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

À quoi ressemblera une régulation des plateformes favorable au chiffrement ? Perspectives transrégionales sur la régulation des plateformes en ligne et le chiffrement'

Maria Paz Canales - Global Partners Digital: Bonjour, je suis Maria Paz Canales. Je suis la responsable des politiques juridiques et de la recherche chez Global Partner Digital. J'ai le plaisir, en tant que membre de la Global Encryption Coalition, d'être votre modératrice aujourd'hui pour cette conversation très pertinente. Intitulée 'À quoi ressemblera une régulation des plateformes favorable au chiffrement ? Perspectives transrégionales sur la régulation des plateformes en ligne et le chiffrement'.

Pour planter un peu le décor de cette conversation que j'ai introduite avec le titre de la session, et qui sera substantiellement partagée par notre merveilleux intervenant, je voudrais dire quelques mots à ce sujet. Nous vivons à une époque où beaucoup plus de personnes ont accès au chiffrement qu'auparavant.

Pourtant, nous voyons également un nombre considérable de nouvelles propositions qui vont l'affaiblir, menaçant ainsi la confidentialité et la sécurité des communications

numériques, mettant en danger les droits et le bien-être de certains individus et groupes. En même temps, il est largement reconnu qu'il faut mieux protéger les enfants contre les dangers et garantir la responsabilité des entreprises en cas d'abus.

Cependant, dans ce contexte complexe, une réponse réglementaire Nos réponses à ces questions doivent être nuancées et consultatives, respectant et se conformant aux principes de légalité, de nécessité, de proportionnalité, de légitimité et de non-discrimination dans notre perspective en tant que défenseurs de la protection du chiffrement. Cette table ronde a pour but de réunir ces merveilleux défenseurs que je vais présenter dans quelques minutes, venant du Royaume-Uni, du Nigeria et du Brésil, qui travaillent à l'intersection des droits de l'homme et de la technologie pour partager leur expérience et leur expertise dans cette discussion sur la régulation des plateformes nationales.

À travers cette discussion, nous espérons changer les tactiques et stratégies pour participer à ce débat. Et quatre réponses réglementaires qui sont proportionnées et protectrices du chiffrement. Notre objectif avec cette session est de produire des enseignements et des points à retenir qui peuvent être utiles à la communauté dans son ensemble pour ce qu'elle doit défendre à différents moments, dans différentes régions, dans différentes juridictions.

Je vais maintenant présenter mon éminent intervenant. Nous avons aujourd'hui avec nous Adeboye Adegoke, qui est Senior Manager pour Paradigm Initiative du Nigeria. Nous avons également avec nous Heloisa Massaro, qui est Directrice de l'Internet Lab au Brésil. Et enfin, mais non des moindres, nous avons Mark Johnson, qui est Advocacy Manager chez Big Brother Watch du Royaume-Uni.

Et nous allons commencer la première partie de cette discussion en plongeant particulièrement dans le plaidoyer pour le processus de régulation des plateformes en ligne au niveau national. Chacun de ces éminents intervenants aura environ quatre minutes. Nous avons quatre minutes pour partager un peu de leur introduction. Et sans plus tarder, je vais commencer avec vous, Mark, en vous demandant de partager un peu de votre expérience étant donné que le Royaume-Uni a été l'un des premiers pays à développer un système de sécurité en ligne dédié, contrairement à l'utilisation des lois existantes pour aborder certaines des préoccupations de régulation des plateformes. Pouvez-vous nous parler de votre engagement dans le processus d'élaboration de l'Online Safety Act, auquel nous faisons référence, et de la lutte pour défendre la forte protection du chiffrement, comment la discussion a-t-elle été cadrée et comment Big Brother Watch et d'autres groupes de la société civile qui se sont coordonnés pour confronter cette proposition ont-ils répondu à cette critique, en particulier sur le rôle du chiffrement ?

Merci beaucoup d'être ici, Mark. La parole est à vous.

Mark Johnson - Big Brother Watch: Merci beaucoup, Maria, et bon après-midi si c'est l'après-midi là où vous êtes.

Oui, si vous ne connaissez pas Big Brother Watch, nous sommes une organisation de défense des libertés civiles basée au Royaume-Uni. Nous nous intéressons particulièrement à l'intersection entre les droits de l'homme et la technologie, et le titre, évidemment, de la discussion est à quoi ressemblerait une réglementation des plateformes favorable au chiffrement.

Je ne veux pas être négatif dans ma perspective, mais malheureusement, d'après mon expérience, j'ai un bon exemple de ce à quoi pourrait ressembler une mauvaise régulation de plateforme non favorable au chiffrement avec la loi britannique sur la sécurité en ligne. Pour ceux qui ne connaissent pas cette loi, c'est une législation adoptée par notre Parlement l'année dernière, et qui a mis plusieurs années à se concrétiser.

L'idée d'une loi britannique sur la sécurité en ligne a été évoquée pour la première fois au début des années 2010, mais en gros, la façon dont ce type de réglementation fonctionne est qu'elle crée ou nomme un régulateur indépendant pour établir des codes de conduite principalement pour les grands sites de médias sociaux ouverts. Et ces codes de conduite dictent des règles sur la manière dont ils doivent modérer le contenu sur leurs sites.

Les premières versions du projet de loi ne mentionnaient pas les services de messagerie privée. En grande partie, les services de messagerie privée étaient exemptés, et l'idée de cette réglementation était de créer un moyen de réguler le contenu sur les grandes plateformes comme Meta, X, et ainsi de suite.

Bien sûr, il y avait un certain nombre de considérations sur la liberté d'expression, et nous avons travaillé sur le projet de loi principalement au début sous l'angle de la liberté d'expression, en réfléchissant à la manière dont la modération du contenu et les règles à ce sujet pourraient affecter le droit des utilisateurs à la liberté d'expression en ligne. Mais pendant que le projet de loi était en cours d'élaboration, il y avait une pression simultanée de notre ministère de l'Intérieur ici au Royaume-Uni pour insérer des dispositions dans la législation concernant les services de messagerie privée et, en particulier, les services de messagerie chiffrée.

Et finalement, la version finale du projet de loi incluait des dispositions qui sont devenues communément connues sous le nom de "notices technologiques". En essence, ces notices technologiques étaient une manière très subtile, très peu examinée et discrète d'imposer aux plateformes l'utilisation de technologies comme le balayage côté client pour lutter contre le matériel d'abus d'enfants sur leurs sites.

C'était malgré le fait qu'au Royaume-Uni, les forces de l'ordre et d'autres agences disposent déjà d'une série de pouvoirs pour s'attaquer à ce problème, qui est bien sûr

une question de droits et doit être pris extrêmement au sérieux, mais il existait déjà une gamme de pouvoirs disponibles pour de nombreuses forces de l'ordre et agences pour y faire face.

Et ces pouvoirs ont été insérés malgré les préoccupations concernant la vie privée, l'exactitude et même la compatibilité des technologies en question ou le manque de compatibilité avec les appareils des utilisateurs. Ainsi, ces dispositions ont été ajoutées à la législation sans un examen approfondi du point de vue de la société civile. Nous avons participé au processus, mais bien sûr, il s'agissait d'un projet de loi vaste qui traitait de la régulation de différentes parties d'Internet, principalement des plateformes de médias sociaux ouvertes. Il prenait également en compte non seulement la modération de contenu, mais aussi la vérification de l'âge et d'autres dispositions diverses, y compris de nouvelles infractions pénales.

D'un point de vue de la société civile, nous étions extrêmement sollicités, étant donné que nous nous concentrions déjà sur les considérations relatives à la liberté d'expression et d'autres questions concernant la législation. Nous avons engagé un dialogue avec le gouvernement à l'époque, mais malheureusement, le gouvernement n'était pas particulièrement disposé à nous écouter, et nous avons avancé les arguments, y compris les arguments relatifs aux droits.

les problèmes de précision en ce qui concerne les technologies comme le balayage côté client et aussi les questions fondamentales sur le fonctionnement des processus. Malheureusement, malgré nos meilleurs efforts en collaboration avec les parlementaires de l'opposition, nous n'avons finalement pas pu retirer ces pouvoirs du projet de loi, donc ils sont entrés en vigueur l'année dernière.

La bonne nouvelle de notre côté, je pense, est que jusqu'à présent, le régulateur que le gouvernement a nommé, Ofcom, a adopté une approche assez prudente, donc les pouvoirs n'ont pas encore été utilisés. Et je pense que nous, c'est bienvenu qu'Ofcom ait été très prudent. Ils sont très conscients des considérations relatives aux droits, de l'impact sur la vie privée et de nombreux autres enjeux.

La difficulté réside dans le fait que nous sommes très dépendants d'Ofcom pour adopter cette approche. Ils peuvent changer d'approche à tout moment. Ils pourraient devenir beaucoup plus interventionnistes. Et le cadre réglementaire de l'Online Safety Act du Royaume-Uni est un cadre qui est ouvert à l'influence politique par la manière dont il est rédigé.

Il y a donc une chance que le gouvernement puisse faire pression sur Ofcom pour utiliser ces pouvoirs afin d'obliger une plateforme de messagerie chiffrée comme WhatsApp ou Signal à scanner tous les messages de tous les utilisateurs du site. Et il y a très peu de moyens pour empêcher cela. Bien sûr, il y a toujours la possibilité, et en fait, je pense qu'il est assez probable que ces pouvoirs puissent être contestés devant un tribunal au Royaume-Uni, et l'organisation des droits de l'homme, l'organisation pour la

liberté d'expression, Index on Censorship, a commandé un avis juridique indiquant qu'il était probable que ces pouvoirs soient illégaux.

En fait, l'avis a été rédigé par Matthew Ryder, qui a effectivement déclaré qu'Ofcom dispose désormais de pouvoirs plus étendus que le GCHQ, notre agence de surveillance numérique ici au Royaume-Uni, en raison de cette loi. Il est rassurant pour le moment qu'Ofcom soit prudent et que les pouvoirs n'aient pas été mis en œuvre. Mais il y a une chance qu'il y ait une contestation juridique s'ils sont jamais utilisés à l'avenir.

De notre côté, c'est une situation difficile car c'est un mauvais précédent que nous avons établi. Cela aura un impact sur les utilisateurs du monde entier car si ces pouvoirs sont utilisés, et si WhatsApp ou Signal étaient contraints de compromettre la sécurité de leurs utilisateurs en affaiblissant le chiffrement de bout en bout, cela aurait également des répercussions sur les gens du monde entier.

Il y a donc un impact sur les droits dans d'autres parties du monde, pas seulement au Royaume-Uni. Et c'est malheureusement un mauvais exemple de réglementation. Mais il y a encore des opportunités pour nous de lutter contre cela. Nous l'examinons aussi attentivement que possible. Et si le gouvernement pense un jour à faire pression sur Ofcom, ou si Ofcom envisage d'utiliser ces pouvoirs, nous serons les premiers à réagir et à essayer de les empêcher d'être utilisés.

Maria Paz Canales - Global Partners Digital: Merci beaucoup, Mark, pour ces perspectives, bien qu'elles soient moins positives que ce que nous aurions souhaité pour cette conversation. Cependant, je pense qu'il y a des enseignements pertinents qui semblent positifs en termes de stratégie et d'opportunité de collaboration avec des organisations travaillant dans d'autres juridictions pour montrer quelles pourraient être les conséquences plus larges de ce type d'approche législative dans d'autres parties du monde. En passant à cette conversation, j'aimerais demander à Boye de nous donner son point de vue sur son expérience et celle de Paradigm Initiative dans le processus de rédaction du projet de loi sur la protection de la santé en ligne au Nigeria, comment vous avez participé à la phase consultative de ce projet de loi pour façonner ce développement, et merci beaucoup de nous avoir rejoints aujourd'hui. Nous espérons que ce sujet du chiffrement a été abordé et que vous pourriez peut-être établir un lien avec certaines des expériences partagées par Mark, et voir comment celles-ci pourraient être utiles ou non dans le déroulement de la discussion au Nigeria.

À vous la parole.

Adeboye Adegoke - Paradigm Initiative: D'accord. Merci, Maria. Je pense que beaucoup de ce que Mark a dit m'a également touché. Mais je pense que la principale différence est qu'en ligne, le projet de loi sur la sécurité en ligne au Royaume-Uni et le projet de loi sur les préjudices en ligne au Nigeria, le projet de loi sur les préjudices en ligne au Nigeria est encore en cours.

Nous n'avons pas encore de loi. En fait, nous n'avons même pas encore de projet de loi. Tout ce que nous avons, c'est un livre blanc qui définit en quelque sorte la direction à suivre. Maintenant, en termes de notre expérience dans ce domaine, je pense que cela s'appuie sur nos années de travail à défendre la protection des droits numériques au Nigeria. Donc, lorsque le gouvernement nigérian a parlé de la création d'un comité pour le conseiller sur ce à quoi devrait ressembler la protection contre les préjudices en ligne au Nigeria.

Ils ont décidé de nous inviter dans la salle, mais ils ne nous ont pas seulement invités. C'était aussi parce que nous essayons de créer un équilibre dans l'engagement en nous disant que vous avez plaidé pour la protection des droits numériques. Vous avez également proposé une loi sur les droits numériques et la liberté au Nigeria.

Donc, ce qu'ils avaient proposé au début, c'était d'avoir une législation qui traite des droits numériques et de la santé en ligne. La proposition à ce moment-là était d'avoir une législation sur la protection des droits numériques et de la santé en ligne. Mais nous avons trouvé cela délicat pour nous, étant donné que nous savons comment ce processus s'est déroulé.

Nous ne voulions pas que les deux questions soient confondues. Nous voulons que le Nigeria ait une législation qui traite des droits et libertés numériques, tout en pouvant également aborder la question des préjudices en ligne dans une législation distincte. Donc, nous avons annulé cela. C'est d'accord. Nous sommes dans ce comité pour garantir qu'il y ait une protection numérique dans vos efforts pour réguler les préjudices en ligne, mais ne lui donnez pas ce nom, car une fois qu'ils lui donnent ce nom, cela deviendra difficile pour nous.

Donc, en ce qui concerne la réglementation, par exemple, lorsque Mark parlait de l'expérience du Royaume-Uni, il a mentionné que dans le produit final, ils ne pouvaient pas changer certaines choses qu'ils auraient aimé changer. Nous savons donc aussi que notre pouvoir était limité en ce qui concerne la capacité de déterminer à quoi ressemblera le document final.

Nous voulons donc mettre fin à notre plaidoyer pour une législation sur les droits numériques au Nigeria en modélisant un sujet qui cherche à protéger les utilisateurs en ligne, étant donné que nous connaissons déjà certains défis qui pourraient survenir dans ce contexte. Nous avons donc commencé à travailler en tant que membre du comité de pilotage de l'initiative aux côtés de nombreuses autres organisations qui font partie de ce comité.

Beaucoup d'entre eux sont des groupes de réflexion, beaucoup d'entre eux travaillent également dans les domaines de la technologie et des politiques. Bien sûr, les enjeux étaient clairs en termes de ce qui est de la plus haute importance pour chacun des parties prenantes. Pour nous, ce qui nous tenait à cœur, c'était de veiller à ce que cela ne devienne pas une autre excuse pour violer les droits.

Comme nous l'avons vu de nombreuses fois dans cette partie du monde, où les lois sur la cybercriminalité sont devenues des outils d'oppression, des outils de suppression de l'espace civique ou de ciblage des défenseurs des droits de l'homme. Cela a donc toujours été une priorité. Ce processus a conduit à la publication d'un livre blanc sur la protection en ligne au Nigeria.

Et si vous regardez ce livre blanc aujourd'hui, il ne semble pas vraiment mauvais en ce qui concerne la question du chiffrement spécifiquement. Mais c'est parce que nous avons commencé la conversation par la protection des droits numériques. Mais comme je l'ai dit, il est encore trop tôt pour célébrer parce que ce que nous avons est un livre blanc, et à partir de ce livre blanc, nous allons avoir un projet de loi, et ce projet de loi passera par de nombreux processus, les politiciens y jetteront un œil, les différentes agences gouvernementales donneront leur avis, et beaucoup de choses peuvent encore se produire.

Mais une chose que nous avons toujours faite de manière très cohérente est de surveiller le processus. Non seulement parce que nous sommes membres du comité de pilotage, mais aussi parce que nous avons toujours surveillé le paysage des droits numériques au Nigeria en général, et nous serons les premiers à tirer la sonnette d'alarme lorsque quelque chose ne va pas.

Donc, l'une des choses que nous avons également faites est d'organiser ce que nous aimons appeler la Série d'Engagement sur la Politique Numérique avec le Groupe de la Société de Radiodiffusion pour les informer de ce qui se passe avec ce processus, car ce n'est pas encore public. Peu de gens savent que ce processus est en cours.

Je suis sûr que les personnes présentes à cet appel se demanderont ce qui se passe au Nigeria. Bien sûr, ce n'était pas public. Mais ce que nous avons fait, c'est organiser cette série d'engagements sur la politique numérique où nous avons informé les parties prenantes, en particulier de la société civile, de ce qui se passe avec le gouvernement nigérian.

C'est ce qu'on nous a demandé de faire. Voici comment nous les avons soutenus jusqu'à présent. De plus, concernant la disposition préoccupante du projet de livre blanc actuel, nous avons également soulevé quelques problèmes. En collaboration avec notre partenaire, Global Partners Digital, nous avons examiné ce livre blanc ensemble. Nous avons identifié certains problèmes et nous les avons communiqués en disant que ce sont des questions que nous aimerions voir abordées.

Jusqu'ici, tout va bien. Ce processus est toujours en cours, comme je l'ai dit, mais il est trop tôt pour se réjouir et dire, oh ce livre blanc est bon pour le chiffrement ou il permet le chiffrement. Tout peut toujours arriver car il y a des intérêts concurrents. Et comme Mark l'a dit, le fait d'être laissé à la merci de l'Ofcom est également une possibilité de failles dans cette partie du monde.

Il y a, nous avons vu de nombreuses lois par ici où, à la lettre, elles ne semblent même pas préoccupantes. Mais d'expérience, nous savons qu'en termes de mise en œuvre, ce qui se passe ensuite dépend de qui applique la loi. Nous sommes donc très conscients de cette perspective également. Et nous essayons aussi de nous prémunir contre cela dans ce qui sera le résultat final de ce processus.

Merci beaucoup.

Maria Paz Canales - Global Partners Digital: Merci, Boye. Certainement, je pense qu'il y a différents défis à surmonter. Certains d'entre eux se posent lors de la rédaction de cette législation, mais comme vos remarques et celles de Mark le soulignent, il y a une autre étape du processus. Il s'agit de la mise en œuvre et de l'interprétation des pouvoirs des autorités pour appliquer ces lois.

En abordant un aspect différent des défis de cette discussion, nous allons entendre Heloisa, et je vais vous demander de nous parler particulièrement de l'expérience d'Internet Lab dans le processus de développement du projet de loi brésilien 2630. Quel est le contexte de cet accord et quelles sont les principales préoccupations qui y sont liées, notamment en ce qui concerne les questions de chiffrement, et comment la société civile s'est-elle mobilisée pour éviter les menaces à la liberté d'expression et à la vie privée qui émergeaient de cette discussion ?

Merci d'être ici, Heloisa, pour votre intervention.

Heloisa Massaro - InternetLab: Merci, Maria Paz. Bonjour à tous. C'est vraiment un plaisir d'être ici aujourd'hui. Je pense que pour parler spécifiquement des problèmes qui sont apparus lors des discussions sur le projet de loi 2630, il est important, je pense, de souligner deux contextes différents.

Cela a en quelque sorte influencé la manière dont les applications de messagerie ont été abordées dans les premières versions du projet de loi. Donc, la première chose est qu'entre 2015 et 2017, le Brésil a connu quelques cas de blocage d'applications de messagerie, spécifiquement WhatsApp. Et à l'époque, les ordres de blocage provenaient de procédures, de procédures pénales dont nous n'avons pas beaucoup de détails, mais le principal problème concernait.

Les juges ou les procureurs souhaitaient accéder aux communications chiffrées, et WhatsApp ne pouvait pas fournir le contenu de ces communications. Le juge bloquait alors l'application jusqu'à ce que l'ordre soit exécuté. Il y a donc eu ces épisodes clés impliquant le chiffrement et beaucoup de malentendus sur le fonctionnement des applications de messagerie à l'époque.

Nous devons nous rappeler qu'en 2015, nous étions, on pourrait dire, dans les premières années d'utilisation massive des applications de messagerie chiffrée, comme

pour diffuser des nouvelles. Et c'est la première chose. Nous avions déjà eu quelques problèmes avec les applications de messagerie. Et il est important de souligner que le Brésil est un grand utilisateur des applications de messagerie.

Nous avons environ 99 % des utilisateurs d'Internet qui utilisent des applications de messagerie dans leur vie quotidienne. Ils utilisent des applications de messagerie tous les jours. WhatsApp Nous avons des recherches qui montrent que 99 % utiliseront WhatsApp tous les jours dans leur vie. Donc, c'est une utilisation vraiment intensive de l'application et étant donné que nous avons environ 85 % de la population connectée, cela fait vraiment beaucoup de gens qui l'utilisent.

Donc, lors des élections de 2018 au Brésil, ce qui s'est passé, c'est que nous avons eu des rapports de messages en masse sur WhatsApp violant la loi électorale. 2018 a été l'année où Bolsonaro a été élu, et c'était une élection fortement marquée par la diffusion de désinformation et des attaques dans un contexte très polarisé.

C'était le scénario, et il y avait cette énorme préoccupation que le principal canal de désinformation, de polarisation, était les applications de messagerie, et en particulier WhatsApp. Donc, en 2020, après de nombreux problèmes concernant cette information et des discussions sur les fausses nouvelles, etc., et puis nous sommes en pleine pandémie, il y a ce projet de loi, le 2630, qui est proposé au Congrès sous le nom de Loi sur les Fake News.

Et les premiers brouillons étaient vraiment préoccupants. Il y avait beaucoup de pression de la part de la société civile. Puis, au milieu de l'année 2020, l'un des premiers brouillons a été approuvé par le CNA. À l'époque, le brouillon portait principalement sur la transparence et certaines questions procédurales, mais il y avait un point vraiment controversé sur la traçabilité.

La règle stipulait essentiellement que chaque message qui était, je ne me souviens plus exactement des détails, mais c'était quelque chose comme chaque message qui était transféré à plus de cinq groupes et atteignait plus de 1 000 personnes dans une certaine période de temps. La plateforme devait conserver les métadonnées de cette action de transfert.

Donc l'idée derrière cela était que si vous pouviez identifier un message en infraction, vous seriez capable, grâce à ces métadonnées, de remonter jusqu'à la première personne qui l'a envoyé. Quels étaient les objectifs ? L'objectif principal était d'identifier d'où provenait cette information. Et, mais quels étaient les problèmes avec cela ?

Cette règle de traçabilité stipule que, tout d'abord, les plateformes, les applications ne seraient pas en mesure d'identifier, une fois qu'un message est envoyé, s'il deviendra viral ou non. Donc, en pratique, elles devraient conserver les métadonnées de chaque message jusqu'à ce que cette période soit atteinte, au moins jusqu'à ce moment-là.

Donc, pour s'assurer que si ce message devenait viral, ils auraient les métadonnées et c'était un mandat pour une rétention massive de données, avec la possibilité d'accéder à ces données dans le cadre de procédures pénales. Il n'y avait pas beaucoup d'exigences pour cet accès, donc c'était assez vague sur la manière dont on pouvait accéder à ces données.

Et en pratique, il y avait beaucoup de risques, mais la règle en elle-même n'était pas vraiment efficace pour son objectif, car elle ne prenait absolument pas en compte le fait que parfois les gens téléchargent simplement le contenu. Parfois, le contenu circule à travers les plateformes. Donc peut-être que le contenu était sur Telegram et que quelqu'un l'a copié et collé là-bas.

Donc, il était difficile de déterminer qui était la première personne à l'avoir envoyé, ce qui créait le risque de criminaliser l'utilisateur au final. Et il y avait un grand défi avec cette règle, car la société civile elle-même était assez divisée, l'opposition à la règle et au projet de loi n'était pas unanime.

À l'époque, il y avait beaucoup de pression de la part d'un groupe, une coalition d'organisations de défense des droits numériques dont nous faisons partie, pour agir ensemble afin de contrer ces règles problématiques dans le projet de loi. Et nous, avec de nombreuses organisations faisant partie de cette coalition pour les droits numériques, avons travaillé à produire à la fois des connaissances et des analyses politiques, tout en essayant de dialoguer avec le rapporteur du projet de loi.

Et c'était vraiment important à l'époque parce que le rapporteur était quelqu'un de très ouvert au dialogue avec la société civile. En 2020, 2021, nous avions produit une analyse politique sur les problèmes liés à ce type de règle. Et au final, il y a eu beaucoup de discussions aller-retour sur ce projet de loi, et il n'a pas été approuvé, principalement, non pas à cause des questions de confidentialité en elles-mêmes, mais surtout à cause des tensions politiques au sein du Congrès.

Et puis en 2023, il est revenu sous forme de projet de loi sur la régulation des plateformes. Donc le même projet de loi, le texte a été complètement reformulé et il est revenu comme un projet de loi sur la régulation des plateformes qui était plus GSA et cette disposition sur la traçabilité a été retirée. Le projet de loi, mais encore une fois, le projet de loi n'a pas été approuvé une fois de plus, également en raison de problèmes politiques.

Et maintenant, nous sommes dans une situation où la Cour suprême décidera probablement de la constitutionnalité de la règle de responsabilité des intermédiaires au Brésil. Cela changera un peu la manière dont la responsabilité est gérée au Brésil et tentera d'ajouter des points pour la régulation des plateformes. Voilà notre situation actuelle.

Merci.

Maria Paz Canales - Global Partners Digital: Merci beaucoup, Heloisa. Et je pense que c'est un moment de transition parfait pour peut-être un dialogue plus pratique dans la section suivante de cette conversation, en termes de réflexion sur la vue d'ensemble fournie par ces trois exemples différents d'engagement face aux menaces de chiffrement dans le contexte de la régulation des plateformes.

Mais aussi en réfléchissant à la manière dont cet espace offert par le travail conjoint au sein de la Global Encryption Coalition et l'opportunité d'élargir la communauté lors de cet événement aujourd'hui, autour de la Journée mondiale du chiffrement, peuvent être utiles pour poursuivre cet échange de tactiques pour l'engagement national et l'engagement.

Merci. Stratégies pour défendre le chiffrement et je veux poser quelques questions supplémentaires aux intervenants dans cette section, mais j'encourage également le public à partager leurs commentaires, leurs questions, leurs réactions, mais vraiment avec cette approche plus stratégique en tête afin que nous puissions tirer le meilleur parti des résultats de cette session en termes de points à retenir.

Et en commençant par Mark, vous avez déjà commencé à partager un peu comment, alors que l'Online Safety Act passe à la mise en œuvre et à l'application, il y a toutes ces attentes et cette possible tension sur la manière dont les autorités, et en particulier l'Ofcom, interpréteront la loi et comment nous interprétons ses propres responsabilités clés prévues dans la loi. Quels sont les messages clés que vous aurez pour les décideurs politiques qui conçoivent ou mettent en œuvre la réglementation sur la sécurité en ligne, en tenant compte de cette tension que vous avez déjà commencé à souligner dans le blog précédent ? Peut-être souhaitez-vous développer un peu plus, mais en pensant également aux interventions qui ont suivi de la part des autres collègues dans d'autres régions, quelles autres choses considérez-vous comme utiles en termes de tactiques et de points focaux d'attention pour traiter cette question de la définition des responsabilités des autorités et des actions qui peuvent être entreprises pendant la période de mise en œuvre que vous commencez déjà à expérimenter vous-même dans la mise en œuvre de l'Online Safety Act.

Merci, Mark.

Mark Johnson - Big Brother Watch: Oui, donc en ce qui concerne les prochaines phases de la mise en œuvre de la loi sur la sécurité en ligne, nous avons en fait eu une très bonne communication avec l'Ofcom, le régulateur indépendant, qui a été assez bon, je dirais, en termes de dialogue avec la société civile et d'écoute des préoccupations. Je pense que lorsque le projet de loi sur la sécurité en ligne, tel qu'il était avant de devenir une loi, passait par le Parlement.

Les débats à ce sujet n'ont pas été approfondis car il y avait presque un consensus bipartisan sur le fait que nous avions besoin d'une législation. Nous n'étions pas d'accord avec le modèle de l'Online Safety Act en raison de toutes les différentes

considérations de droits, qu'il s'agisse de la liberté d'expression, de la vie privée ou d'autres ramifications de la législation.

Mais il y avait beaucoup de soutien dans les deux chambres du Parlement. Donc, le débat n'a jamais été aussi complet qu'il aurait dû l'être au Parlement. Et il y a des leçons que nous pouvons tirer de cette expérience et sur la manière dont nous pouvons être meilleurs en tant que défenseurs et essayer de pousser pour un débat plus approfondi. Mais je pense qu'Ofcom a adopté une approche après l'adoption de la législation, sachant que nous avons soulevé des préoccupations tout au long du processus, même si ce débat n'a pas été aussi complet et approfondi qu'il aurait dû l'être au Parlement.

Et ils ont été à l'écoute, ils nous ont écoutés et consultés, ce qui est très apprécié. De plus, ils ont adopté une approche prudente car ils savent que certaines des modifications apportées par les lois seront assez radicales et pourraient vraiment reformuler notre relation avec les plateformes de médias sociaux ou les services de messagerie à l'avenir.

Ils ont donc été, ils ont engagé notre. Le plan de notre organisation, du point de vue organisationnel, est de continuer à surveiller le processus aussi attentivement que possible et de continuer à nous engager. Ofcom a mené des consultations ouvertes. Nous avons participé en termes de ce que nous pouvions faire collectivement.

J'ai trouvé que le fait d'avoir des voix externes dans le débat est extrêmement utile parce que lorsque nous engagions des discussions avec le gouvernement et avec les politiciens, même les politiciens de l'opposition, car l'opposition du Parti travailliste, évidemment ils sont maintenant au gouvernement, mais tout cela s'est passé quand les Conservateurs étaient au pouvoir au Royaume-Uni, l'opposition n'était pas très forte sur les droits numériques, le Parti travailliste n'était pas fort sur les droits numériques, et la difficulté, le défi que nous avions était que nous avions, avec cette législation, tous les différents problèmes devant nous, que ce soit en rapport avec la liberté d'expression, la vérification de l'âge, les implications sur la vie privée, ou le chiffrement.

Et donc, nous étions très dispersés. Il y avait aussi le défi du fait que les deux partis voulaient que quelque chose se passe dans ce domaine. C'était donc très difficile. Et souvent, nous approchions les mêmes politiciens encore et encore, et ils disaient, Oh, c'est encore Big Brother Watch. Ils font toujours les mêmes arguments.

Mais si nous avions des voix externes, et vers la fin du projet de loi, nous avons réussi à faire entrer plus de voix externes dans la salle. Cela crée une image plus large. Cela donne une certaine couleur aux arguments parce que nous pouvons dire que cela violera nos droits à la vie privée et que cela aura un impact sur les journalistes ou les défenseurs des droits de l'homme dans d'autres juridictions à travers le monde également.

Cela ne change pas vraiment, ce seraient les mêmes arguments que nous avançons, alors que si nous pouvions apporter d'autres voix d'autres juridictions, d'autres horizons, nous avons eu une table ronde avec une autre organisation de défense des droits où Amnesty était présente. Nous avions une organisation LGBT, divers groupes et organisations représentant des personnes pour parler des journalistes ou des défenseurs des droits de l'homme dans différentes parties du monde.

Avoir d'autres voix dans la salle a été vraiment utile, donc bien que le résultat de la législation n'ait pas été aussi positif que nous l'aurions souhaité, ce qui est utile, c'est que nous pouvons regarder en arrière avec réflexion et dire voilà ce que nous aurions pu faire davantage à l'avenir. Voilà ce que d'autres peuvent faire à l'avenir s'ils rencontrent des menaces similaires.

Évidemment, comme je l'ai dit, la bonne nouvelle est qu'Ofcom n'a pas utilisé ces pouvoirs et qu'ils sont très prudents. Ce n'est donc pas une histoire terrible, mais il y a certainement beaucoup à apprendre de cette expérience législative, qui était définitivement moins satisfaisante que souhaité.

Maria Paz Canales - Global Partners Digital: Merci, Mark.

Je pense aussi que nous ne devrions pas être trop durs avec nous-mêmes. Je pense qu'à la fin, même si le résultat final n'était peut-être pas celui que vous souhaitiez, il aurait certainement pu être pire. Vous n'auriez pas mené tous ces efforts. Donc, je pense que vous et d'autres travaillant dans ce domaine méritez du crédit.

Il est possible que la retenue dans la phase de mise en œuvre que vous observez soit également due au fait que l'autorité est consciente de la manière dont cela crée des tensions et des critiques lors de la discussion du projet de loi. Donc, je pense qu'il faut aussi voir ce côté positif dans le résultat. Et en revenant à Boye, je pense que vous mentionniez déjà dans votre intervention précédente ce concept que Mark nous a apporté en termes d'élargissement de la participation, en incluant non seulement les suspects habituels, mais aussi des groupes supplémentaires de la société civile. Je suis curieux de savoir si vous pouvez en dire plus sur ce sujet et j'espère que vous comprenez un peu mieux, Boye, en termes des choses que vous avez vues, par exemple, comment le contexte provenant d'autres juridictions et des expériences précédentes a été utile ou non dans la discussion que vous avez au Nigeria concernant l'Internet.

Et qu'est-ce qu'on peut apprendre de l'expérience des défenseurs au Nigeria au-delà de cet élément que vous avez déjà mentionné concernant l'élargissement de la participation, qui a également des points communs avec ce que Mark a apporté. La parole est à vous, Boye.

Adeboye Adegoke - Paradigm Initiative: D'accord. Merci beaucoup, Maria. C'est intéressant parce que je ne pense même pas que nous aurions cette conversation au Nigeria si la loi britannique sur la sécurité en ligne n'existait pas.

Pas parce que la réflexion n'existait pas ou n'existerait pas toujours, mais c'est aussi une question de réputation d'utiliser des législations. qui cherchent à traiter des armes, que ce soit dans les espaces numériques ou hors ligne, comme un outil pour réprimer les espaces civiques. Il y a eu des réactions très significatives de la part de la société civile ou même des citoyens contre le gouvernement chaque fois qu'il essaie d'introduire une législation de ce type.

Ainsi, le gouvernement doit pouvoir citer des exemples de pays qui seraient généralement considérés comme de bons exemples pour que le gouvernement nigérian puisse dire confortablement que vous pouvez voir ce qui se passe ailleurs dans le monde. Et c'est aussi ce qui se passe dans des endroits que vous appelleriez des sociétés justes ou démocratiques.

Cela donne donc une sorte de validation supplémentaire, même pour envisager de le faire en premier lieu. Cela vous montre que c'est d'une très grande influence en regardant ce qui s'est passé en Australie et au Royaume-Uni. Cela a influencé la décision du gouvernement d'être suffisamment audacieux pour se manifester sans trop de résistance de la part des citoyens, car le déficit de confiance est très faible ici entre le gouvernement et le peuple.

Et donc, chaque fois que le gouvernement envisage certains types de législation, les citoyens ont tendance à voir cela sous un angle négatif et tout ça. Mais ensuite, quand le gouvernement peut pointer des exemples de ce qui se passe au Royaume-Uni et en Australie, que la personne moyenne ici considère comme des sociétés saines, alors si cela se passe dans ces juridictions, pourquoi ne pourrions-nous pas avoir cette conversation ici?

Voilà jusqu'à quel point cela a influencé la décision d'entreprendre ce voyage au Nigeria. Cependant, au-delà de cela, cela influence également le test, le contenu de la législation proposée. Parce que ce qui se passe généralement, c'est que les pays qui adoptent ce type de législation en premier deviennent un modèle pour les autres.

En ce moment même, si vous regardez bien, même dans le livre blanc, des références ont été faites à l'Online Safety Act du Royaume-Uni. Des références ont également été faites à la version australienne, car cela sert de modèle que nous utilisons. Et nous essayons ensuite de contextualiser tout ce que nous voyons dans ces modèles à notre réalité en tant que Nigérians et Africains.

Nous, nous sommes très conscients et très attentifs à l'impact ou à quel point ce qui se passe ailleurs influence ce qui se passe dans notre partie du monde. Et, cela vous

intéresserait même, je dirais même que même les processus mondiaux comme les cadres de l'ONU.

Comme le cadre de la GDC ou de l'UNESCO, par exemple, ou la régulation des plateformes, ils n'ont pas autant d'impact que les cadres nationaux de certains pays. Dans de nombreux pays africains, y compris le Nigeria. Ces lois nationales qui ont été promulguées, que ce soit au Royaume-Uni, dans l'UE, aux États-Unis ou ailleurs, ont une importance significative.

Influencer la forme de l'approche. Et en fait, laissez-moi aussi vous donner une anecdote très intéressante au Nigeria lorsque nous avons introduit le projet de loi sur le Digitaliste et la Liberté. Et lorsque nous avons présenté le projet de loi au Parlement, l'une des choses qu'on nous a demandées est que le parlement aimerait voir l'entrepôt.

Cela a été fait, ils aimeraient même probablement aller en mission d'étude pour voir ce qui se passe dans cette tradition. Et au moment où nous avons rédigé le projet de loi sur la liberté numérique, aucun pays n'avait une conversation similaire à l'époque. La chose la plus proche à ce moment-là était le Marco Civil au Brésil, ce qui a ensuite créé une discussion sur la manière dont nos gouvernements africains abordent la législation, en particulier la réglementation et la législation numériques.

C'est une supposition que vous devez attendre que les grands frères montrent la direction avant de prendre une décision. C'est cette réticence à assumer un rôle de leadership lorsqu'il s'agit de définir la direction pour la régulation des plateformes numériques ou de la technologie en général. Merci.

Maria Paz Canales - Global Partners Digital: Merci, Boye. Oui, c'est certainement un défi. Je pense que tout le monde peut s'y retrouver, en particulier dans les pays de la majorité mondiale, en cherchant des modèles bons et mauvais et en continuant dans cette voie. Le Brésil a été un leader dans de nombreux domaines liés au numérique, comme vous venez de le mentionner, le Marco Civil.

C'est pourquoi il est si intéressant de vous avoir ici, Heloisa, pour parler de votre expérience. Quels sont vos enseignements en termes de pièges et d'opportunités liés à la régulation des plateformes en ligne, en particulier en ce qui concerne la discussion sur le chiffrement ? Et peut-être que je pourrais faire une provocation pour un dernier tour de commentaires un peu plus tard pour chacun de vous en tant que panélistes, donc pas seulement pour Heloisa, mais pour vous trois dans vos remarques finales, j'aimerais que vous abordiez.

À quoi ressemblera une approche favorable au chiffrement dans le contexte de la régulation des plateformes en ligne selon l'expérience que vous avez déjà eue en abordant cette question ? Parlez-nous un peu des leçons tirées du processus brésilien. Et si vous souhaitez aborder cette question plus générale, ce serait également

formidable et je donnerai la parole plus tard à Mark et Voya pour qu'ils partagent leur point de vue.

À toi Heloisa, merci.

Heloisa Massaro - InternetLab: Merci Maria Paz. Tout d'abord, je dirais que nous apprenons des choses depuis 2020, donc quatre ans d'apprentissage avec cet accord qui va et vient et prend de nombreuses formes et approches différentes. Mais, je dirais que, tout d'abord, une chose qui a été vraiment centrale dans notre travail est d'offrir des diagnostics meilleurs et plus nuancés.

Et je sais que cela a un impact limité d'une certaine manière, mais il est vraiment important d'apporter cela à la conversation. Et pourquoi je dis cela, je le dis parce que lorsque nous parlons des applications de messagerie, par exemple, nous avons commencé à développer des recherches quantitatives et qualitatives sur l'utilisation des applications de messagerie au Brésil pour la communication politique.

Et l'un de nos principaux enseignements est de voir comment la messagerie, principalement WhatsApp, est une plateforme vraiment importante et connecte d'autres plateformes, mais ce n'est pas le seul protagoniste. Merci beaucoup. De plus, nous avons pu montrer la variété d'utilisations de WhatsApp, donc lorsque vous mettez en œuvre une mesure visant à, je ne sais pas, traiter un problème lié à cette information qui pourrait ne pas être une question spécifique sur une application de messagerie, vous impactez vraiment les petites entreprises.

Vous impactez vraiment la vie quotidienne des gens. Et nous avons essayé d'apporter cela au dialogue ces dernières années. Et c'est l'une des choses que nous avons trouvées vraiment importantes et utiles car cela aide à l'analyse des politiques et nous permet de développer de meilleures approches. L'autre chose, c'est que travailler en coalition pendant ce processus a été vraiment important.

Les organisations de défense des droits numériques ont vraiment travaillé ensemble pendant le processus de régulation des plateformes, et cela a été vraiment important pour créer, en quelque sorte, pour essayer de résoudre les désaccords entre nous dans cet espace sûr avant de vraiment plaider pour une autre approche.

Et cela a été vraiment important pour ce processus. Je dirais que beaucoup de victoires que la société civile a obtenues pendant ce processus ont été grâce à ce travail de coalition. Et nous avons également pu tirer le meilleur de chaque organisation. Nous avions des organisations comme Internet Lab, qui produisaient des recherches axées sur les faits.

Vous auriez des organisations qui seraient plus sur le terrain à faire du plaidoyer au Congrès. Donc, c'était vraiment important. Et une dernière leçon que je tirerais de ces

aspects positifs est le dialogue avec les parties prenantes. Et quand je dis dialogue avec les parties prenantes, c'est vraiment écouter et prendre en compte les problèmes.

que les parties prenantes essaient de résoudre ou quels sont les défis auxquels elles sont confrontées. Et cela s'applique aussi bien au secteur privé pour vraiment comprendre en profondeur quels sont les problèmes qui apparaissent, mais aussi en travaillant avec des professionnels du droit, par exemple. Donc, dialoguer vraiment avec les procureurs, les juges, et développer ce type de.

une capacité d'écoute qui aide vraiment dans ce processus également. Et en ce qui concerne les défis, j'ajouterais deux choses avant de conclure. Je dirais que malgré toutes ces victoires que nous avons eues, nous n'avons pas de projet de loi qui a été approuvé. Donc, à la fin de la journée, vous avez les disputes politiques qui éclipsent tout et supplantent en quelque sorte tout le travail qui a été accompli.

Et le pouvoir des médias traditionnels, surtout au Brésil, ne peut pas être sous-estimé. Les médias traditionnels ont joué un rôle crucial dans ce processus de négociation et ont été l'un des éléments qui ont bloqué le projet de loi. Ce sont mes dernières considérations, et en ce qui concerne la question de Maria Paz sur la régulation des plateformes favorables au chiffrement, je n'ai pas la réponse, mais j'ajouterais une chose que je pense vraiment importante à prendre en compte : il est essentiel de bien distinguer les réseaux sociaux des applications de messagerie privée.

et comprendre que la réglementation est différente. Et quand je dis cela, j'inclus également dans la conversation le fait que parfois les applications de messagerie deviennent des plateformes de médias sociaux et cela doit également être pris en compte. Sinon, nous aurons des réglementations qui visent à attaquer les fonctionnalités de médias sociaux des applications de messagerie et à saper la vie privée et la liberté d'expression.

C'est tout. Merci à tous.

Maria Paz Canales - Global Partners Digital: Merci, Heloisa. Donc, je pense que, comme d'habitude, nous manquons de temps avec cette discussion très intéressante, mais je suis intéressé d'entendre ton avis, Mark, et ton avis, Boye, sur cette question, à quoi ressemble une bonne approche pour vous. De plus, je suis conscient qu'il y a une question supplémentaire qui a été posée dans le chat et que je pourrais peut-être essayer de prolonger notre temps et vous la poser, l'inclure dans votre réponse, qui est liée à des opportunités plus spécifiques que vous voyez venir dans le pipeline en termes de collaboration sur des propositions législatives ou en termes de canaux de mise en œuvre ou de défis dans la mise en œuvre de certaines des législations que vous suivez ou toute autre opportunité que vous voyez à l'horizon où ce travail de coalition plus global peut être utile au service des autres qui commencent à avoir cette discussion.

Donc pour les deux questions, peut-être. Très rapidement, vous pouvez répartir votre temps comme vous le souhaitez. Mark, puis Boye, merci.

Mark Johnson - Big Brother Watch: Oui, je vais essayer d'être bref. Oui, sur la question de ce à quoi pourrait ressembler une bonne régulation, c'est une question très difficile. Nous, lorsque nous abordons le projet de loi sur la sécurité en ligne, nous sommes très clairs, nous ne sommes pas amis, pas proches amis ou alliés des plateformes de médias sociaux, nous reconnaissons qu'il y a beaucoup à faire pour tenir ces entreprises responsables, mais nous ne pensions pas que la loi sur la sécurité en ligne était nécessairement la bonne approche.

Nous préférerions voir une réglementation qui s'attaque aux modèles économiques des entreprises, qui mette fin au commerce massif des données et qui considère la confidentialité et la liberté d'expression comme des éléments centraux de toute réglementation. Je pense. En ce qui concerne les défis spécifiques que différentes juridictions tentent de relever lorsqu'elles réfléchissent à contourner ou à saper le chiffrement de bout en bout, il s'agit généralement de contenus liés au terrorisme, de matériel d'abus sexuels sur enfants, et peut-être de désinformation, comme nous l'avons entendu dans le cas du Brésil. Le principe doit rester que le chiffrement de bout en bout ne peut pas être compromis et que toute surveillance doit être basée sur des soupçons raisonnables, et doit être ciblée, et que l'ensemble de la plateforme ne doit pas être compromis.

Je sais que de nombreuses grandes entreprises de messagerie privée collaborent très étroitement avec les forces de l'ordre dans différentes juridictions à travers le monde. Il pourrait y avoir des moyens de formaliser certaines de ces relations sans compromettre l'ensemble des canaux et la confidentialité des personnes qui les utilisent.

C'est une réponse un peu vague, mais je pense que la chose la plus importante, évidemment, comme tout le monde à l'école le sait, c'est qu'il devrait y avoir certaines lignes rouges que nous ne devrions jamais être prêts à franchir. En termes d'opportunités de collaboration, il est possible que WhatsApp ou Signal ou d'autres grands services de messagerie chiffrée de bout en bout puissent facilement se tourner vers les régulateurs britanniques ou le gouvernement britannique et dire qu'ils sont heureux de ne pas se conformer à ce que vous faites. En fait, les deux grandes plateformes ont évoqué la possibilité de se retirer du marché ou de résister aux menaces, au chiffrement de bout en bout posées par la législation sur la sécurité en ligne.

Mais il existe des marchés ou des juridictions plus importants pour ces plateformes qui envisagent actuellement une régulation, comme le contrôle des discussions dans l'UE. Avec 400 millions d'utilisateurs ou plus, il est beaucoup plus difficile pour ces plateformes de résister ou de menacer de se retirer.

Donc, la probabilité qu'ils doivent modifier leur produit ou service dans ce cas est nettement plus élevée par rapport à un exemple plus petit comme le Royaume-Uni. Donc évidemment, pour les collègues dans l'UE, nous ne sommes plus dans l'UE, mais pour les collègues qui y sont, si c'est utile et que nous pouvons aider, et je sais que les discussions sont toujours en cours en ce moment, je pense que nous sommes dans une assez bonne position, mais s'il y a quoi que ce soit que nous puissions faire et pour les collègues du monde entier, alors j'imagine que ce serait une juridiction assez importante pour s'exprimer et aider.

Oui.

Maria Paz Canales - Global Partners Digital: Merci, Mark. Boye, quelle est votre opinion sur cette approche favorable au chiffrement pour la régulation des plateformes, à quoi cela ressemblerait-il ?

Adeboye Adegoke - Paradigm Initiative: Oui, je pense que le débat pour nous, dans le cadre du débat de longue date autour de la vie privée et de la sécurité, concerne à quoi pourrait ressembler une réglementation de plateforme favorable au chiffrement.

Je pense que ce qui est important, c'est de reconnaître les enjeux conflictuels en termes de la manière dont, par exemple, compromettre le chiffrement peut avoir des impacts significatifs sur la vie privée, les droits des utilisateurs à la vie privée, et peut également exposer certains utilisateurs à des risques. Mais nous ne devons pas non plus négliger l'aspect de la manière dont le chiffrement peut également être mal utilisé ou devenir un outil pour les acteurs malveillants.

Je pense que ce qui est important, c'est la mise en place de garanties qui assurent également que les autorités ne puissent pas utiliser le chiffrement comme une arme pour atteindre des objectifs politiques. Utiliser, affaiblir le chiffrement pour cibler certaines personnes, probablement en raison de leurs croyances politiques, religieuses ou de leur mode de vie, ou de toute autre caractéristique distinctive qu'elles possèdent.

Je pense que nous sommes guidés par les Instruments Nationaux des Droits de l'Homme en ce qui concerne notre approche des limitations des droits, tels que les droits humains de pouvoir communiquer, d'avoir des communications chiffrées. Je pense que la limitation de ces droits doit suivre des directives très claires. La procédure des 3 tests, par exemple.

Je ne crois pas que les autorités devraient avoir un pouvoir général leur permettant d'accéder aux communications chiffrées par des portes dérobées, par exemple, ce qui est en termes pratiques et en termes d'expériences réelles de nombreuses personnes, ce qui est généralement le cas, notamment dans les pays où les institutions sont faibles, et je pense que cela sera très parlant pour la plupart des pays du Sud global.

Le manque d'institutions solides a créé un système dans lequel les autorités profitent généralement de cette faiblesse institutionnelle pour contourner les règles, harcelant parfois les entreprises de médias sociaux ou les entreprises fournissant des services de communication, exigeant un accès, exigeant un accès clandestin aux communications sans suivre la procédure, sans respecter l'état de droit, sans aucune légitimité, et tout cela.

Donc, je pense que l'équilibre, ce à quoi l'équilibre ressemblera pour moi, c'est de créer un système qui respecte la procédure, qui respecte l'état de droit, qui n'accommode que les préoccupations légitimes, que ce soit par les agences de sécurité ou les autorités, mais pas un accès généralisé ou une interdiction généralisée des communications chiffrées. Nous devons limiter le pouvoir des forces de l'ordre, le pouvoir des autorités d'accéder aux coulisses des conversations et des communications importantes.

Cela doit être des cas exceptionnels où cela est nécessaire. Cela ne doit pas, cela ne devrait pas être la norme. Cela ne devrait pas être la norme. C'est essentiellement ce que je dis. Et dans notre travail au Nigeria également autour de l'exploitation en ligne, notre argument a été de créer de solides garanties, une protection en termes de principes contenus dans les lois internationales sur les droits de l'homme pour guider les efforts du gouvernement à cet égard.

Je suis très conscient du temps, donc je vais m'arrêter là.

Maria Paz Canales - Global Partners Digital: Merci beaucoup, Boye, et tu me donnes la clé parfaite pour les conclusions finales. Merci beaucoup à vous tous pour vos perspectives. J'espère que cela pourra être utile en termes de points d'action pour les personnes qui suivent la conversation d'aujourd'hui.

Et je résumerai que certains des éléments clés à prendre en considération d'après votre expérience sont cette idée d'élargir le groupe. Et je pense qu'il est important d'avoir ce type de participation afin d'avoir une communauté plus large pour s'occuper de cela et comprendre les nuances pour différentes communautés de l'impact négatif de l'utilisation du chiffrement, l'idée de travailler en coalition pour façonner cette discussion dans un espace plus sûr avant d'engager d'autres batailles avec les autorités, la diversité des contextes et des usages différents et des acteurs différents ici, en ne pensant pas seulement aux grandes entreprises technologiques, mais aussi à la diversité des mises en œuvre de ces différentes applications et le rôle qu'elles jouent dans la société. L'accent sur le défi, revenant au dernier point de Boye, sa remarque de clôture, les défis, et j'essaie de me concentrer sur ces défis et l'approche gouvernementale d'un point de vue des droits de l'homme.

Avec cela, je vous remercie tous et je vais clore cette session en vous invitant à la prochaine de cette très intéressante Conférence de la Coalition pour la Journée Mondiale du Chiffrement. Merci.