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

Como será a regulamentação de plataformas amigáveis à criptografia? Perspectivas inter-regionais sobre a regulamentação de plataformas online e criptografia

Maria Paz Canales - Global Partners Digital: Boa tarde, eu sou Maria Paz Canales. Sou a Chefe de Política Jurídica e Pesquisa e Parceira Global Digital. E tenho o prazer, como minha organização, como membro da Coalizão Global de Criptografia, de ser sua moderadora hoje nesta conversa muito relevante que temos. Intitulada 'Como será a regulamentação de plataformas amigáveis à criptografia? Perspectivas inter-regionais sobre a regulamentação de plataformas online e criptografia'.

Para contextualizar um pouco esta conversa que eu estava introduzindo com o título da sessão, e que será compartilhada substancialmente pelo nosso maravilhoso palestrante, quero compartilhar algumas palavras sobre isso. Vivemos em uma era onde muito mais pessoas têm acesso à criptografia do que nunca antes.

No entanto, também estamos vendo um número alarmante de novas propostas que irão minar isso, ameaçando a privacidade e a segurança da comunicação digital,

colocando em risco os direitos e o bem-estar de indivíduos e grupos específicos. Ao mesmo tempo, há necessidades bem reconhecidas de proteger melhor as crianças contra danos e garantir a responsabilização por abusos das empresas.

No entanto, neste contexto complexo, uma resposta regulatória Nossas respostas a essas questões devem ser nuançadas e consultivas, respeitando e cumprindo os princípios de legalidade, necessidade, proporcionalidade, legitimidade e não discriminação em nossa perspectiva como defensores da proteção da criptografia. Esta discussão em painel pretende reunir esses maravilhosos defensores que vou apresentar em alguns minutos, do Reino Unido, Nigéria e Brasil, que têm trabalhado na interseção de direitos humanos e tecnologia para compartilhar suas experiências e conhecimentos nesse engajamento na discussão sobre regulação de plataformas nacionais.

Através desta discussão, o que esperamos é mudar táticas e estratégias para engajar nesta discussão. E quatro respostas regulatórias que sejam proporcionais e protetoras da criptografia. Nosso objetivo com esta sessão é produzir aprendizados e lições que possam ser úteis para a comunidade em geral no que eles precisam defender em diferentes momentos, em diferentes geografias, em diferentes jurisdições.

Agora vou apresentar meu ilustre palestrante. Hoje temos conosco Adeboye Adegoke, que é Gerente Sênior da Paradigm Initiative da Nigéria. Temos também Heloisa Massaro, que é Diretora do Internet Lab Brasil. E, por último, mas não menos importante, temos Mark Johnson, que é Gerente de Advocacy na Big Brother Watch do Reino Unido.

E vamos começar a primeira parte desta discussão, particularmente com uma análise aprofundada da defesa no processo regulatório das plataformas online nacionais. Cada um desses ilustres palestrantes terá cerca de quatro minutos. Temos quatro minutos para compartilhar um pouco de sua introdução. E sem mais delongas, começarei com você, Mark, pedindo que compartilhe um pouco de sua experiência, considerando que o Reino Unido foi um dos primeiros países a desenvolver um sistema dedicado à segurança online, em vez de utilizar leis existentes para abordar algumas das preocupações com a regulamentação das plataformas. Você pode nos contar sobre seu envolvimento no processo de elaboração do Online Safety Act, ao qual estamos nos referindo, e a luta para defender a forte proteção da criptografia? Como foi enquadrada a discussão e como o Big Brother Watch e outros grupos da sociedade civil que se coordenaram para enfrentar essa proposta responderam a essa crítica, particularmente sobre o papel da criptografia?

Muito obrigado por estar aqui, Mark. A palavra é sua.

Mark Johnson - Big Brother Watch: Muito obrigado, Maria, e boa tarde, se for tarde onde você está.

Sim, se você não conhece a Big Brother Watch, somos uma organização de liberdades civis baseada no Reino Unido. Temos um interesse particular na interseção entre direitos humanos e tecnologia e o título, obviamente, da discussão é como seria uma regulamentação de plataformas amigável à criptografia.

Não quero ser negativo na minha perspectiva, mas infelizmente, pela minha experiência, tenho um bom exemplo de como pode ser uma regulamentação ruim e não amigável à criptografia com o Ato de Segurança Online do Reino Unido. Para aqueles que não estão familiarizados com este Ato, foi uma legislação aprovada pelo nosso Parlamento no ano passado, e levou vários anos para ser elaborada.

A ideia de um Ato de Segurança Online do Reino Unido foi sugerida pela primeira vez no início dos anos 2010, mas basicamente a forma como esse tipo de regulamentação funciona é que cria ou nomeia um regulador independente para estabelecer códigos de prática predominantemente para grandes sites de mídia social abertos. E esses códigos de prática ditam regras sobre como eles devem moderar o conteúdo em seus sites.

As primeiras versões do esboço do projeto de lei não mencionavam serviços de mensagens privadas. Na maior parte, os serviços de mensagens privadas estavam isentos, e a ideia dessa regulamentação era criar uma forma de regular o conteúdo nas principais plataformas como Meta, X, e assim por diante.

Claro, havia várias considerações sobre a liberdade de expressão, e trabalhamos no projeto de lei predominantemente no início a partir de uma perspectiva de livre expressão, pensando em como a moderação de conteúdo e as regras em torno disso poderiam impactar o direito dos usuários à liberdade de expressão online. Mas enquanto o projeto de lei estava sendo desenvolvido, houve uma pressão simultânea do nosso Departamento de Interior aqui no Reino Unido para inserir disposições na legislação sobre serviços de mensagens privadas e, em particular, serviços de mensagens criptografadas.

E, por fim, a versão final do projeto de lei incluiu disposições que ficaram conhecidas coloquialmente como notificações de tecnologia. Em essência, essas notificações de tecnologia eram uma maneira muito sutil, pouco examinada e silenciosa de essencialmente obrigar as plataformas a usar tecnologias como a varredura no lado do cliente ao lidar com material de abuso infantil em seus sites.

Isso apesar do fato de que, no Reino Unido, os órgãos de aplicação da lei e outras agências já possuem uma série de poderes para lidar com essa questão, que obviamente é uma questão de direitos e deve ser levada extremamente a sério, mas já havia uma gama de poderes disponíveis para muitos dos nossos órgãos e agências de aplicação da lei para lidar com isso.

E esses poderes foram inseridos apesar das questões de privacidade, precisão e até mesmo compatibilidade das tecnologias em questão ou a falta de compatibilidade com

os dispositivos dos usuários. E assim, essas disposições foram adicionadas à legislação sem um grande escrutínio do ponto de vista da sociedade civil. Nós nos envolvemos no processo, mas, claro, este era um projeto de lei vasto que tratava da regulamentação de várias partes diferentes da Internet, predominantemente plataformas de mídia social abertas, mas também considerava não apenas a moderação de conteúdo, mas também a verificação de idade e outras várias disposições, incluindo alguns novos crimes.

Do ponto de vista da sociedade civil, estamos extremamente sobrecarregados, considerando que já estávamos focados em questões de liberdade de expressão e outros problemas relacionados à legislação. Nós nos envolvemos com o governo na época, mas infelizmente o governo não estava particularmente disposto a nos ouvir, e apresentamos os argumentos, tanto os argumentos de direitos.

os problemas de precisão quando se trata de tecnologias como a varredura no lado do cliente e também os tipos básicos de questões sobre como os processos funcionariam. Infelizmente, apesar de nossos melhores esforços trabalhando com parlamentares da oposição, não conseguimos remover esses poderes do projeto de lei, então eles se tornaram lei no ano passado.

A boa notícia do nosso lado, eu acho, é que até agora o regulador que o governo nomeou, a Ofcom, tem adotado uma abordagem bastante cautelosa, então os poderes ainda não foram usados. E eu acho que é bem-vindo que a Ofcom tenha sido muito cautelosa. Eles estão muito atentos às considerações sobre direitos, ao impacto na privacidade e a muitas das questões em jogo.

A dificuldade é que estamos muito à mercê da Ofcom para adotar essa abordagem. Eles podem mudar sua abordagem a qualquer momento. Eles podem se tornar significativamente mais intervencionistas. E o quadro regulatório do Ato de Segurança Online do Reino Unido é um quadro que está aberto à influência política pela forma como está escrito.

Portanto, existe a chance de que o governo possa pressionar a Ofcom a usar esses poderes para obrigar uma plataforma de mensagens criptografadas como o WhatsApp, como o Signal, a escanear todas as mensagens de todos os usuários no site. E há muito poucas maneiras de impedir isso. Claro, sempre há a chance, e na verdade, acho bastante possível que esses poderes possam ser contestados em um tribunal no Reino Unido, e a Organização de Direitos Humanos, a Organização de Liberdade de Expressão, Index on Censorship, encomendou uma opinião legal que dizia que era provável que os poderes fossem ilegais.

Na verdade, a opinião foi escrita por Matthew Ryder, que disse que a Ofcom agora tem mais poderes do que a GCHQ, nossa agência de espionagem digital aqui no Reino Unido, como resultado da lei. É bem-vindo no momento que a Ofcom esteja cautelosa, os poderes não foram implementados. Mas há uma chance de que haja um desafio legal se eles forem usados no futuro.

Do nosso lado, é uma situação difícil porque estabelecemos um precedente ruim. Isso terá um impacto nos usuários ao redor do mundo, porque se esses poderes forem usados, e se o WhatsApp ou o Signal forem forçados a comprometer a segurança de seus usuários ao minar a criptografia de ponta a ponta, isso também afetará pessoas em todo o mundo.

Portanto, há um impacto nos direitos em outras partes do mundo, não apenas no Reino Unido. E, infelizmente, é um mau exemplo de regulamentação. Mas ainda há oportunidades para lutarmos contra isso. Estamos analisando isso o máximo que podemos. E se o governo algum dia pensar em pressionar a Ofcom, ou se a Ofcom algum dia pensar em usar esses poderes, seremos os primeiros a reagir e tentar impedir que eles sejam usados.

Maria Paz Canales - Global Partners Digital: Muito obrigado, Mark, por essas perspectivas, embora, sim, sejam menos positivas do que gostaríamos para esta conversa, mas acho que há aprendizados relevantes que parecem positivos em termos de estratégia e uma oportunidade para também colaborar com uma organização que trabalha em outras jurisdições para mostrar quais poderiam ser as maiores consequências desse tipo de abordagem legislativa em outras partes do mundo. E, passando para essa conversa, gostaria de pedir ao Boye que compartilhe sua perspectiva sobre qual tem sido sua experiência e a experiência da Paradigm Initiative ao se envolver no processo de elaboração do projeto de lei de proteção contra danos online na Nigéria, como você tem participado da fase consultiva desse projeto para moldar esse desenvolvimento e como muito obrigado por se juntar a nós hoje, e esperamos que este tópico de criptografia tenha surgido e como talvez você possa conectar algumas das experiências compartilhadas por Mark e como essas poderiam ser úteis ou não ou diferentes no desenrolar da discussão na Nigéria.

A palavra é sua.

Adeboye Adegoke - Paradigm Initiative: Tudo bem. Obrigado, Maria. Acho que muito do que o Mark disse também ressoou comigo. Mas acho que a principal diferença é que, online, o projeto de lei de segurança online do Reino Unido e o projeto de lei de danos online na Nigéria, o projeto de lei de danos online na Nigéria ainda está em andamento.

Ainda não temos uma lei. Na verdade, nem temos um projeto de lei. Tudo o que temos é um documento preliminar que define a direção que seguiremos. Agora, em termos da nossa experiência com isso, acho que se baseia em nossos anos de trabalho defendendo a proteção dos direitos digitais na Nigéria. Então, quando o governo nigeriano falou sobre a criação de um comitê para aconselhá-lo sobre como deveria ser a proteção contra danos online na Nigéria.

Eles decidiram nos convidar para a sala, mas não nos convidaram apenas. Foi também porque estamos tentando criar um equilíbrio no engajamento, dizendo que vocês têm

defendido a proteção dos direitos digitais. Vocês também propuseram uma lei sobre direitos digitais e liberdade na Nigéria.

Então, o que eles propuseram no início foi ter uma legislação que abordasse direitos digitais e saúde online. A proposta naquela época era ter uma legislação de proteção de direitos digitais e saúde online. Mas achamos isso complicado para nós, dado que sabemos como esse processo aconteceu.

Não queríamos que as duas questões se misturassem. Queremos que a Nigéria tenha uma legislação que trate dos direitos e liberdades digitais, enquanto pode também abordar a questão dos danos online em uma legislação separada. Então, cancelamos isso. Está bem. Estamos neste comitê para garantir que haja proteção digital em seu esforço para regular os danos online, mas não dê esse nome porque, uma vez que o fizerem, será difícil para nós.

Então, a forma de regulamentação, por exemplo, quando Mark estava falando sobre a experiência do Reino Unido, ele mencionou algo sobre como, no produto final, eles não puderam mudar certas coisas que gostariam de mudar. Então, também sabemos que nosso poder era limitado em termos de poder determinar como o documento final iria ficar.

Portanto, queremos encerrar nossa defesa por uma legislação de direitos digitais na Nigéria, modelando um tópico que busca proteger as atividades online, dado que já conhecemos certos desafios que podem surgir nesse contexto. Então, começamos a trabalhar como membro do comitê diretor, parte da iniciativa junto com muitas outras organizações que fazem parte desse comitê.

Muitos deles são grupos de reflexão, muitos deles também trabalham nas áreas de tecnologia e políticas. Claro, as questões eram claras em termos do que é de extrema importância para cada uma das partes interessadas. Para nós, o que era fundamental era garantir que isso não se tornasse mais uma desculpa para violar direitos.

Como vimos muitas vezes nesta parte do mundo, onde a lei que aborda o cibercrime se tornou uma ferramenta de opressão, uma ferramenta para suprimir o espaço cívico ou para alvejar defensores dos direitos humanos. Portanto, isso sempre foi uma prioridade. Esse processo levou ao lançamento de um livro branco sobre a proteção online na Nigéria.

E se você olhar para esse white paper hoje, ele não parece tão ruim quando se trata da questão da criptografia especificamente. Mas isso é porque começamos a conversa a partir da proteção dos direitos digitais. Mas, como eu disse, ainda é cedo para comemorar porque o que temos é um white paper, e do white paper vamos ter um projeto de lei, e o projeto de lei passará por muitos processos, os políticos vão analisá-lo, as diferentes agências governamentais vão opinar sobre tudo isso, e muitas coisas ainda podem acontecer.

Mas uma coisa que temos feito de forma muito consistente é monitorar o processo. Não apenas porque somos membros do comitê gestor, mas também porque sempre monitoramos o cenário dos direitos digitais na Nigéria em geral, e seremos os primeiros a soar o alarme quando algo der errado.

Então, uma das coisas que também fizemos foi realizar o que gostamos de chamar de Série de Engajamento em Políticas Digitais com o Grupo da Sociedade de Radiodifusão para informá-los sobre o que está acontecendo com esse processo, porque isso ainda não é público. Poucas pessoas sabem que esse processo está em andamento.

Tenho certeza de que as pessoas nesta chamada estarão se perguntando o que algo assim está acontecendo na Nigéria. Claro, não era público. Mas o que fizemos foi realizar essa série de engajamento de políticas digitais onde informamos as partes interessadas sobre o que está acontecendo, especialmente do espaço da sociedade civil, para dizer o que está acontecendo com o governo nigeriano.

Isso é o que nos pediram para fazer. É assim que os temos apoiado até agora. Além disso, em relação à provisão preocupante do rascunho do white paper neste momento, também levantamos algumas questões. Trabalhando com nosso parceiro, Global Partners Digital, analisamos esse white paper juntos. Identificamos alguns problemas e os comunicamos, dizendo que são questões que gostaríamos que fossem abordadas.

Até agora, tudo bem. Esse processo ainda está em andamento, como eu disse, mas é muito cedo para comemorar e dizer, oh, este livro branco é bom para criptografia ou permite criptografia. Qualquer coisa pode acontecer porque há interesses concorrentes. E assim como Mark disse, a questão de ficar à mercê da Ofcom também é uma possibilidade de falhas nesta parte do mundo.

Existem, temos visto muitas leis por aqui onde, na letra da lei, nem parecem preocupantes. Mas, pela experiência, sabemos que em termos de implementação, o que acontece depois depende de quem implementa a lei. Então, estamos muito conscientes dessa perspectiva também. E também estamos tentando nos proteger contra isso no que será o resultado final deste processo.

Muito obrigado.

Maria Paz Canales - Global Partners Digital: Obrigado, Boye. Com certeza, acho que há diferentes desafios a serem superados. Alguns deles ocorrem durante o processo de elaboração desta legislação, mas, sem dúvida, como seus comentários e os de Mark destacam, há outra etapa do processo. Preocupação em termos de implementação e interpretação dos poderes das autoridades para aplicar essas leis.

Indo para um sabor diferente nos desafios desta discussão, ouviremos Heloisa, e eu vou pedir que você nos conte particularmente sobre a experiência do Internet Lab ao se

envolver no processo de desenvolvimento do Projeto de Lei 2630 do Brasil, qual é o contexto do acordo e as principais preocupações relacionadas a ele, especialmente sobre questões de criptografia, e como a sociedade civil se mobilizou para evitar ameaças à liberdade de expressão e privacidade que surgiram nesta discussão.

Obrigado por estar aqui, Heloisa, para a sua palestra.

Heloisa Massaro - InternetLab: Obrigada, Maria Paz. Olá a todos. É realmente um prazer estar aqui falando hoje. Acho que, para falar especificamente sobre as questões que surgiram durante as discussões do projeto de lei 2630, é importante destacar dois contextos diferentes.

Isso influenciou um pouco a forma como os aplicativos de mensagens foram abordados pelo projeto de lei em seus primeiros rascunhos. Então, o primeiro ponto é que entre 2015 e 2017, o Brasil teve alguns casos envolvendo o bloqueio de aplicativos de mensagens, especificamente o WhatsApp. E naquela época, as ordens de bloqueio vinham de processos criminais dos quais não temos muitos detalhes, mas a questão principal envolvia.

Juízes querendo acesso ou promotores querendo acesso às comunicações que estavam criptografadas e o WhatsApp não conseguia fornecer o conteúdo dessas comunicações, e o juiz bloqueava o aplicativo até que a ordem fosse cumprida. Então, houve esses episódios-chave envolvendo criptografia e muito desse mal-entendido sobre como os aplicativos de mensagens funcionavam naquela época.

Precisamos lembrar que em 2015, estávamos, podemos dizer, nos primeiros anos de uso massivo de aplicativos de mensagens criptografadas, como espalhar notícias. E isso é a primeira coisa. Já tivemos alguns problemas com aplicativos de mensagens. E é importante destacar que o Brasil é um grande usuário de aplicativos de mensagens.

Temos cerca de 99 por cento dos usuários da Internet usando aplicativos de mensagens em suas vidas diárias. Eles usam aplicativos de mensagens todos os dias. Temos pesquisas que mostram que 99 por cento usam o WhatsApp todos os dias em suas vidas. Então, é um uso realmente intenso do aplicativo e considerando que temos cerca de 85 por cento da população conectada, é realmente muita gente usando.

Então, quando chegamos em 2018, nas eleições no Brasil, o que aconteceu foi que tivemos alguns relatos de envio em massa de mensagens no WhatsApp violando a lei eleitoral e 2018 foi o ano em que Bolsonaro foi eleito, e foi uma eleição fortemente caracterizada pela disseminação de desinformação e ataques em um contexto realmente polarizado.

Esse era o cenário, e havia uma grande preocupação de que o principal canal de desinformação, de polarização, eram os aplicativos de mensagens, especialmente o

WhatsApp. Então, quando chegamos em 2020, após muitos problemas relacionados a essa informação e discussões sobre fake news, etc., e então estamos na pandemia, surge o projeto de lei 2630, proposto no Congresso sob o nome de Lei das Fake News.

E os primeiros rascunhos eram realmente preocupantes. Houve muita pressão da sociedade civil. E então, no meio de 2020, um dos primeiros rascunhos foi aprovado no CNA. Naquela época, o rascunho tratava principalmente de transparência e algumas questões processuais, mas havia um ponto realmente controverso sobre rastreabilidade.

A regra basicamente dizia que toda mensagem que fosse, não me lembro exatamente dos detalhes, mas era algo como toda mensagem que fosse encaminhada para mais de cinco grupos e alcançasse mais de 1.000 pessoas em um certo período de tempo. A plataforma precisaria manter os metadados dessa ação de encaminhamento.

Então, a ideia por trás disso era que, se você pudesse identificar uma mensagem violadora, seria capaz, através desses metadados, de voltar à primeira pessoa que a enviou. Quais eram os objetivos? O principal objetivo era identificar de onde essa informação estava vindo. E, mas quais eram os problemas com isso?

Essa regra de rastreabilidade é que, antes de tudo, as plataformas, os aplicativos não seriam capazes de identificar, uma vez que uma mensagem é enviada, se ela se tornará viral ou não. Então, na prática, eles precisariam manter os metadados de cada mensagem até que esse período de tempo fosse alcançado.

Então, para garantir que, se essa mensagem se tornasse viral, eles teriam os metadados e isso era um mandato para a retenção massiva de dados, e havia a possibilidade de acessar esses dados em procedimentos criminais. Não havia muitos requisitos para esse acesso, então era bastante vago como você poderia acessar esses dados.

E, na prática, você tinha muitos riscos, mas a regra em si não era realmente eficaz para seu objetivo, porque desconsiderava completamente o fato de que às vezes as pessoas simplesmente baixam o conteúdo. Às vezes, o conteúdo viaja por plataformas. Então, talvez o conteúdo estivesse no Telegram e alguém copiou e colou lá.

Então você realmente não conseguia acessar quem foi a primeira pessoa. A pessoa que enviou e isso criava o risco de criminalizar o usuário no final das contas. E havia um grande desafio dentro dessa regra, pois a sociedade civil em si estava bastante dividida, não havia unanimidade na oposição à regra e ao projeto de lei em si.

E naquela época, havia muita pressão de um grupo, uma coalizão de organizações de direitos digitais da qual fazemos parte, para agir em conjunto contra essas regras problemáticas dentro do projeto de lei. E nós, junto com muitas organizações que

fazem parte dessa coalizão de direitos digitais, trabalhamos produzindo tanto conhecimento quanto análises políticas e tentando dialogar com o relator do projeto de lei.

E isso foi algo realmente importante na época, porque o relator era alguém muito aberto ao diálogo com a sociedade civil. E nós havíamos produzido, em 2020, 2021, uma análise de políticas sobre as questões envolvidas nesse tipo de regra. E, no final das contas, houve muitas discussões de vai e vem com esse projeto de lei, e ele acabou não sendo aprovado, principalmente não por causa das questões de privacidade em si, mas principalmente por causa das tensões políticas dentro do Congresso.

E então, em 2023, ele voltou como um projeto de lei de regulação de plataformas. Então, o mesmo projeto, o texto foi completamente reformulado e veio como um projeto de regulação de plataformas que era mais GSA e essa provisão sobre rastreabilidade foi retirada. O projeto, mas novamente, o projeto não foi aprovado mais uma vez, também por questões políticas.

E agora estamos em um cenário em que provavelmente teremos o Supremo Tribunal decidindo sobre a constitucionalidade da regra de responsabilidade dos intermediários no Brasil. E isso mudará um pouco como a responsabilidade é tratada no Brasil e tentará adicionar alguns pontos para a regulamentação das plataformas. Então, este é o nosso cenário atual.

Obrigado.

Maria Paz Canales - Global Partners Digital: Muito obrigado, Heloisa. E acho que este é um momento perfeito de transição, talvez para um diálogo mais prático na próxima seção desta conversa, pensando no panorama geral fornecido por esses três diferentes exemplos de engajamento ao lidar com as ameaças à criptografia que ocorrem no contexto da regulamentação de plataformas.

Mas também pensando em como esse espaço proporcionado pelo trabalho conjunto na Global Encryption Coalition e a oportunidade de expandir a comunidade também neste evento de hoje, em torno do Dia Global da Criptografia, pode ser útil para continuar essa troca de táticas para engajamento nacional e envolvimento.

Obrigado. Estratégias para defender a criptografia e quero fazer algumas perguntas adicionais aos palestrantes nesta rodada, nesta seção, mas também incentivo o público a compartilhar seus comentários, suas perguntas, suas reações, mas realmente com essa abordagem mais estratégica em mente para que possamos aproveitar ao máximo o resultado desta sessão em termos de aprendizado.

E começando com o Mark primeiro. Você já começou a compartilhar um pouco sobre como, à medida que o Online Safety Act passa para a implementação e aplicação, há

toda essa expectativa e possível tensão em como as autoridades, e particularmente a Ofcom, interpretarão a lei e como interpretamos suas próprias responsabilidades chave fornecidas na lei. Quais são as principais mensagens que você teria para os formuladores de políticas que estão projetando ou implementando a regulamentação de segurança online, considerando essa tensão que você já começou a destacar no blog anterior? Talvez você queira expandir um pouco mais, mas também pensando nas intervenções que vieram depois de você, de outros colegas em outras regiões. Quais outras coisas você considera que poderiam ser úteis em termos de táticas e pontos focais de atenção ao lidar com essa questão da definição das responsabilidades das autoridades e as coisas que podem ser feitas durante o período de implementação que você já está começando a experimentar por si mesmo na implementação do Online Safety Act?

Obrigado, Mark.

Mark Johnson - Big Brother Watch: Sim, então, em termos das próximas fases da implementação da Lei de Segurança Online, na verdade tivemos uma comunicação muito boa com a Ofcom, o regulador independente, que tem sido bastante eficaz, eu diria, em falar com a sociedade civil e ouvir as preocupações. Acho que quando o projeto de lei de segurança online, antes de se tornar uma lei, estava passando pelo Parlamento.

Os debates em torno disso não foram aprofundados porque havia quase um consenso bipartidário de que precisávamos de algum tipo de legislação. Discordamos do modelo do Ato de Segurança Online por causa de todas as diferentes considerações de direitos, seja a liberdade de expressão, a privacidade ou outras ramificações da legislação.

Mas houve bastante apoio em ambas as Casas do Parlamento. Então, o debate nunca foi tão completo quanto deveria ter sido no Parlamento. E há algumas lições que podemos aprender com essa experiência e como podemos ser melhores como defensores e tentar promover mais debate. Mas eu acho que a Ofcom adotou uma abordagem após a aprovação da legislação, que é saber que levantamos preocupações durante todo o processo, mesmo que o debate não tenha sido tão completo e minucioso quanto deveria ter sido no Parlamento.

E eles têm ouvido e nos consultado, o que acho muito positivo. Além disso, eles adotaram uma abordagem cautelosa porque sabem que algumas das mudanças que as leis trarão serão bastante radicais e realmente reformularão como nosso relacionamento com as plataformas de mídia social ou serviços de mensagens poderá funcionar no futuro.

Então, eles têm se envolvido, eles têm engajado nosso. O plano da nossa organização, do ponto de vista organizacional, é continuar a monitorar como o processo funciona tão atentamente quanto possível e continuar a nos envolver. A Ofcom realizou algumas consultas abertas. Nós nos envolvemos no que poderíamos fazer coletivamente.

Descobri que ter vozes externas como parte do debate é extremamente útil porque, quando estávamos nos envolvendo com o governo e quando estávamos nos envolvendo com políticos, até mesmo políticos da oposição, porque a oposição no Partido Trabalhista, obviamente agora eles estão no governo, mas tudo isso aconteceu quando os Conservadores estavam no governo do Reino Unido, a oposição não era muito forte em direitos digitais, o Partido Trabalhista não era forte em direitos digitais, e a dificuldade, o desafio que tivemos foi que, com essa legislação, todos os diferentes problemas estavam diante de nós, fosse relacionado à liberdade de expressão, fosse relacionado à verificação de idade, implicações de privacidade, fosse relacionado à criptografia.

E assim, estávamos muito sobrecarregados. E havia também o desafio de que ambos os partidos queriam que algo acontecesse nesse espaço. Então, era muito difícil. E muitas vezes abordávamos os mesmos políticos repetidamente, e eles diziam: Ah, é o Big Brother Watch de novo. Eles sempre fazem os mesmos argumentos.

Mas se tivéssemos vozes externas, e conseguimos isso mais para o final, conseguimos trazer mais vozes externas para a sala. Isso cria um quadro mais amplo. Dá mais cor aos argumentos, porque podemos dizer que isso violará nossos direitos de privacidade e que terá um impacto sobre jornalistas ou defensores dos direitos humanos em outras jurisdições ao redor do mundo também.

Não realmente, seriam os mesmos argumentos que estamos fazendo, enquanto que se pudéssemos trazer outras vozes de outras jurisdições, de outros contextos, tivemos uma mesa redonda com outra organização de direitos onde tivemos a Anistia presente. Tivemos uma organização LGBT, vários grupos e organizações diferentes que representavam pessoas para falar sobre jornalistas ou defensores dos direitos humanos em diferentes partes do mundo.

Ter outras vozes na sala foi realmente útil, então, embora o resultado da legislação não tenha sido tão positivo quanto gostaríamos, o que é útil é que podemos olhar para trás com reflexão e dizer: isso é o que poderíamos ter feito mais no futuro. Isso é o que outras pessoas podem fazer no futuro se enfrentarem ameaças semelhantes.

Obviamente, como eu disse, a boa notícia é que a Ofcom não usou esses poderes e está sendo muito cautelosa. Então, não é uma história terrível, mas certamente há muito a ser aprendido com esse tipo de experiência legislativa, que foi definitivamente menos do que o desejado.

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

Acho que também não devemos ser tão duros conosco. Acho que, no final, o resultado final talvez não tenha sido o que você desejava, mas definitivamente poderia ser pior. Você não estava conduzindo todos esses esforços. Então, acho que você e outros que trabalham nessa área merecem crédito por isso.

Possivelmente, também a restrição na fase de implementação que você está vendo é resultado do fato de que a autoridade está ciente de como isso cria tensão e críticas durante a discussão do projeto de lei. Então, acho que devemos considerar também esse lado positivo no resultado. E passando para Boye, de volta para Boye novamente, acho que você já mencionou em sua intervenção anterior, esse conceito que Mark nos trouxe em termos de expandir a participação, não apenas dos suspeitos habituais, mas de grupos adicionais da sociedade civil entrando. Estou curioso se você pode falar mais sobre isso e espero que você entenda um pouco mais, Boye, em termos das coisas que você viu, por exemplo, como o contexto vindo de outras jurisdições e experiências anteriores tem sido útil ou não na discussão que você está tendo na Nigéria sobre a Internet.

E o que pode ser aprendido com a experiência dos defensores na Nigéria além desse elemento que você já mencionou sobre a ampliação da participação, que também tem semelhança com o que o Mark estava trazendo. Então, a palavra é sua, Boye.

Adeboye Adegoke - Paradigm Initiative: Muito obrigado, Maria. É interessante porque eu nem acho que estaríamos tendo essa conversa na Nigéria se o Ato de Segurança Online do Reino Unido não existisse.

Não porque a contemplação não existisse ou não estivesse sempre presente, mas também pela reputação de usar legislações que buscam abordar armas, seja nos espaços digitais ou nos espaços offline, como uma ferramenta para suprimir os espaços cívicos. Houve uma resistência muito significativa da sociedade civil ou até mesmo dos cidadãos contra o governo sempre que tenta introduzir qualquer legislação dessa natureza.

Então, o governo precisa apontar exemplos de países que normalmente seriam considerados bons exemplos para que o governo nigeriano possa dizer confortavelmente que isso é o que está acontecendo em outras partes do mundo. E isso também está acontecendo em lugares que você chamaria de sociedade justa ou democrática.

Então, isso dá uma espécie de validação adicional para até mesmo considerar fazer isso em primeiro lugar. Isso mostra que é de uma influência muito grande olhar para o que aconteceu na Austrália e no Reino Unido. Influenciou a decisão do governo de ser ousado o suficiente para se manifestar sem enfrentar muita resistência dos cidadãos, porque o déficit de confiança é muito baixo por aqui entre o governo e o povo.

E assim, toda vez que o governo contempla certos tipos de legislação, os cidadãos tendem a ver do ponto de vista negativo e tudo mais. Mas então, quando o governo consegue apontar exemplos do que está acontecendo no Reino Unido e na Austrália, que uma pessoa comum por aqui considera uma sociedade sã, se está acontecendo nessas jurisdições, por que não podemos ter essa conversa aqui?

Então, esse é o grau de influência na decisão de seguir esse caminho na Nigéria. No entanto, além disso, também influencia até mesmo o teste, o conteúdo da legislação proposta. Porque o que geralmente acontece é que os países que lançam algumas dessas legislações primeiro se tornam um modelo para os outros usarem.

Enquanto falamos, você pode, se olhar bem, até mesmo no documento oficial, foram feitas referências ao Ato de Segurança Online do Reino Unido. Também foram feitas referências à versão australiana, porque isso serve como um modelo que estamos usando. E estamos tentando contextualizar tudo o que vemos nesses modelos para a nossa realidade como nigerianos e africanos.

Nós, nós estamos muito cientes e conscientes do impacto ou de quanto o que acontece em outros lugares afeta o que acontece em nossa parte do mundo. E, pode até te interessar, eu até argumentaria que até processos globais, como os frameworks da ONU.

Como o quadro da GDC ou da UNESCO, por exemplo, ou a regulamentação de plataformas, eles não têm tanto impacto quanto os quadros nacionais de certos países. Em muitos países africanos, incluindo a Nigéria, essas leis nacionais que foram promulgadas, seja no Reino Unido, na UE, nos EUA ou em qualquer outro lugar, têm importância.

Influenciar a forma da abordagem. E, de fato, deixe-me também contar uma narrativa muito interessante na Nigéria quando introduzimos o projeto de lei Digitalista e Liberdade. E quando levamos o projeto ao Parlamento, uma das coisas que nos perguntaram foi se o parlamento gostaria de ver o armazém.

Isso foi feito, eles provavelmente adorariam até mesmo fazer um estudo de campo para ver o que está acontecendo nessa tradição. E na época em que redigimos o projeto de lei sobre liberdade digital, não havia nenhum país que estivesse tendo uma conversa semelhante. A coisa mais próxima disso na época era o Marco Civil no Brasil, o que então cria uma conversa sobre como nossos governos africanos abordam a legislação, especialmente a regulamentação e legislação digital.

Essa é uma suposição de que você tem que esperar pelos irmãos mais velhos para mostrar a direção antes de tomar uma decisão. Existe essa relutância em assumir um papel de liderança quando se trata de definir a direção para a regulamentação de plataformas digitais ou tecnologia em geral. Obrigado.

Maria Paz Canales - Global Partners Digital: Obrigado, Boye. Sim, definitivamente, isso é um desafio. Acho que todos podem se relacionar, especialmente nos países da maioria global, ao olhar para bons e maus modelos e continuar nessa linha. O Brasil tem sido um líder em muitas coisas relacionadas ao digital, como você acabou de mencionar, o Marco Civil.

Por isso é tão interessante ter você aqui, Heloisa, falando sobre a experiência. Quais são suas conclusões em termos de aprendizados sobre as armadilhas e oportunidades de regular plataformas online, particularmente ligadas à discussão sobre criptografia? E talvez eu possa fazer uma provocação para uma rodada final de comentários um pouco mais tarde para cada um de vocês como painelistas, então não só para Heloisa, mas para os três em suas considerações finais, eu gostaria que vocês abordassem.

Como seria uma abordagem amigável à criptografia no contexto da regulamentação de plataformas online, de acordo com a experiência que você já teve ao lidar com essa questão? Então, um pouco sobre as lições aprendidas no processo brasileiro. E se você quiser abordar essa questão mais ampla, também será ótimo e depois darei a palavra ao Mark e ao Voya para que eles também possam dar suas opiniões.

Para você, Heloisa, obrigado.

Heloisa Massaro - InternetLab: Obrigado, Maria Paz. Primeiro, eu diria que estamos, temos aprendido coisas desde 2020, então são quatro anos de aprendizado com esse acordo que vai e volta e assume muitas formas e abordagens diferentes. Mas, eu diria que, antes de tudo, uma coisa que tem sido realmente central para o nosso trabalho é oferecer diagnósticos melhores e mais detalhados.

E sei que isso tem um impacto limitado de alguma forma, mas é realmente importante trazer isso para a conversa. E por que estou dizendo isso? Estou dizendo isso porque, quando falamos sobre aplicativos de mensagens, por exemplo, começamos a desenvolver pesquisas quantitativas e qualitativas sobre como os aplicativos de mensagens são usados no Brasil para comunicação política.

E uma das nossas principais conclusões é como a mensagem, principalmente o WhatsApp, é uma plataforma realmente importante e conecta outras plataformas, mas não é a única protagonista. Muito obrigado. E também, conseguimos mostrar a variedade de usos que o WhatsApp tem, então quando você implementa uma medida que está buscando, não sei, resolver algum problema com essa informação que pode não ser uma questão específica em um aplicativo de mensagens, você está realmente impactando pequenos negócios.

Você está realmente impactando a vida diária das pessoas. E temos tentado trazer isso para o diálogo nos últimos anos. E isso é uma das coisas que achamos realmente importante e útil porque ajuda na análise de políticas e desenvolvemos abordagens melhores também. Outra coisa, e é que trabalhar em coalizão durante esse processo foi realmente importante.

As organizações de direitos digitais realmente trabalharam juntas durante o processo de regulamentação das plataformas, e isso foi realmente importante para criar, de certa forma, um espaço seguro para tentar resolver os desacordos entre nós antes de realmente defender uma outra abordagem.

E isso tem sido realmente importante para esse processo. Eu diria que muitas das vitórias que a sociedade civil teve durante esse processo foram através desse trabalho em coalizão. E também pudemos aproveitar o melhor de cada organização nisso. Teríamos organizações como o Internet Lab, que estariam produzindo pesquisas orientadas por fatos.

Você teria organizações mais atuantes no Congresso fazendo advocacia. Então, isso foi realmente importante. E uma última lição que eu diria dessas coisas positivas é o diálogo com as partes interessadas. E quando eu digo diálogo com as partes interessadas, é realmente ouvir e levar em consideração quais são as questões.

que as partes interessadas estão tentando resolver ou quais são os desafios que estão enfrentando. E isso se aplica tanto ao setor privado para realmente entender profundamente quais são os problemas que têm surgido, quanto ao trabalho com profissionais jurídicos, por exemplo. Então, realmente dialogar com promotores, com juízes e desenvolver esse tipo de.

capacidade de escuta que realmente ajuda nesse processo também. E quanto aos desafios, eu acrescentaria duas coisas e então encerraria. Eu diria que, apesar de todas essas vitórias que tivemos, não temos um projeto de lei aprovado. Então, no final das contas, você tem as disputas políticas que ofuscam tudo e meio que sobrepõem todo o trabalho que foi feito.

E o poder da mídia tradicional, especialmente no Brasil, não pode ser subestimado. A mídia tradicional foi realmente importante nesse processo de negociação e foi um dos elementos que bloqueou o projeto de lei. Estas são minhas considerações finais, e quanto à pergunta de Maria Paz sobre a regulamentação de plataformas amigáveis à criptografia, eu não tenho a resposta, mas acrescentaria uma coisa que acho muito importante considerar, que é, acho que precisamos, é realmente importante aprofundar a distinção entre redes sociais e aplicativos de mensagens privadas.

e entender que a regulamentação é diferente. E quando digo isso, também estou incluindo na conversa a questão de que, às vezes, os aplicativos de mensagens se tornam plataformas de mídia social e isso também precisa ser levado em consideração. Caso contrário, teremos regulamentações que visam atacar as funcionalidades de mídia social dos aplicativos de mensagens, prejudicando a privacidade e a liberdade de expressão.

É isso. Obrigado a todos.

Maria Paz Canales - Global Partners Digital: Obrigado, Heloisa. Então, acho que estamos, como de costume, ficando sem tempo com essa discussão muito interessante, mas estou interessado em ouvir sua opinião, Mark, e sua opinião, Boye, sobre essa questão, como seria uma boa abordagem para vocês. Além disso, estou ciente de que há uma pergunta adicional que foi postada no chat que talvez eu possa tentar estender

nosso tempo e perguntar a vocês, incluindo-a em sua resposta, que está relacionada a oportunidades mais específicas que vocês veem surgindo no pipeline em termos de trabalhar juntos em qualquer proposta legislativa ou relacionadas aos canais de implementação ou desafios na implementação de algumas das peças de legislação que vocês têm acompanhado ou quaisquer outras oportunidades que vocês veem no horizonte em que esse trabalho de coalizão global possa ser útil em termos de serviço para outros que estão começando a ter essa discussão.

Então, nas duas perguntas, talvez. Muito rapidamente, vocês podem distribuir o tempo como quiserem. Mark, e depois Boye, obrigado.

Mark Johnson - Big Brother Watch: Sim, vou tentar ser breve. Sim, sobre a questão de como poderia ser uma boa regulamentação, é uma pergunta muito difícil. Quando abordamos o projeto de lei de segurança online, fomos muito claros, não somos amigos, nem amigos próximos ou aliados das plataformas de mídia social, reconhecemos que havia muito a fazer para responsabilizar essas empresas, mas não achamos que a Lei de Segurança Online fosse necessariamente a abordagem correta.

Preferimos ver uma regulamentação que aborde os modelos de negócios das empresas, que acabe com o tipo de comércio massivo de dados e que considere a privacidade e a liberdade de expressão como centrais para qualquer tipo de regulamentação. Acho que, em termos dos desafios específicos que diferentes jurisdições tentam enfrentar quando pensam em contornar ou minar a criptografia de ponta a ponta, normalmente é algo relacionado a conteúdo de terrorismo, material de abuso sexual infantil e talvez desinformação, como ouvimos no caso do Brasil. O princípio deve permanecer que a criptografia de ponta a ponta não pode ser comprometida e que qualquer vigilância deve ser baseada em suspeita razoável e deve ser direcionada, e que toda a plataforma não deve ser comprometida.

Sei que muitas das principais empresas de mensagens privadas colaboram muito de perto com as autoridades em várias jurisdições ao redor do mundo. Poderiam haver maneiras de formalizar algumas dessas relações sem comprometer canais inteiros e a privacidade das pessoas que usam esses canais.

Então, essa é uma resposta um pouco vaga, mas acho que o mais importante, obviamente, como todos na escola sabem, é que deve haver certas linhas vermelhas que nunca devemos estar preparados para cruzar. Em termos de oportunidades de colaboração, é possível que o WhatsApp ou o Signal ou outros grandes serviços de mensagens criptografadas de ponta a ponta possam facilmente se dirigir aos reguladores do Reino Unido ou ao governo do Reino Unido e dizer que estão felizes em não cumprir com o que estão fazendo. E, de fato, ambas as grandes plataformas falaram sobre a possibilidade de sair do mercado ou certamente resistir às ameaças, à criptografia de ponta a ponta que foram colocadas pela legislação de segurança online.

Mas há mercados maiores ou jurisdições maiores para essas plataformas que estão considerando regulamentação no momento, como a consideração de controle de chat na UE, e onde você tem 400 milhões ou mais usuários, é muito mais difícil para essas plataformas individuais resistirem ou ameaçarem sair.

Então, a probabilidade de que eles tenham que mudar seu produto ou serviço nesse caso é significativamente maior em comparação com um exemplo menor como o Reino Unido. Então, obviamente, para colegas na UE, obviamente não estamos mais na UE, mas para colegas que estão na UE, se for útil e pudermos ajudar, e sei que as conversas ainda estão em andamento no momento, acho que estamos em uma posição bastante boa, mas se houver algo que possamos fazer e para colegas ao redor do mundo, então imagino que seria uma jurisdição bastante importante para se manifestar e ajudar.

Sim.

Maria Paz Canales - Global Partners Digital: Obrigado, Mark. Boye, qual é a sua opinião sobre essa abordagem amigável à criptografia na regulamentação das plataformas, como seria?

Adeboye Adegoke - Paradigm Initiative: Sim, eu acho que o debate para nós dentro do antigo debate sobre privacidade e segurança em termos de como uma regulamentação de plataforma amigável à criptografia pode ser.

Eu acho que o importante é reconhecer os problemas conflitantes em termos de como, por exemplo, comprometer a criptografia pode ter impactos significativos na privacidade, nos direitos de privacidade dos usuários, e também pode expor certos usuários a riscos. Mas também não devemos ignorar o aspecto de como a criptografia pode ser mal utilizada ou ser uma ferramenta para atores mal-intencionados.

Acho que o importante é a provisão de salvaguardas que também garantam que as autoridades não usem a criptografia como arma para alcançar fins políticos. Usar, enfraquecer a criptografia para atingir certos indivíduos, provavelmente por causa de suas crenças políticas, crenças religiosas ou estilo de vida, ou quaisquer outras características distintivas que possuam.

Acredito que somos guiados pelos Instrumentos Nacionais de Direitos Humanos em termos de como abordamos a limitação de direitos, como o direito humano de se comunicar e ter comunicações criptografadas. Acho que limitar esses direitos deve seguir diretrizes muito claras. O Procedimento dos 3 Testes, por exemplo.

Eu não acredito que as autoridades devam ter um poder irrestrito para acessar comunicações criptografadas por meio de backdoors, por exemplo, o que, em termos práticos e na experiência real de muitas pessoas, é geralmente o caso, especialmente

em países onde há instituições fracas, e acho que isso será muito relacionável para a maioria dos países do sul global.

A falta de instituições fortes criou um sistema em que as autoridades, tipicamente, aproveitam essa fraqueza institucional para, às vezes, assediar empresas de mídia social ou empresas que fornecem serviços de comunicação, exigindo acesso, exigindo acesso por portas dos fundos à comunicação sem seguir procedimentos, sem seguir o estado de direito, sem qualquer legitimidade e tudo mais.

Então, acho que o equilíbrio, o que o equilíbrio parecerá para mim, é criar um sistema que respeite os procedimentos, que respeite o estado de direito, que acomode apenas preocupações legítimas, seja por agências de segurança ou autoridades, mas não um acesso irrestrito ou uma proibição geral de comunicação criptografada. Precisamos limitar o quanto de poder as forças de segurança têm, o quanto de poder as autoridades têm para acessar conversas e comunicações importantes.

Tem que ser casos excepcionais onde isso é necessário. Não tem que ser, não deve ser a norma. Não deve ser a norma. Basicamente, é isso que estou dizendo. E no nosso trabalho na Nigéria também, em relação à exploração online, nosso argumento tem sido em torno de criar fortes salvaguardas, proteção em termos dos princípios contidos nas leis internacionais de direitos humanos para orientar os esforços do governo nesse sentido.

Estou muito consciente do tempo, então vou encerrar por aqui.

Maria Paz Canales - Global Partners Digital: Muito obrigado, Boye, você me deu a chave perfeita para as considerações finais. Muito obrigado a todos vocês por suas perspectivas. Espero que isso possa ser útil em termos de pontos de ação para as pessoas que acompanharam a conversa de hoje.

E eu resumirei que alguns dos elementos-chave a serem considerados a partir da sua experiência são essa ideia de ampliar o grupo. E acho importante ter esse tipo de participação para ter uma comunidade mais ampla cuidando disso e entendendo as nuances para diferentes comunidades sobre as implicações de impactar negativamente o uso da criptografia, a ideia de trabalhar em coalizão para moldar essa discussão em um espaço mais seguro antes de entrar em outras batalhas com a autoridade, a diversidade de contextos e diferentes usos e diferentes atores aqui, não apenas pensando nas grandes empresas de tecnologia, mas também na diversidade de implementação desses diferentes aplicativos e o papel que desempenham na sociedade. O foco no desafio, voltando ao último ponto de Boye, sua observação final, desafios, e estou tentando focar nesses desafios e na abordagem do governo a partir de uma perspectiva de direitos humanos.

Com isso, agradeço muito a todos vocês e encerrarei esta sessão, convidando-os para a próxima nesta Conferência da Coalizão do Dia Global da Criptografia, que é muito interessante. Obrigado.