chaque intermédiaire, WhatsApp, soient facilement inclus.

Donc, si vous avez plus de 50 lakh utilisateurs, vous seriez classé comme un intermédiaire de médias sociaux significatif. et ce que cela a fait, donc il y avait deux parties dans la règle. D'abord, je vais parler de la partie qui, d'une certaine manière, a été contestée mais a été complètement respectée. Cela répond à votre question, Karthika, où nous nous demandons, quel est l'argument du gouvernement ?

Donc, l'argument du gouvernement, dans une certaine mesure, était que toutes ces plateformes de médias sociaux, aucune d'entre elles n'a de bureaux en Inde, n'est-ce pas ? Tous leurs bureaux sont aux États-Unis. Donc, chaque fois que nous avons une demande d'application de la loi, il est très difficile d'obtenir les données pour nous. parce qu'ils diront, nous n'avons pas les données ne sont pas stockées en Inde, les données sont soumises à la loi américaine.

Donc, ce que ces règles ont fait, c'est qu'elles ont exigé que chaque intermédiaire de médias sociaux significatif ait un responsable des plaintes résident. Qui soit basé en Inde. Et ce que cela fait, c'est que lorsque toute entreprise doit avoir un responsable qui doit être basé en Inde et est donc soumis très directement à la juridiction des lois indiennes et des tribunaux indiens, cela encourage la conformité.

C'était donc l'argument du gouvernement. Ils ont dit que nous devons avoir une meilleure conformité. Nous devons avoir des données, accéder aux données utilisées dans les crimes, et donc nous avons besoin que toutes ces entreprises aient une demande de grief distincte. Donc, si vous allez sur Facebook, Instagram, WhatsApp, toutes ces pages, elles auront Twitter, elles ont toutes un responsable de traitement des griefs désigné pour les lois indiennes.

Donc, le gouvernement a agi ainsi parce qu'il a déclaré qu'il était très difficile pour nous d'obtenir des données dans le cadre du processus MLAT, qui est le processus de Traité d'Assistance Juridique Mutuelle. Donc, c'était la première partie. La partie plus controversée, et ce que nous avons abordé un peu, c'est que la Règle 4.2 exige effectivement que ces entreprises, qui fournissent des services de messagerie, divulguent l'expéditeur du message sur n'importe quel ordre, n'est-ce pas ?

Cette divulgation doit maintenant être faite pour des cas de sécurité nationale, d'ordre public, d'infractions, de matériel d'abus sexuel sur enfants, etc. Et le principal défi que WhatsApp a soulevé est qu'ils ont dit, regardez, cela va briser le chiffrement. Nous ne pouvons pas divulguer l'origine du message à moins de savoir qui est l'expéditeur du message.

et ce que je veux également souligner, c'est qu'il est en fait très rare pour les plateformes technologiques en Inde, et j'aimerais connaître les expériences d'autres pays, mais il est assez rare pour les plateformes technologiques en Inde de contester activement la loi. Habituellement, elles sont des répondants ou, elles sont citées comme répondants contre, un autre pétitionnaire contestant ou l'ordre du gouvernement.

Mais il est très rare qu'une plateforme de médias sociaux conteste activement la loi. Et donc, c'était un exemple intéressant parce que c'était l'un des premiers cas. Twitter a ensuite suivi avec une contestation de blocage. Mais c'était intéressant parce que c'était la première fois que WhatsApp disait : Nous ne pouvons pas identifier l'origine de l'information.

Faire cela brisera et déchiffrera le cryptage. Ce n'est pas ainsi que nous fonctionnons. Une fois que nous créons une porte dérobée pour une personne, nous devons en créer une pour tout le monde. Donc, la règle était en fait très claire. Le gouvernement essayait de dire, regardez, nous avons mis en place de nombreuses garanties, donc vous n'avez pas à briser le cryptage. D'autres moyens moins intrusifs sont possibles.

Les règles prévoient également, selon le gouvernement, que si vous devez vous conformer à l'identification du premier émetteur, vous n'êtes pas tenu de divulguer le contenu de tout message, ni toute autre information liée au premier émetteur ou à ses utilisateurs.

Et puis, les règles stipulent également que lorsque le premier émetteur de l'information se trouve à l'extérieur, le gouvernement de l'Inde ne s'intéresse qu'au premier émetteur situé en Inde. Donc, vous voyez, il ne s'agit pas seulement de briser le chiffrement, il faut aussi le faire géographiquement. Il faut donc identifier qui est l'émetteur, qui est le premier en Inde.

donc je pense que c'est tout en termes de contexte pour ce défi de la Règle 4.2. Ce que je dirai, c'est que bien que cela soit apparu en 2021, enfin, trois ans plus tard, le gouvernement, la cour, la Haute Cour de Delhi entend maintenant des pétitions contestant ces règles, et ils ont finalement fixé une date pour l'audience. Et donc nous espérons que peut-être en novembre, décembre, ou au début de l'année prochaine, les audiences à ce sujet se concluront.

donc en fait, après de nombreuses années, sur ce point, nous allons enfin pouvoir assister à des audiences. Nous sommes donc en attente de cela. Et puis très rapidement, je veux aussi mentionner, en plus de ces règles, il y aura également des

règles CERT. Ce sont les règles de l'agence de centralisation de la sécurité, et cela concerne les fournisseurs de VPN.

Et je voulais juste aborder ce point parce que cela dit essentiellement que tous les fournisseurs de VPN doivent obligatoirement activer les journaux de tous les systèmes d'information, tous les utilisateurs, les noms, adresses, coordonnées, adresses e-mail, etc., ce qui a également été contesté par un autre fournisseur de VPN, les systèmes de fournisseur IFF dans ces deux pétitions.

Et donc, c'est une autre chose dont nous pouvons parler davantage si les gens sont intéressés, car cela traite du chiffrement d'une manière différente ou de la confidentialité dans un autre type de scénario. Je pense que c'est tout pour l'instant pour l'Inde.

Karthika Rajmohan - Internet Freedom Foundation: Merci. C'était très utile. Beaucoup de contexte intéressant.

C'est quelque chose que je pense avoir... donc j'ai dit la jurisprudence à travers, plusieurs autres juridictions également. Maintenant, si nous pouvions entendre M. Shahzeb Mahmood, aimeriez-vous commencer par votre déclaration d'ouverture ?

Shahzeb Mahmood - Tech Global Institute: Merci, Karthika. J'aimerais donc commencer par aborder certaines des questions soulevées par mes précédents intervenants sur le sujet.

Donc, Dr. Sanjana Patatua, je pense qu'il a souligné très justement que l'héritage des lois coloniales, les langues utilisées dans cette école, certaines des lois coloniales que nous partageons, ont imprégné le paysage juridique actuel régissant Internet, ce qui caractérise fortement la manière dont les politiques sont développées en Asie du Sud.

Mme Vrinda Bhandari a également mentionné que les cas où les entreprises technologiques poursuivent proactivement des affaires sont une exception. Et mes recherches ont également montré, et je suis d'accord, que ce n'est pas une exception, et que cela repose principalement sur les politiques internes des entreprises. Nous en parlerons davantage. En ce qui concerne le Bangladesh, les tribunaux ont eu un engagement limité avec la jurisprudence antérieure.

Il y a quelques années, il y a eu un cas où la division de la haute cour a reconnu que la collecte systématique de détails d'appels et d'enregistrements audio sans suivre la procédure légale et leur divulgation non autorisée en tant qu'audio divulgué constitue une violation des droits fondamentaux garantis.

Article 43 de la Constitution. Pourtant, l'intervention judiciaire robuste contre l'empiètement de l'État dans les domaines du chiffrement, de la surveillance et de la vie

privée numérique reste assez minimale. J'aimerais donc souligner trois problèmes qui caractérisent ce manque d'intervention. Le premier est la surveillance faciale et l'interception, qui sont régulièrement effectuées de manière clandestine par le régime récemment évincé, souvent en collaboration avec l'opérateur de télécommunications, y compris de nombreuses filiales multinationales.

Cela a été rendu possible par des dispositions larges dans la loi sur la régulation des télécommunications du Bangladesh et le régime de licences télécoms. Et justifié par une interprétation extensive de l'exception de l'article 43, qui permet des restrictions sur la vie privée pour des raisons de sécurité nationale et d'ordre public.

Et ces termes restent problématiquement mal définis au Bangladesh. Je sais qu'ils sont assez bien définis en Inde, mais au Bangladesh, ils restent relativement indéfinis. La Cour suprême du Bangladesh a le mandat d'évaluer la constitutionnalité des lois et des actions administratives. Et au fil des ans, historiquement, elle a été assez proactive dans les réformes juridiques par le biais de décisions suamotu, en exerçant une juridiction extraordinaire, en émettant des directives, en rendant des décisions marquantes.

Mais l'inertie relative de la justice face à leurs actions. La surveillance systémique de l'État, au cours de la dernière décennie, est quelque chose que je crois n'a pas passé inaperçu. Le deuxième point que j'aimerais aborder est la question du chiffrement, qui est un problème latent au Bangladesh, et un excellent cas d'étude pour la contagion régionale.

L'Inde a promulgué les règles de la technologie de l'information en 2020-2021, introduisant la disposition de traçabilité, qui est essentiellement une exigence pour identifier le premier émetteur d'un message partagé sur des services ou d'autres services intermédiaires de messagerie. Maintenant, Mme Vrinda Bhandari l'a bien couvert, donc je ne vais pas entrer dans les détails.

Mais c'est assez, c'est, assez intéressant de voir comment cela s'est produit au Bangladesh. Cela est venu par le biais d'un défi constitutionnel, par, deux voies de répétition et, cela, impliquant la régulation du contenu. Et l'exigence de traçabilité a été introduite dans le premier projet de règlement proposé soumis à la Haute Cour par la Commission de Régulation des Télécommunications du Bangladesh.

Contrairement à l'Inde, cependant, il n'y a pas de seuils requis, et la disposition était censée avoir une portée extraterritoriale. Donc techniquement, tous les fournisseurs de services, et même les non-résidents étaient concernés par la réglementation. Nous avons donc, avec l'Internet Society et Access Now, sensibilisé sur la manière dont cela nuirait aux journalistes, aux défenseurs des droits et à l'opposition, car à l'époque, il y avait peu ou pas de compréhension et de sensibilisation sur le fonctionnement de ces dispositions.

Et nous avons démystifié beaucoup de choses à ce sujet, en montrant comment c'est une solution inefficace à un problème réel. Maintenant, il y avait deux arguments à l'époque que j'ai entendus de la part des partisans des dispositions de traçabilité. Le premier argument est que la traçabilité est essentielle dans un pays comme le Bangladesh, pour identifier les auteurs de violences communautaires.

Et dans le cadre constitutionnel, cela est à la fois raisonnable et justifié pour des raisons de sécurité nationale et d'ordre public, avec un contrepoids par rapport aux considérations précédentes. Et étant donné que les intermédiaires, dans la plupart des cas, ne se conforment que lorsqu'ils le souhaitent, une résistance face à des demandes excessives est naturellement attendue.

C'était donc le premier argument. Le deuxième argument, que j'ai trouvé plus intéressant, est que la traçabilité est présentée comme une disposition violant la vie privée alors qu'en fait ce n'est pas le cas, selon l'argument. Les intermédiaires n'ont pas nécessairement à casser un chiffrement. Et qu'ils peuvent facilement développer des portes dérobées technologiques respectueuses des droits pour aider les autorités de l'État à résoudre les problèmes concrets auxquels le Bangladesh est confronté.

L'argument était que vous n'avez pas nécessairement besoin de casser un chiffrement pour appliquer la disposition de traçabilité et remonter jusqu'au premier expéditeur du message. Il existe d'autres moyens de le faire, tout comme Google, par exemple, a développé Content ID pour identifier le contenu protégé par le droit d'auteur. Il suffit d'investir dans la technologie pour arriver à un point où vous pouvez le faire sans casser un chiffrement.

Finalement, ce qui s'est passé, c'est qu'en l'absence de politique ou de solution technologique proposée par les partisans de la traçabilité, cette disposition a été finalement retirée de la version révisée du règlement soumise à la cour. Cependant, le silence de la cour sur cette question n'est pas passé inaperçu.

Et enfin, très rapidement, le troisième problème est de savoir comment, au fil des ans, de nombreux services permettant le chiffrement de bout en bout ont été restreints au Bangladesh, surtout au cours de la dernière décennie et demie. Là encore, l'intervention judiciaire a fait défaut. J'ai documenté ces restrictions dans un rapport sur les coupures d'Internet publié par Internews et Optima, ainsi que dans des articles publiés dans des quotidiens nationaux.

Dans l'intérêt du temps, sur ce, je voudrais remercier le modérateur. Pour le moment, je suis prêt à répondre à toutes les questions.

Karthika Rajmohan - Internet Freedom Foundation: Merci beaucoup. Encore une fois, un point intéressant soulevé auquel nous aimerions revenir. Mais maintenant, si nous pouvions avoir Mme Farieha Aziz pour faire sa déclaration d'ouverture.

Farieha Aziz - Bolo Bhi: Merci, Karthika. J'entends tellement de similitudes et de parallèles avec les intervenants précédents. Permettez-moi de vous guider à travers cette année au Pakistan en ce qui concerne ce qui a été mis en place.

Donc, c'était une année électorale, des élections très controversées, et la question de la légitimité et des mandats persiste encore, et nos tribunaux sont littéralement à la croisée des chemins en ce moment. Ce matin même, à 4 heures du matin, un amendement constitutionnel a été adopté en force par les deux chambres du parlement, sans aucun débat.

Le processus de nomination judiciaire a été modifié, et c'est encore un amendement controversé, où le choix du juge en chef va se faire, la commission qui va nommer les juges est maintenant fortement biaisée en faveur de l'actuel système politique. Nous allons donc voir comment tout cela va se dérouler et maintenant des bancs constitutionnels ont été formés au sein de la Cour suprême et de la Haute Cour et comment cette bifurcation va se produire.

Nous allons voir, car les litiges étaient une voie, même si parfois on n'allait pas très loin. Mais les tribunaux restaient un lieu pour contester certaines violations qui se produisaient. Et tout cela est maintenant incertain, et nous verrons comment tout cela se résout. Mais en février, nous avons eu les élections, des perturbations d'Internet se produisaient, et ensuite nous voyons que X est bloqué.

D'abord, il n'y avait aucune reconnaissance officielle de la part du gouvernement, puis il s'est avéré qu'il y avait une notification, et le ministre de l'information. Et enfin, il y avait essentiellement des affaires devant diverses hautes cours du pays. Actuellement, dans toutes les hautes cours du pays, il y a des pétitions en attente concernant l'interdiction de X.

Et ce qu'ils ont finalement soumis au tribunal, c'est que X a été interdit pour des raisons de sécurité nationale. Et évidemment, en le liant d'abord à la désinformation liée aux élections. Mais ensuite, il s'est également agi de terrorisme, comme l'a également mentionné le Dr Sanjana, par exemple, et pas seulement du terrorisme dans le contexte de ce que le gouvernement appelle les mouvements séparatistes dans les différentes provinces, mais les chefs militaires sont également apparus à la télévision pour inventer l'expression "terrorisme numérique" en relation avec les partis politiques et leurs militants utilisant les réseaux sociaux. Donc, il y a aussi cet aspect-là.

Et puis la deuxième chose que le gouvernement a dite dans sa soumission au tribunal, et c'est quelque chose dont Mme Rinder a également parlé, ce sont les règles. Nous avons donc les règles des réseaux sociaux en vertu de la loi sur la prévention des crimes électroniques, qui a été promulguée en 2016, la première loi sur la cybercriminalité.

Et dans ce cadre, ce qui a été fait, et nous avons, j'en suis sûr, des cadres partagés. L'article 19 sur la liberté d'expression de notre constitution a littéralement été copié-

collé dans cette législation pénale et l'Autorité des télécommunications s'est vue attribuer, à mon avis, nos pouvoirs judiciaires et législatifs pour essentiellement interpréter et appliquer les exceptions qui existent, et nous avons une longue liste d'exceptions dans l'article 19. Vous avez le droit à la liberté d'expression, mais sous réserve de la gloire de l'Islam, de la sécurité nationale et des relations amicales, et la liste continue encore et encore, pour les exceptions. Et nous avons vu arbitrairement comment l'Autorité des télécommunications a bloqué différents sites web et ensuite sont venues les règles des réseaux sociaux, et encore une fois, en empruntant à l'Inde et à d'autres juridictions, et l'intention a toujours été que nous voulons que ces entreprises ouvrent des bureaux et nomment du personnel.

Et encore une fois, le reproche avec X en particulier est qu'ils ne se conforment pas à nos demandes et n'ont pas ouvert de bureaux selon nos exigences. Et au Pakistan, aucune de ces entreprises n'a de présence contrairement à d'autres régions. Donc, c'est la différence. Et encore une fois, le même argument que nous leur envoyons des demandes et qu'ils ne se conforment pas à ces demandes.

Et donc, cela devient une tactique de la carotte et du bâton où ils les maintiennent bloqués jusqu'à ce qu'ils viennent à la table et commencent à se conformer dans une certaine mesure. Et cela s'est produit avec d'autres plateformes dans le passé. Donc, cela arrive. Et puis. Nous entendons également que l'Internet a été excessivement lent, on nous dit que ce sont des pannes de câbles sous-marins, mais aussi qu'un soi-disant pare-feu national est en cours d'installation et utilisé de manière interchangeable avec un système de surveillance du web ou un système de gestion, et auparavant il y avait eu des achats de Sandvine, une technologie d'inspection approfondie des paquets. Donc, cette partie aussi s'ajoute et vous savez ce qui a été mentionné, je pense, dans le contexte indien également, c'est que ceux qui sont localement incorporés, donc les opérateurs de télécommunications et les FAI, sentent qu'ils peuvent faire très peu parce que leurs licences peuvent être annulées à tout moment et donc pour eux, c'est comme le chemin de moindre résistance, et ils se conforment.

Une affaire judiciaire très importante récemment concernait ce système de surveillance, le Système de Gestion d'Interception Légale, comme on l'appelait. Et il est en place depuis 2013, mais ce n'est que dans une affaire politique où des enregistrements audio avaient été divulgués, de l'ancienne Première Dame et aussi du fils d'un ancien Président de la Cour Suprême, qu'ils sont allés en justice, et les audiences et ordonnances ont suivi.

Il s'avère que les données de 4 millions d'abonnés à la fois sont transmises à un système centralisé, simplement remises sans aucune surveillance. Et lorsque le tribunal a demandé sous quelle autorité cela se faisait, il s'est avéré qu'aucune agence n'était autorisée. Et donc, ce qui se passe, c'est qu'après coup, une notification exécutive est émise autorisant l'agence interservices, qui est l'ISI, à mener cette surveillance. Cela a également été contesté, mais ce qui s'est passé, c'est que l'ordonnance de la Haute Cour a été contestée devant la Cour suprême, et la Cour suprême a essentiellement

suspendu et rétabli le régime de surveillance, qui avait été suspendu précédemment par la Haute Cour. Nous voyons donc ici comment différents tribunaux, différents juges réagissent aux choses.

Les pétitions de l'ex BAN sont en attente depuis des mois maintenant, et les ordonnances de la Haute Cour sont également violées. Nous sommes également dans le contexte du soi-disant pare-feu. ils ont pu perturber certaines fonctionnalités. Un signal a été bloqué. Dysfonctionnement des médias WhatsApp. donc sur les données mobiles, nous ne pouvons pas transmettre les médias WhatsApp à moins qu'il y ait un VPN activé.

Alors, quelles capacités améliorées ont-ils pour pouvoir faire cela ? L'enregistrement et le blocage des VPN, d'autre part, se poursuivent, ainsi que la mise sur liste blanche des IPs, que les entreprises sont invitées à suivre et auxquelles elles se conforment car elles ont également rencontré des problèmes. Donc cela aussi est en cours en ce moment.

Et bien sûr, nous avons des réglementations. Donc, en termes de, même s'ils n'ont pas accès aux données de contenu, les métadonnées, comme mentionné, sont volontairement remises, et ensuite vous avez des systèmes centralisés où ils peuvent obtenir tout cela. Ils veulent donc savoir d'où proviennent les messages, qui communique avec qui, même si ce n'est pas les données.

Et d'autre part, en ce qui concerne l'accès aux données, nous avons eu des raids généralisés, des arrestations, des détentions illégales, des perquisitions et des saisies, malgré le fait que la loi exige un mandat, qui n'est pas demandé. Les gens sont ensuite forcés de fournir des mots de passe ou l'accès à leurs téléphones, et c'est ainsi que l'information et le contenu sont accessibles, donc les discussions, avec qui vous communiquez, établir ces liens, construire ces dossiers, parfois même les lois antiterroristes sont utilisées en combinaison avec les lois sur la cybercriminalité, et tout cela est ensuite admis comme preuve.

dans les procès, et généralement ces procès ne visent pas nécessairement toujours à obtenir une condamnation, mais comme je le répète, c'est le processus comme punition. Une fois que vous avez pu obtenir l'accès et contraindre et faire ce que vous devez, alors c'est, essentiellement l'objectif est atteint. Donc c'est essentiellement là où nous en sommes actuellement, où tout cela continue de se dérouler.

Et maintenant, nous avons l'impression que même les tribunaux, nous ne savons pas ce que cette nouvelle structure sous l'amendement, va nous réserver.

Karthika Rajmohan - Internet Freedom Foundation: Merci pour cela, Farieha, beaucoup de points très intéressants que j'aimerais approfondir. Enfin, si nous pouvions avoir Santosh Sigdel pour donner sa déclaration d'ouverture, s'il vous plaît.

Santosh Sigdel - Digital Rights Nepal: Merci, Karthika. Après avoir écouté Dr. Sanjana, Vrinda, Shahzab et Farieha, je peux conclure que nous avons une tendance similaire à travers l'Asie du Sud en ce qui concerne la régulation de l'espace numérique et les droits numériques, les tactiques du gouvernement sont également similaires.

Au Népal, il existe deux types de régulation. L'une se fait par des décrets et des actions exécutives, et l'autre par des lois et des politiques. Depuis quelques années, le gouvernement a commencé à proposer un certain nombre de politiques visant à réguler l'espace numérique. Et dans une perspective plus large, c'était aussi dû au fait que, lors des dernières élections, il y avait de nouveaux partis politiques et de jeunes candidats indépendants.

Ils ont pris le contrôle des anciens gardes et dans beaucoup d'endroits, y compris la capitale, une densité métropolitaine de la capitale. Il y avait un jeune homme qui a réussi à se faire élire maire. Il était rappeur. Donc, ces gens pensaient que c'était entièrement dû aux réseaux sociaux. Nous ne pouvons pas tenir le coup, nous ne pouvons pas être dans la course.

Nous, si nous ne pouvons pas contrôler les réseaux sociaux. Il y avait une sorte de, un sentiment parmi les anciens, partis, anciens gardes, et, au niveau exécutif, il y a eu plusieurs cas où le gouvernement essaie de.

Surveiller, la communication, tout en gardant un œil sur les gens. Ils ont proposé ce Service de Gestion des Dispositifs Médias, MDMS, via les codes de queue.

Et en même temps, il y a le mécanisme de surveillance du trafic des télécommunications et de contrôle de la fraude, TeraMox. Il y a également eu des accusations de corruption lors des processus d'approvisionnement et une requête a été déposée contre cette proposition devant le tribunal. Finalement, la question a été portée devant le comité parlementaire et le comité parlementaire a suspendu le processus pour l'instant, donc le TeraMox n'a pas été mis en œuvre.

Et l'année dernière, le gouvernement a adopté une Politique Nationale de Cybersécurité. Il y a un certain nombre de dispositions problématiques dans cette politique, y compris la provision d'une Passerelle Internet Nationale. Ils veulent établir une Passerelle Internet Nationale similaire à celle proposée au Cambodge, où tout le trafic entrant dans le pays doit passer par un point de contrôle dédié du gouvernement, un réseau dédié du gouvernement, et tout le trafic sortant du pays doit également passer par là, leur donnant ainsi accès.

Sur l'ensemble du trafic Internet.

qui est dans la politique. Nous ne savons pas comment ils vont la mettre en œuvre, mais, après la pression de la société civile et des médias, ils l'ont maintenant renommée

en une sorte de politique de gestion du haut débit. maintenant ils sont. Le dernier gouvernement, ils avaient une étude que nous avons déposée.

Digital Rights Nepal avait déposé une demande d'accès à l'information pour obtenir une copie de ce rapport, mais celui-ci n'a pas été publié. Ils ont donc lancé une étude sur cette politique de gestion du haut débit où ils ne veulent plus en parler comme d'une initiative nationale, mais préfèrent la déguiser sous un autre nom technique.

comme vous le savez peut-être, ils veulent, que le même argument que Brinda et d'autres ont fourni, à savoir que les entreprises de médias sociaux ne sont pas enregistrées au Népal, donc l'année dernière, ils ont adopté une directive sur les médias sociaux, qui exigeait qu'une entreprise de médias sociaux s'enregistre au Népal dans un délai de trois mois, et immédiatement après une semaine, TikTok a été interdit en novembre dernier, et plus d'une douzaine de requêtes ont été déposées à la Cour suprême.

Et finalement, TikTok s'est également rapproché du gouvernement. Et la tendance est similaire. Comme je l'ai dit plus tôt, TikTok faisait de la diplomatie, cette négociation en coulisses plutôt que de contester la décision. Et ce sont les organisations de la société civile et d'autres qui contestaient la décision.

Contester cette décision et finalement ils ont accepté, ils ont négocié. Et, les organisations de la société civile sont toujours, parce que les détails de la négociation entre TikTok et le gouvernement ne sont pas très clairs. Donc, TikTok avait dit plus tôt qu'ils fourniraient un système pour signaler le contenu que le gouvernement juge inapproprié et qu'ils examineraient ces contenus.

Donc, maintenant nous ne savons pas quoi. La société civile est-elle méfiante d'autres négociations possibles avec TikTok, mais cela a repris en août 2024. Et, maintenant TikTok a commencé le processus d'enregistrement au Népal. C'est caractéristique. Et après cela, après l'avoir bloqué pendant un an, ils sont de retour dans le pays et ont commencé ce processus d'enregistrement.

Le gouvernement a également proposé deux nouveaux projets de loi qui comportent des dispositions très problématiques. L'un est un projet de loi sur l'utilisation et la régulation des médias sociaux, que nous, Digital Rights Nepal, avons analysé et l'année dernière, nous avons fourni des commentaires au gouvernement, au ministre. Et il est maintenant dans le comité législatif du cabinet, et il sera présenté au parlement lors de la prochaine session.

Et il y a seulement la cybersécurité, ce projet de loi sur la technologie de l'information et la cybersécurité. Et nous croyons que de nombreuses dispositions de la politique nationale de cybersécurité seront intégrées à ce projet de loi. Ce projet de loi sur la cybersécurité comporte de nombreuses dispositions problématiques concernant la

suppression de contenu et donne à de nombreuses institutions le pouvoir d'ordonner aux entreprises de médias sociaux de retirer le contenu.

le pouvoir a été donné à au moins cinq agences, donc si l'une de ces agences trouve un contenu problématique, elle peut émettre un ordre et si le contenu n'est pas retiré dans les 24 heures, elles seront sanctionnées d'une amende de 10 000. Jusqu'à 10 lakhs de roupies, ce qui équivaut à environ 70 000, je crois. Donc, il y a beaucoup d'autres dispositions problématiques.

Une disposition majeure est la responsabilité des intermédiaires. Nous avons donc également analysé cela. Nous coordonnons avec d'autres organisations pour proposer des amendements à ce projet de loi, et nous travaillons également avec un membre du parlement. En parlant des tribunaux, comme l'ont partagé Sajab ou d'autres, les tribunaux ont un rôle minimal, cependant, il y a eu quelques cas où ils ont joué un rôle très important.

Il y a quelques années, un juge en exercice de la Cour suprême a été impliqué dans une affaire sordide, et à ce moment-là, les agences d'enquête avaient collecté plus d'un demi-million de dossiers de la cour et des milliers de contenus de réseaux sociaux, de textes, de SMS. À ce moment-là, nous avons saisi la cour pour contester la décision des agences d'enquête, et la Cour suprême a alors émis des directives pour légiférer sur ce processus, tout en exigeant une sanction judiciaire.

l'approbation du tribunal de district pour collecter tout détail d'appel auprès des opérateurs télécoms. C'est ainsi que le tribunal a pu mettre en œuvre le droit à la vie privée, un droit à la vie privée inscrit dans la constitution. Et il y a, un certain nombre d'autres affaires également qui sont actuellement en instance devant la Cour suprême.

Ce qui peut, par exemple, il y a eu un cas concernant ce Teramox, son implication sur le droit à la vie privée. Nous attendons avec impatience le résultat de cette affaire en cours pour voir comment la cour va défendre le droit à la vie privée. Voici quelques scénarios généraux, le dernier point à conclure est que le gouvernement essaie également de, car maintenant, en comparaison avec les médias traditionnels, les médias en ligne sont très robustes et critiques, donc ils ont proposé ces directives pour les médias en ligne.

Et maintenant, le gouvernement a proposé un projet de loi sur le conseil des médias, qui régulera également les médias en ligne. Beaucoup des questions que nous avons discutées seront également impactées, car les plateformes de médias sociaux, les médias traditionnels ou les médias en ligne seront également soumis à ce projet de loi sur les médias sociaux et à la loi sur les technologies de l'information.

Et l'impact se fera également sentir sur la liberté de la presse dans les jours à venir. D'accord, c'est tout pour l'instant, en guise de contexte général.

Karthika Rajmohan - Internet Freedom Foundation: Merci beaucoup. Nous avons reçu de nombreux points très perspicaces de la part de tous nos intervenants. Pour résumer, je pense qu'un fil conducteur commun que nous avons remarqué chez tous les intervenants est qu'il y a une liste de raisons que les gouvernements semblent utiliser pour justifier les répressions sur le chiffrement de bout en bout.

Tout d'abord, la sécurité nationale. Ensuite, le maintien de l'ordre public, la régulation des discours de haine et des fausses nouvelles. Et enfin, faciliter les enquêtes criminelles et lutter contre les abus sexuels sur les enfants.

Tout d'abord, j'aimerais poser une question à Mme Vrinda et à Dr. Sanjana, pour qu'elles nous expliquent ce que font les tribunaux dans votre pays pour équilibrer le besoin d'assurer un espace sûr pour les femmes et les enfants avec le droit à la vie privée et la liberté d'expression.

Quels sont les types d'arguments que les tribunaux ont pris en compte, quels sont les types d'équilibres que les débats ont entourés ? Si vous voulez commencer, madame Vrinda.

Vrinda Bhandari - Internet Freedom Foundation: Oui. Mes excuses, Dr. Sanjana. J'ai dû partir plus tôt, c'est pourquoi j'ai demandé à parler en premier. Donc, en fait, c'est intéressant que dans de nombreux cas, ce qui se passe, c'est que lorsque le tribunal est concerné, et je pense que cette expérience sera peut-être partagée, j'aimerais savoir cela. Par exemple, quand nous parlons des droits des enfants, ce qui se passe souvent, c'est que cela ne surgit pas dans un cas spécifique, mais cela est déposé comme ce que nous appelons en Inde un litige d'intérêt public.

Donc, cela sera déposé par, disons, une organisation de défense des droits de l'enfant disant, regardez, c'est un problème sérieux, nous devons faire quelque chose. Et ce qui se passe, c'est que comme cela est déposé en tant que PIL, beaucoup d'intermédiaires ne sont pas impliqués, n'est-ce pas ? Donc, c'est la cour et le pétitionnaire du PIL. Et donc, la cour ne comprend pas vraiment quels sont les aspects techniques, ce que cela signifie quand vous dites, oh, vous devez tous donner vos données au gouvernement à tout moment. Donc, bien qu'ils soient bien intentionnés, je pense que ce que nous voyons souvent, et cela s'est même produit récemment, avec la Cour suprême et un autre jugement, c'est qu'ils émettent des directives à divers intermédiaires.

Ce qui devient alors difficile à respecter opérationnellement, n'est-ce pas ? Mais comme ils n'ont jamais entendu ces préoccupations, c'est un problème. J'ai également envoyé un lien vers un article que j'ai eu le privilège d'écrire avec Anya Kovacs, et nous avons en fait examiné comment les tribunaux en Inde abordent les questions de genre et de sexualité.

A-t-il élargi les droits numériques ou les a-t-il en fait restreints ? Donc, j'ai partagé cela dans le chat et je pense que vous pouvez le partager avec le panel plus large ainsi

qu'avec le public plus large, mais ce que nous avons trouvé, c'est que souvent, bien que bien intentionnés, pour protéger les femmes ou pour protéger la moralité des femmes, surtout lorsqu'il s'agit de quelque chose d'obscène, les tribunaux finissent par restreindre les droits numériques.

Et nous considérons les droits numériques de manière très large en termes de liberté d'expression, de vie privée, toutes ces choses. Donc, c'est une chose. En ce qui concerne la sécurité nationale, malheureusement, dans la plupart des cas, le gouvernement, la cour adopte une approche non interventionniste. Ils peuvent, sur des faits spécifiques, c'est très difficile, donc il y avait un cas de blocage qui est apparu à la Haute Cour de Delhi, où il y avait un logiciel, qu'ils avaient contesté, et il avait été temporairement bloqué au Jammu-et-Cachemire.

Et la cour a dit, oh, regardez, c'est un blocage très temporaire, c'est pour des raisons de sécurité nationale, c'est au Cachemire. Et puis c'est presque intouchable, non? aucune cour ne va aller de l'avant et contester cela. Nous avons vu cela avec les coupures d'Internet également, quand cela s'est produit au Cachemire et nous avons contesté cela en justice et bien que nous ayons obtenu un jugement, il n'y avait en fait aucune mise en œuvre spécifique, comme il n'y avait pas de jugement sur les ordonnances en tant que telles, comme sur les faits réels de l'affaire, c'était plus un jugement sur la manière dont les coupures d'Internet devraient être traitées, donc ce que nous constatons souvent malheureusement, c'est que lorsqu'il s'agit spécifiquement de sécurité nationale, cela devient très difficile. Pour les tribunaux, d'exercer réellement leurs pouvoirs de révision judiciaire. Ils ont tendance à adopter une approche plus détachée. Et ce que nous avons toujours essayé de faire valoir, c'est que dire simplement qu'il s'agit d'une question de sécurité nationale ne devrait pas suffire.

Il doit y avoir une base, car sinon il est impossible pour vous, en tant que pétitionnaire, de montrer un soutien, ou de réfuter cette présomption ou de dire pourquoi c'est disproportionné. Donc, il y a eu, c'est là que je pense que nous faisons face à un défi. Cela dit, je voudrais recommander à tout le monde de lire la récente décision de la Haute Cour de Bombay, sur un autre aspect de ces règles informatiques, et peut-être que Karthika, tu pourrais partager le lien vers le jugement, mais où la cour a annulé par deux voix contre une.

Il y a eu un premier verdict partagé, qui a été soumis à un troisième juge et il a statué en faveur des pétitionnaires. L'IFF avait également aidé dans ce cas. Et ils ont annulé la création d'une unité de vérification des faits, qui aurait examiné les informations fausses, trompeuses ou diffamatoires concernant le gouvernement.

Et donc, c'était une unité de vérification des faits notifiée par le gouvernement et la cour l'a annulée. C'était un développement vraiment positif, mais je pense que dans l'ensemble, c'est ainsi que nous avons géré la situation. Je suis vraiment désolé, je dois partir. Je vais juste laisser mes coordonnées au cas où quelqu'un voudrait me contacter.

J'adorerais faire cela.

Karthika Rajmohan - Internet Freedom Foundation: Merci beaucoup. Un plaisir de vous avoir ici. Dr. Sanjana, si vous souhaitez ajouter quelque chose.

Sanjana Hattotuwa - ICT4Peace Foundation: Oui, donc la seule chose que je peux ajouter à cela, c'est que nous ne sommes pas, en tant que pays, aussi développés dans notre PIL et que nos tribunaux ont été sous la botte de l'exécutif, de la même manière que, constitutionnellement, le bureau du président exécutif est construit depuis 1977, date à laquelle la constitution actuelle est née.

Le président exécutif est intouchable. Et quiconque a occupé ce poste a continué à empiéter sur les droits de toutes les manières possibles. Et les tribunaux ont été soumis à cette autorité. C'est presque divin. Quand nous parlons du discours sud-asiatique aujourd'hui, et que nous parlons, par exemple, du décret de Modi.

Nous avons eu des présidents exécutifs comme Raj Paksa depuis 2005 qui ont complètement piétiné les droits. Donc, le PIL a été assez efficace, mais cela a eu un coût significatif. Des militants ont été arrêtés, blessés, torturés, assassinés et tués de manière extrajudiciaire. Ainsi, même s'engager dans le PIL, en particulier sur les questions de sécurité nationale, représente un énorme obstacle.

Donc ce n'est pas facile. Et nous avons ce genre de scénario kafkaïen, qui fait allusion à ce que l'orateur précédent a dit, où pour découvrir quel est le problème de sécurité nationale, ils ne révèlent pas quel est le problème de sécurité nationale. Cela devient donc un peu absurde, car vous ne savez pas contre quoi vous êtes censé vous battre, mais on vous dit d'accepter sur parole que c'est un problème de sécurité nationale.

L'autre point que je voulais souligner, et encore une fois, quand j'entends les exemples de l'Inde, je me sens assez triste. L'un des aspects sur lesquels le département du procureur général et la Cour suprême se sont prononcés concernant la loi sur la sécurité en ligne, qui a été adoptée au Parlement de manière très inconstitutionnelle, est également contesté.

Mais le jugement lui-même était extraordinairement mauvais. Et l'un des, pour le dire simplement, je pense qu'il est très clair quand on lit le jugement que le banc ne sait pas, n'est pas au courant, et n'a pas été informé de ce que constituent les préjudices en ligne. Ils s'appuient donc sur une compréhension et une notion de la régulation, des préjudices, des médias et du paysage de l'information très datées, dépassées et obsolètes.

Et il ne semble pas y avoir de problème à la Cour suprême, ni dans la communauté juridique en général concernant certains des sujets dont nous parlons lors de cet appel, ce qui est un nœud gordien. Ils n'ont pas de jurisprudence particulièrement claire, mais

même sur ce point, la magistrature et la communauté juridique du Sri Lanka ne sont pas liées.

À jour. Et c'est très clair dans le jugement. Nous avons donc beaucoup de retard à rattraper à cet égard, ce qui engendre une peur autocratique. Le résultat net est que notre gouvernement et nos présidents exécutifs ont une propension et une culture d'impunité, étant donné que même le recours en justice est si faible qu'ils peuvent agir à leur guise, comme d'autres l'ont mentionné dans d'autres pays, avec des réglementations arbitraires, des lois arbitraires, des ordres extra-constitutionnels ou contra-constitutionnels donnés aux opérateurs de télécommunications, des métadonnées à grande échelle. Et je terminerai en disant que l'un des enjeux de pointe que nous considérons est l'avènement de l'IA générative. Et ce que cela signifiera pour les autorités étatiques dans la collecte à grande échelle de ce qu'elles font et ensuite le ciblage subséquent de manière individuelle, institutionnelle ou spécifique à une question.

de manière qu'il n'y a actuellement aucune jurisprudence légale ou cadre réglementaire envisagé dans le pays. Donc ce n'est pas seulement une question de frontière, c'est en fait une question fondamentale. Je pense que c'est une question de première importance, étant donné ce que nous avons vu dans le pays, mais c'est peut-être une discussion différente. Mais de la manière la plus simple que je puisse dire, c'est qu'en ce qui concerne la réponse donnée par l'Inde, nous en sommes à un stade beaucoup plus embryonnaire, et je dirais qu'en conséquence, nous sommes plus fragiles et ouverts à la peur et à l'abus autocratiques, en raison de la fragilité et de la nature limitée de nos tribunaux.

Karthika Rajmohan - Internet Freedom Foundation: Merci beaucoup pour cela, Dr. Sanjana. Je sais que nous manquons de temps, mais j'aimerais rapidement avoir l'avis de Fareeha à ce sujet également. Surtout parce que nous avons parlé de la sécurité nationale, qui est une justification pour l'érosion du chiffrement de bout en bout. Brinda a également mentionné qu'il est difficile pour les tribunaux de trouver un équilibre entre ces intérêts.

Dr. Sanjana a également mentionné que, surtout en période de fragilité, ces questions deviennent encore plus exacerbées. Et étant donné que vous avez mentionné que le Pakistan, en cette année électorale, procède à des nominations judiciaires en cours de route. Comment le Pakistan gère-t-il ce débat entre la sécurité nationale et d'autres défis possibles concernant la vie privée, la liberté d'expression et de parole ?

Farieha Aziz - Bolo Bhi: Le problème, comme l'a souligné Dr. Farieha, ce sont les affirmations non qualifiées de sécurité nationale. Et nous nous attendons à ce que les tribunaux s'affirment un peu plus et demandent à l'exécutif de préciser ce qui menace exactement la sécurité nationale dans le contexte de l'interdiction de X. et ils l'ont bloqué. Les ministres utilisent X via des VPN, qu'ils bloquent et enregistrent également.

Voyez simplement l'hypocrisie de tout cela. Et au moins, posez-vous la question de pourquoi et dans quel but, et à quoi cela sert-il ? Il y a donc cet aspect. Et encore une fois, en termes d'autorisation d'une agence de renseignement a posteriori pour ensuite mener une surveillance de masse, quelle est également la nécessité ? Et d'un autre côté, parce que beaucoup de pétitions d'habeas corpus pour des enlèvements de citoyens sont déposées devant les hautes cours.

Dans ces cas-là, les CDR ne sont jamais fournis. D'une manière ou d'une autre, les caméras de la ville sécurisée ne fonctionnent jamais. Ils ne peuvent jamais retrouver les personnes qui ont réellement enlevé. Aucun des systèmes existants n'est jamais utilisé pour retrouver les coupables. Mais d'un autre côté, et en plus de ce qui se passe, nous avons aussi des tribunaux qui ont une vision antagoniste des réseaux sociaux.

Et donc, nous avons eu l'actuel président de la Cour suprême, disant que tous ces vloggers qui gagnent des dollars et sont sur des listes de paie, etc. Et parce qu'il y a eu des critiques, évidemment, de la Cour suprême et des juges et d'autres aussi. Et d'autre part, nous avons traversé cette crise judiciaire où des juges de la Haute Cour ont en fait écrit une lettre et ont déclaré que l'établissement contrôle, des caméras ont été trouvées dans les chambres des juges.

il s'est passé beaucoup de choses, et la Cour suprême et le juge en chef ont essentiellement détourné le regard. Et donc, au sein des tribunaux, certains penchent dans une direction et d'autres dans l'autre. Mais les procédures pour outrage, parce que vous avez alors ces guerres par procuration où ces juges ont été calomniés.

parce qu'ils s'attaquaient à l'institution, mais ensuite ils ont aussi pris la voie du mépris en disant oh maintenant il doit y avoir du scraping de données et qui fait tendance avec ces hashtags et où ces données personnelles des juges sont divulguées et des campagnes sont menées contre eux, y compris dans les médias traditionnels, donc il y a beaucoup de friction au sein de la magistrature également et maintenant avec le Dr.

Farieha a mentionné les bottes militaires et c'est tout. Nous avons eu une histoire judiciaire mouvementée, mais en même temps, ici à l'Exécutif, il y a plus d'enracinement en termes de, vous, vous voulez une justice indépendante qui défie l'Exécutif lorsque les citoyens vont en justice contre l'Exécutif.

Vous voulez que les tribunaux puissent rendre des décisions. Cependant, lorsque cela se produit, les juges sont mis à l'écart ou, par exemple, l'ordonnance de la Haute Cour d'Islamabad, qui a ensuite été suspendue par la Cour suprême, et maintenant ils veulent simplement réorganiser les juges et aussi l'ensemble de la magistrature. Donc, pour le moment, nous ne savons pas.

De plus, toute la pratique des appareils simplement confisqués. Les gens sont enlevés, arrêtés, leurs appareils sont pris. Il n'y a donc aucune protection. Même un projet de loi sur la protection des données, en cours d'élaboration, offre plus d'accès au

gouvernement, facilite davantage l'accès du gouvernement aux données plutôt que de les protéger.

Et donc pour moi, l'intention est toujours en question. Les récits sont les mêmes. Nous devons protéger les citoyens et protéger également les femmes et les enfants. Ces récits protectionnistes et paternalistes, mais rien de tout cela ne se réalise réellement. Et sous le couvert de tout cela et de la sécurité nationale, l'empiètement de l'État est enraciné.

Et c'est essentiellement ce que nous avons observé à travers la loi, la création de règles au sein de la magistrature, les problèmes d'attitude. Et à ce stade, honnêtement, même les gains que nous avons quelque peu réalisés, je, ils peuvent être annulés, étant donné comment les tribunaux vont être restructurés, si la jurisprudence s'appliquera toujours, allons-nous repartir de zéro, et puis qui va diriger ces bancs constitutionnels.

ce qui, évidemment, nous semble être des nominations triées sur le volet qui bloqueront toute forme de défense des droits et de litiges. Et il y a divers cas en attente, mais ils n'avancent pas. Oui.

Karthika Rajmohan - Internet Freedom Foundation: Merveilleux. C'était vraiment intéressant. J'aurais aimé que nous puissions continuer plus longtemps, mais si nous pouvions maintenant passer aux questions-réponses. D'accord, je crois que nous avons dépassé le temps. Nous allons devoir clore le panel ici. Je suis vraiment désolé, Santosh et Shazeb. Je voulais spécifiquement vous poser quelques questions que j'avais notées, mais nous manquons de temps. Donc, je pense que nous allons devoir clore la session ici. Je tiens à saisir cette occasion pour remercier tous nos merveilleux panélistes.

C'était une discussion formidable, très enrichissante et perspicace que nous avons eue, et ce fut un plaisir de participer à cette discussion avec vous tous. Merci beaucoup.