DEPARTAMENTO DE TAQUIGRAFIA, REVISÃO E REDAÇÃO

NÚCLEO DE REDAÇÃO FINAL EM COMISSÕES

TEXTO COM REDAÇÃO FINAL

Versão para registro histórico

Não passível de alteração

CPI - CRIMES CIBERNÉTICOS			
EVENTO: Audiência Pública	REUNIÃO Nº: 2595/15	DATA: 01/12/2015	
LOCAL: Plenário 14 das Comissões	INÍCIO: 15h06min	TÉRMINO: 18h20min	PÁGINAS: 69

DEPOENTE/CONVIDADO - QUALIFICAÇÃO

MARK KAHN - Vice-Coordenador Jurídico Geral do WhatsApp.
BRUNO MAGRANI - Diretor de Relações Institucionais do Facebook Serviços Online do Brasil.
ALEXANDER CASTRO - Diretor Regulatório do Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal — SINDITELEBRASIL.
LUIZ FERNANDO MONCAU - Professor do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas.
PABLO DE CAMARGO CERDEIRA - Professor da Fundação Getúlio Vargas.

SUMÁRIO

Debate sobre o aplicativo WhatsApp.

OBSERVAÇÕES

Houve intervenção fora do microfone. Inaudível.
Houve exibição de vídeo.
Houve exibição de imagens.
Há expressão ininteligível.
Houve exposição em inglês sem tradução simultânea.
Há orador não identificado em breve intervenção.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Boa tarde a todos!

Declaro aberta a 35ª reunião ordinária da Comissão Parlamentar de Inquérito que investiga a prática de crimes cibernéticos.

Encontra-se à disposição dos senhores membros a cópia da ata da 34ª reunião, realizada no dia 26 de novembro.

Pergunto se há necessidade de leitura da ata.

O SR. DEPUTADO ESPERIDIÃO AMIN - Sra. Presidente, peço a dispensa da leitura da ata.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Fica dispensada a leitura da ata, a pedido do Deputado Esperidião Amin.

Em discussão a ata*. (Pausa.)*

Não havendo quem queira discuti-la, coloco a ata em votação.

Os Srs. Deputados que a aprovam permaneçam como se encontram. *(Pausa.)*

A ata é aprovada.

Ordem do Dia.

Audiência pública.

A reunião de hoje prevê a realização de audiência pública com a presença de representantes das empresas Facebook e WhatsApp, do SINDITELEBRASIL e também de professores da Fundação Getúlio Vargas.

Esta audiência decorre da reunião que trouxe aqui à CPI os provedores de acesso às empresas de telefonia, na semana passada.

A reunião tem como base a aprovação do Requerimento nº 65, de 2015, de autoria do Sr. Deputado Delegado Éder Mauro, do Requerimento nº 111, de 2015, proposto pelo Deputado Sandro Alex, e do Requerimento nº 131, de 2015, apresentado pelo Deputado Paulo Henrique Lustosa.

Estão presentes — e desde logo convido para tomarem assentamento à Mesa — o Sr. Mark Kahn, Vice-Coordenador Jurídico Geral do WhatsApp, o Sr. Bruno Magrani, Diretor de Relações Institucionais do Facebook Serviços Online do Brasil, o Sr. Alexander Castro, Diretor Regulatório do Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal — SINDITELEBRASIL,

e o Sr. Luiz Moncau, Professor do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas.

O SR. DEPUTADO ESPERIDIÃO AMIN - Sra. Presidente, antes da oitiva aqui dos nossos convidados, eu queria fazer uma ponderação a V.Exa. sobre o relatório. V.Exa. já organizou a Mesa?

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Posso chamar o último convidado? Em seguida, passo a palavra a V.Exa.

O SR. DEPUTADO ESPERIDIÃO AMIN - Sim.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Gostaria também de convidar, para compor a Mesa, o Prof. Pablo de Camargo Cerdeira, da Fundação Getúlio Vargas.

Com a palavra o Deputado Esperidião Amin.

O SR. DEPUTADO ESPERIDIÃO AMIN - Eu pretendo, Sra. Presidente, fazer a leitura do relatório, com a ajuda dos nossos Relatores Setoriais. Eu inclusive abri um espaço, até porque a nossa Comissão Parlamentar de Inquérito inovou ao atribuir missões bastante amplas para os Relatores Adjuntos e Setoriais. Queria combinar com V.Exa. para fazer essa leitura depois da audiência.

Então, queria pedir ao Carlos Alberto que avisasse os Relatores Setoriais que é imperiosa a presença deles — eu vou dar por lido. Se houver a prorrogação do prazo por 15 dias, como eu quero crer que haverá, nós tomaremos outro encaminhamento. Caso contrário, para que nós tenhamos um relatório aprovado, na quinta-feira, dia 4, que é o prazo limite, nós temos que fazer a leitura hoje, abrir vista e marcar a votação para o dia 3. Caso haja alguma novidade em matéria de prorrogações para as CPIs como um todo, que é o que se discute, adotaremos outro procedimento. E, com a autorização de V.Exa. e dos membros da CPI, eu recolheria o relatório até para dar um prazo maior de vista. Pode ser?

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Sem dúvida.

O SR. DEPUTADO ESPERIDIÃO AMIN - Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Fica aceito aqui o pedido de V.Exa.

Quanto ao nosso pedido para o adiamento da CPI por 60 dias, ainda não houve resposta. Acredito que, na reunião de Líderes, deva sair essa decisão e até

mesmo o prazo de 15 dias, mas não sei se será para todas as CPIs em andamento na Casa. Estamos esperando que seja aceito o nosso pedido de 60 dias. Caso não seja, que pelo menos a Presidência e as Lideranças dos partidos aqui na Câmara deem um prazo de pelo menos mais 15 dias para se concluírem todos os relatórios.

Cada convidado disporá de 20 minutos para apresentação. Informo que o primeiro orador falará na língua inglesa, havendo equipamento de tradução simultânea para todos os presentes.

Com a palavra o Sr. Mark Khan, Vice-Coordenador Jurídico Geral do WhatsApp

O SR. MARK KAHN - *(Exposição em inglês.)*

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - O próximo orador é o Sr. Bruno Magrani, que falará em nome do Facebook Serviços Online do Brasil.

O SR. BRUNO MAGRANI - Obrigado, Presidente Mariana pela oportunidade de estar aqui mais uma vez.

Estou aqui representando o Facebook Serviços Online do Brasil. Queria, mais uma vez, agradecer a oportunidade de estar aqui e poder esclarecer um pouco melhor sobre o tema de hoje, que é criptografia de plataformas digitais.

Como eu disse da última vez em que fui convidado para participar desta Comissão, o Facebook e o WhatsApp são empresas diferentes. Como não posso falar em nome do WhatsApp, no momento em que esta Comissão expressou interesse em ouvi-lo mais, eu repassei essa mensagem ao Mark, e ele, voluntariamente, decidiu aparecer aqui para trazer mais informações sobre a operação desse serviço.

O foco da minha fala hoje é muito sobre o uso de criptografia, em geral, pela indústria e pelo Facebook.

No Facebook, nós tratamos da segurança dos nossos usuários com muita seriedade. Quando as pessoas usam o Facebook, elas têm a expectativa de que estarão efetivamente seguras. Então, com o intuito de honrar continuamente a confiança dos mais de um 1,5 bilhão de pessoas que escolhem utilizar os nossos serviços a cada mês, o Facebook emprega algumas das tecnologias mais avançadas que existem no mercado.

Há um amplo consenso entre especialistas em segurança, acadêmicos e desenvolvedores de que o uso de uma criptografia robusta é um componente fundamental da segurança *on-line* e um recurso crítico para manter a segurança das pessoas e de suas informações. Ao utilizar a criptografia, empresas de tecnologia estão ajudando a manter as informações dos cidadãos brasileiros a salvo de ataques de criminosos *on-line*. Nós entendemos que prevenir a ocorrência desses crimes é uma das principais preocupações desta Comissão Parlamentar de Inquérito, assim como acreditamos que podemos ajudar nos trabalhos desta Comissão, exatamente empregando criptografia e, mais do que isso, também compartilhando um pouco da nossa experiência sobre o uso de criptografia pela indústria.

Então, deixem-me começar falando um pouco mais sobre criptografia. Seguindo a crescente demanda dos usuários por segurança e a sofisticação dos ataques cibernéticos hoje em dia, a indústria de tecnologia e outras indústrias também têm utilizado cada vez mais a criptografia como forma de proteger as pessoas. O principal objetivo da criptografia é proteger a confidencialidade dos dados digitais armazenados em sistemas de computadores ou transmitidos através da Internet para outros computadores. Em poucas palavras, é uma forma de garantir que dados enviados sejam decifrados ou possam ser lidos apenas pelos seus reais destinatários.

Durante a nossa navegação diária na Internet, a criptografia atua para proteger a segurança e a privacidade das nossas comunicações, muitas vezes sem mesmo percebermos que ela está presente. Todas as vezes que compramos algo com cartão de crédito, seja numa loja física ou na *web*, ou mesmo quando sacamos dinheiro no caixa eletrônico, a criptografia, ainda que não seja visível, se aplica ou está presente naquela transação para conferir a confidencialidade e a segurança necessárias para torná-la possível.

As técnicas de criptografia têm sido utilizadas para proteger as pessoas há bastante tempo. O Mark trouxe até alguns exemplos aqui, e vou retomar um pouco. O setor bancário, por exemplo, usa criptografia para garantir a segurança de transações monetárias, incluindo a segurança de cartões de crédito, senhas de computador e comércio eletrônico. Então, toda vez que alguém entra no *site* do

banco *on-line*, pode-se não perceber, mas há criptografia ali protegendo a confidencialidade daquelas informações. Então, quando vemos o "s" no nosso navegador, naquele cadeado ou naquele início do endereço *https*, significa que estamos em uma conexão segura.

Então, ao visitar a página de acesso a um banco *on-line*, o navegador do cliente estabelece uma sessão segura com o servidor do banco. Antes, mais uma vez, de fazer qualquer compra *on-line* ou de acessar um *site*, para você verificar se aquele é realmente o *site* ou saber se a sua informação está segura e protegida, é importante estar atento a esse mecanismo: ou cadeado ou o sinal do *https*.

As tecnologias de criptografia, então, são utilizadas majoritariamente para proteger usuários legítimos de criminosos cibernéticos, também conhecidos como *crackers*. Qualquer tentativa de enfraquecer essa tecnologia vai acabar reduzindo também a segurança das pessoas. Nós temos aqui também a participação de dois professores da FGV, que podem, talvez, tratar um pouco mais desse ponto. Mas a questão principal é que, se você coloca qualquer forma de acesso àquela tecnologia que não seja a implementação exata da criptografia, você pode acabar enfraquecendo a criptografia para a indústria como um todo.

Bem, como é que o Facebook usa essa criptografia? Primeiro, o Facebook usa criptografia em toda a sua infraestrutura e na oferta dos serviços. Então, mais uma vez, aquele símbolo *https* aparece também quando você acessa o Facebook. Se você for lá em *facebook.com*, você vai ver aquilo e vai conseguir verificar a autenticidade do *site* do Facebook. Por que isso é importante? Porque isso impede que você acabe se deparando com outro *site* que tente se passar pelo *site* do Facebook e só queira, na verdade, capturar as suas informações de *login* e senha. Então, é sempre importante estar atento àquilo, para ter certeza de que você está efetivamente utilizando o Facebook.

Além disso, o Facebook permite também que os usuários incluam as suas chaves criptográficas públicas ou PGP em seu perfil no Facebook. Eu acredito que o Prof. Pablo vai tratar um pouco melhor dessa tecnologia depois. Nessa tecnologia, basicamente você tem uma chave, uma chave pública. E se a pessoa tem a sua chave pública, ela pode criptografar ou codificar aquela mensagem para enviar diretamente para você. Então, o Facebook permite que você coloque no seu perfil

anunciando, digamos assim, a sua chave pública para quem quiser mandar mensagens para você.

Mais uma vez, só reforçando o ponto da criptografia pela indústria, ele tem efetivamente como objetivo proteger os dados das pessoas e evitar atividades criminosas *on-line*. Nós acreditamos que, ao empregar criptografia, as empresas ajudam a promover o nível de segurança que esta Comissão busca.

É importante também enfatizar a importância econômica da criptografia tanto para empresas brasileiras quanto globais. O uso de tecnologias robustas de segurança, como a criptografia, serve como um diferencial competitivo decisivo para as empresas nacionais que oferecem serviços *on-line* e aplicativos móveis, não só no Brasil, mas no mundo inteiro.

Então, com a crescente necessidade de proteger os segredos comerciais, segredos industriais, do acesso por eventuais concorrentes, os departamentos de TI das empresas estão contando cada vez mais com a criptografia para proteger efetivamente os seus negócios. Isso significa que as empresas de tecnologia brasileiras e globais competem com base no nível de criptografia e de outros recursos de segurança que elas oferecem aos seus usuários finais. Em outros termos, os consumidores cada vez mais demandam produtos que forneçam a segurança que a tecnologia da criptografia proporciona.

O setor de tecnologia brasileira, em particular, tem um enorme potencial para contribuir para o crescimento do País. Um artigo recente publicado pela revista *on-line* especializada em tecnologia TechCrunch trouxe uma história bastante interessante sobre como *startups* brasileiras continuam a receber investimentos e a inovar, apesar das atuais incertezas econômicas. Se essas empresas forem proibidas de utilizar criptografia, a sua capacidade de inovar e de competir em escala global pode acabar sendo afetada de maneira significativa.

As *startups* brasileiras interessadas em aproveitar as oportunidades do mercado global proporcionado pela Internet precisam empregar uma criptografia robusta a fim de serem bem-sucedidas. Nós acreditamos que esta Comissão deve, sim, proteger o interesse das *startups* brasileiras. E acreditamos que uma das formas de se fazer isso é através do incentivo à utilização de criptografia.

As comunicações criptografadas também têm papel fundamental na proteção de direitos humanos, incluindo a liberdade de expressão e a privacidade. O Relator Especial da ONU sobre liberdade de expressão endossou explicitamente a disponibilidade irrestrita de tecnologias de criptografia robustas em um relatório recente que foi publicado em junho de 2015. Mais uma vez, isso reforça o ponto de que usuários comuns da Internet também enfrentam uma série de perigos *on-line.* E eles estariam expostos à atividade de criminosos e de outros agentes maliciosos na ausência de uma criptografia robusta.

Nós entendemos que um dos objetivos desta Comissão tem sido exatamente o de lutar contra atividades criminosas *on-line* e prevenir que elas comprometam o uso da Internet por todos os cidadãos. Quaisquer vulnerabilidades nessa linha impostas à tecnologia da criptografia invariavelmente podem ser exploradas por maus atores, colocando-se em risco a segurança dessas pessoas.

Deixem-me, agora, trazer um pouco do qual eu já falei na audiência anterior, mas acho que é bom reforçá-lo: a forma como o Facebook tem trabalhado com a Polícia e Ministério Público no âmbito das investigações criminais que ocorrem. O Facebook disponibiliza um portal *on-line* em que qualquer autoridade de investigação, seja a Polícia, seja o Ministério Público, de qualquer lugar do mundo, pode encaminhar diretamente ao Facebook quaisquer solicitações, quaisquer ordens judiciais que se refiram a acesso a dados. Então, nós temos um sistema e uma equipe que analisa esses dados e responde diretamente a essas autoridades, através desse portal.

Além disso, o Facebook trabalha com organizações e autoridades para impedir atividades ilegais na plataforma. Nessa linha, o Facebook já fez milhares de denúncias a organizações, como Nec Mac, que trabalham em conjunto com as autoridades policiais, para combater casos de exploração infantil. Desde 2011, o Facebook tem usado uma ferramenta chamada foto DNA, ou *DNA photo*, em inglês, para bloquear o *upload* no Facebook de imagens que tenham sido identificadas como relacionadas à exploração sexual infantil. Essa ferramenta examina cada foto que é enviada para o *site* para garantir que materiais ilícitos não possam ser distribuídos.

Se conteúdo dessa natureza for encontrado, a conta é imediatamente desativada, mas seus dados são preservados para ajudar a qualquer investigação subsequente e para ajudar à denúncia daquele conteúdo para todas as instâncias desse centro que eu mencionei.

A vantagem de o Facebook trabalhar com um centro como o Nec Mac está exatamente no fato de que, sendo uma organização internacional, ele tem a possibilidade de trabalhar com polícias e autoridades de investigação em diversos países do mundo. Muitas vezes, vemos que essas atividades ilícitas são cometidas por organizações transnacionais. E trabalhar com uma entidade que possa, por sua vez, interagir com essas diversas polícias proporciona ganhos de eficiência enormes.

Aqui no Brasil, o Facebook também tem trabalhado com entidades brasileiras, como, por exemplo, a SaferNet, que, no meu entendimento, já participou inclusive dos trabalhos desta CPI. Além das nossas políticas, o Facebook também desenvolve programas para promover a segurança e o bem-estar das pessoas que usam nossos serviços todos os dias. E, nessa linha, nós trabalhamos em inúmeras campanhas educacionais e de sensibilização voltadas para essas questões. Em 2011, por exemplo, representantes do Facebook vieram aqui ao Congresso brasileiro e, em conjunto com Deputado Sandro Alex, lançaram uma campanha pioneira contra o *bullying on-line*, através da página Chega de Bullying.

Essa iniciativa eventualmente evoluiu para se tornar um projeto internacional que hoje nós chamamos de Centro de Prevenção de Bullying ou Bullying Prevention Hub. Essa segunda fase da iniciativa contou com o apoio do Centro da Universidade de Yale para Inteligência Emocional. E nós temos trabalhado agora com a UNICEF, para expandir o projeto não só para outros lugares do Brasil, mas também para o resto da América Latina.

Além disso, o Facebook desenvolveu a Central de Segurança da Família, que oferece recursos para ajudar pessoas a aprender como manter a segurança da Internet e o que fazer caso se deparem com ameaças ou com conteúdos que elas julguem não serem seguros. Essa central também possui extenso conteúdo para a prevenção do *bullying*, incluindo dicas, ferramentas e um guia para todas as partes interessadas, sejam elas pais, educadores, adolescentes e até mesmo pessoas

acusadas de *bullying*. Ela também está ligada diretamente a um canal de denúncia, porque o Facebook sabe quão importante é dar essa informação às pessoas no momento em que elas estejam precisando dela, ou seja, quando elas vão denunciar eventualmente uma prática de *bullying* na plataforma.

Nós acreditamos que garantir a segurança de todos é uma responsabilidade compartilhada pela comunidade. Dessa maneira, todo mundo tem o direito de estar seguro, mas ao mesmo tempo também temos a responsabilidade de cuidar uns dos outros, tanto em comunidades *on-line* quanto *off-line*. Parte dessa responsabilidade compartilhada envolve encorajar as pessoas a pensar e ponderar antes de postar. Para promover isso, nós criamos inclusive um programa chamado Pense antes de Postar em parceria com a Childnet International para aumentar a conscientização das pessoas e mostrar como elas podem ser ainda mais cuidadosas com um conteúdo compartilhado no Facebook.

Com isso, eu já vou me encaminhando para o final da minha fala. Eu queria só agradecer, mais uma vez, a oportunidade de estar aqui na Comissão e dizer, mais uma vez, que o Facebook está efetivamente comprometido em garantir uma plataforma segura onde as pessoas se sintam à vontade para interagir e compartilhar conteúdos.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Concedo a palavra ao Sr. Alexander Castro, Diretor Regulatório do Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal — SINDITELEBRASIL.

O SR. ALEXANDER CASTRO - Eu gostaria de cumprimentar, primeiramente, a Deputada Mariana, Presidente da Comissão, também os demais Parlamentares. Senhoras e senhores, eu vou fazer uma pequena apresentação aqui e vou sair da frente de vocês, para que vocês possam enxergar.

(Segue-se exibição de imagens.)

Eu gostaria de iniciar fazendo uma pequena diferenciação entre o que é telecomunicações e o que é Internet. Como representante do Sindicato das Operadoras de Telecomunicações, nós representamos todas as principais operadoras do serviço de telefone fixo comutado, também do serviço móvel pessoal e do serviço de comunicação multimídia. Dois desses serviços dão suporte ao

acesso a Internet: o SMC — Serviço de Comunicação Multimídia e o SMP — Serviço Móvel Pessoal.

É importante que neste momento façamos uma pequena diferenciação. O que o Comitê Gestor da Internet — CGI estabelece no recente documento que enviou ao Ministério da Justiça sobre a regulamentação do Marco Civil da Internet? Ele colocou lá que as redes de telecomunicações, na verdade, servem como alternativa de suporte para o funcionamento da Internet. Apesar de estarem intimamente relacionadas, elas são atividades distintas. Então, as operadoras de telecomunicações são, na verdade, provedoras de acesso e de conexão dos usuários à Internet. Fornecem a infraestrutura para navegação na rede mundial.

Então, nós somos, na verdade, o transportador. Em cima das redes das operadoras, diversos serviços da Internet e diversas aplicações são ofertados. Podem ser serviços de vídeo, *streaming*, *e-commerce*, podem ser aplicações e serviços educacionais, serviços públicos de entretenimento, etc. Essas informações são transportadas por pacotes de dados, e fazemos esse transporte de forma quase transparente. Nós não trabalhamos, não tratamos esses pacotes, até por uma vedação do próprio Marco Civil da Internet, conforme eu vou mencionar aqui na frente.

Então, o que diz o Marco Civil da Internet sobre a monitoração dos pacotes? O § 3º do art. 9º, que trata da neutralidade de rede, diz claramente que é vedado às operadoras monitorar, filtrar ou analisar o conteúdo dos pacotes. Então, nós não podemos acessar a informação que o usuário está retirando da Internet ou está inserindo nela. Por uma questão de privacidade, não podemos ter acesso a esses dados.

O CGI também trata dessa questão de conexão à Internet e menciona que as operadoras podem fazer um gerenciamento rotineiro de suas redes, normais, que são necessários para otimizar a passagem do tráfego nas suas redes, evitar congestionamentos e garantir a segurança, a estabilidade das redes, porém elas não podem — isso seria uma discriminação, está no quadro de definição de discriminação — fazer redirecionamento, por exemplo, filtragens no pacote. Então, não podemos também, a nosso bel-prazer, pegar esses pacotes e redirecioná-los, salvo se houver uma ordem expressa judicial.

A Constituição Federal também estabelece, no art. 5º, que é inviolável o sigilo das correspondências, da comunicação telegráfica e também das comunicações telefônicas, seja uma comunicação telefônica de um serviço convencional de voz, serviço telefônico fixo comutado ou SMP, seja uma navegação na Internet. Para alguém que está falando com outra pessoa através do Skype, através do WhatsApp, através de qualquer outro aplicativo ou serviço, essa comunicação não pode ser monitorada, ela não pode ser "paralelada", ela não pode ser ouvida pelas operadoras. E isso cogitou em crime fazer, realizar a interceptação das comunicações telefônicas, sejam elas, novamente, um serviço convencional, seja através da Internet por meio de uma tecnologia, por exemplo, de voz.

Então, com relação a esses *slides* que eu já passei, podemos direcionar três conclusões bem rápidas. A primeira conclusão é que os provedores de acesso e conexão, entre eles as operadoras de telecomunicações, não podem manipular a informação do usuário que está inserido em cada pacote de dados. A questão da criptografia, por exemplo, como foi mencionado pelo Bruno e pelo Mark, deve ser implementada pelos provedores de conteúdo, pelos provedores de aplicação, de maneira geral. As operadoras de telecomunicação apenas transportam. Tal qual a recebemos, transportamos, como eu expliquei aqui, sem acessar, sem entrar no mérito do que estamos transportando.

Os provedores de acesso e conexão não podem monitorar, só podem monitorar os metadados, não podem monitorar a informação. No pacote de dados, existe uma série de *bits*, uma série de informações que são inseridas no pacote junto com a informação para controle, para controle do gerenciamento do tráfego. Esses metadados, esses *bits* adicionais, podemos monitorar; agora, a informação especificamente do usuário, não.

O SR. DEPUTADO SILAS FREIRE - Mas o tempo de ligação, sim?

O SR. ALEXANDER CASTRO - Sim, isso eu vou colocar mais à frente.

Os provedores de acesso e as operadoras também não podem monitorar, gravar ou interceptar as comunicações privadas. Como eu falei, as comunicações são privadas, sejam feitas por um aplicativo, como eu mencionei, baseado em voz, por exemplo. Essas comunicações também, apesar de serem feitas através da Internet, elas seguem o mesmo rigor porque a Constituição se aplica a todos,

independentemente da mídia e do serviço que está sendo prestado. Então, também estão garantidos o sigilo e a privacidade dos usuários no entendimento da monitoração, gravação ou interceptação dessas comunicações privadas.

Agora vou falar um pouquinho sobre a guarda dos registros no Marco Civil da Internet. O Comitê Gestor da Internet, no mesmo documento que enviou ao Ministério da Justiça apresentando suas recomendações com relação à regulamentação do Marco Civil, também faz algumas menções nesse documento com relação à guarda de registros. Basicamente, o que o CGI e o Marco Civil estabelecem é que a guarda e a disponibilização desses registros de conexão... Os registros de conexão são os registros do usuário que acessa a Internet, o momento em que ele acessou a Internet, o tempo em que ele ficou acessando a Internet e qual foi o número IP que ele utilizou para acessar a Internet. Esses são os dados do registro de conexão. O IP de destino não faz parte do registro de conexão. Ele faz parte do registro de aplicação, e as operadoras de serviços de comunicação estão proibidas de guardar informação do registro de aplicação, ou seja, da informação do IP de destino. Nós só guardamos o IP de origem, o início da navegação e o tempo que durou a navegação.

A disponibilização e a guarda desses registros, também dos dados pessoais que os usuários fornecem às operadoras na hora em que contratam um serviço, comunicações privadas, que eu já mencionei, essas informações devem atender à preservação da intimidade, da vida privada, da honra e da imagem.

Eu queria chamara atenção para as comunicações privadas porque, como eu mencionei, as operadoras não guardam comunicações privadas, não gravam. Dentro do ecossistema da Internet, se há algum provedor, algum agente que atua na Internet, provedor de aplicação, que guarde essas comunicações... Por exemplo, eu ouvi agora do nosso primeiro interlocutor que o WhatsApp, por exemplo, não guarda as comunicações. As operadoras, da mesma forma, não guardam também nenhum tipo de comunicação, nenhum registro de comunicação privada.

Também o CGI estabelece que, na provisão do serviço de conexão à Internet, apenas os administradores de sistemas autônomos ISP têm obrigação de guardar os registros de conexão. Isso se aplica às operadoras. Todas as operadoras de telecomunicações são sistemas autônomos, mas nem todas as empresas e

organizações que podem oferecer algum tipo de conexão à Internet e não são administradoras de sistemas autônomos não precisam guardar os registros de conexão. Essa é a posição oficial do CGI, enviada para o Ministério da Justiça. E o Marco Civil da Internet obriga a guarda dos registros de conexão pelo período de 1 ano.

Também o mesmo documento do CGI encaminhado ao Ministério da Justiça coloca o seguinte: o Marco Civil da Internet estabelece que os dados cadastrais podem ser disponibilizados independentemente de uma ordem judicial por uma autoridade administrativa competente. Quem é a autoridade administrativa competente? Existia sempre uma dúvida por parte das operadoras. Para quem elas poderiam ter que disponibilizar esse dado em função da lei do Marco Civil da Internet? E o CGI, Comitê Gestor da Internet, estabeleceu o que está nesse *slide*, ou seja, o acesso aos dados cadastrais, independentemente de ordem judicial, por autoridades somente deverá ocorrer nas hipóteses determinadas nas duas leis que estão mencionadas aqui, as leis que definem organização criminosa e lavagem de dinheiro.

Também gostaria de lembrar que na provisão de conexão onerosa ou gratuita, como mencionei, as operadoras não podem fazer a guarda dos registros de acesso, dos registros de acesso a aplicações. Fica por conta dos provedores de aplicação, que têm um prazo de 6 meses para isso.

Neste *slide* estamos apresentando alguns exemplos de ações que as operadoras fazem para colaborar com a segurança na Internet, com a elaboração de cartilhas, estabelecimento de *links* para *sites* de denúncias de crimes cibernéticos, campanhas de combate à pedofilia e também criação de processos internos permanentemente para combate a crimes.

Gostaríamos de deixar sempre registrado que nenhuma operadora fornece ou facilita informações que possam quebrar o sigilo de seus usuários. As operadoras possuem, aqui no Brasil, os maiores *datacenters* da América Latina. Nós investimos em proteção e em segurança dos dados. Os maiores *datacenters* da América Latina são de propriedade das operadoras de telecomunicação e estão localizados aqui no Brasil.

Os sistemas de operação e suporte para fazer qualquer tipo de ação, para fazer, por exemplo, um aprovisionamento de um cliente dentro da base de dados da operadora, qualquer sistema desses possui acessos restritos e protegidos e são rastreáveis. E o nosso histórico, ao longo dos últimos 17 ou 18 anos de privatização, atesta o padrão de comportamento das operadoras na garantia da inviolabilidade da intimidade, da vida privada e do sigilo das comunicações.

Faltam só mais dois *slides.*

No caso dos crimes cibernéticos, as operadoras de telecomunicações bloqueiam quando recebem essa determinação do ponto de vista da esfera judicial, bloqueiam os endereços IP e URL, fornecem os dados dos usuários e efetuam a interceptação telemática solicitada e autorizada pelo juiz.

Como última conclusão, então: os provedores de acesso à conexão — mais uma vez eu repito, são as operadoras de comunicações — não guardam registro de aplicação. Tomamos todos os cuidados para garantir a privacidade, a segurança dos dados e o registro dos usuários, repudiamos qualquer tipo de crime cibernético e colaboramos ativamente com as autoridades competentes.

Essa era a mensagem que eu queria passar nesse intervalo de tempo.

Eu agradeço à Presidente.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada.

Concedo a palavra ao Prof. Luiz Fernando Moncau, Professor do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas.

O SR. LUIZ FERNANDO MONCAU - Bom, em primeiro lugar, eu gostaria de dizer boa tarde a todos os presentes, aos Deputados e às Deputadas. Quero agradecer o convite para poder contribuir com um pouco do que nós pesquisamos lá no Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas — FGV Direito Rio.

Quero dizer que nós somos um centro que está trabalhando há um pouco mais de 12 anos com essas questões. Uma das questões que nós trabalhamos bastante ativamente foi justamente a do Marco Civil da Internet. Nós fizemos uma parceria com o Ministério da Justiça para ajudá-lo a realizar a primeira consulta pública de um anteprojeto de lei na Internet, a receber as contribuições, a digerir essas contribuições e preparar o texto. Este depois foi enviado à Câmara dos

Deputados, onde foi debatido, e depois no Senado Federal, e se tornou esta lei que hoje é bastante elogiada no mundo inteiro.

Não trouxe uma apresentação. Queria fazer considerações em três níveis: umas considerações de contexto, umas considerações de ordem técnica — reconheço que eu não seja a melhor pessoa para fazê-las, há pessoas mais qualificadas na mesa para isso — e algumas considerações de ordem jurídica.

Sobre contexto, há algumas coisas que eu acho que todos nós já sabemos, mas é importante nós repisarmos. Uma coisa bastante importante é que nós temos hoje uma dependência absoluta da infraestrutura de telecomunicações e da Internet. Se há 10 anos, 15 anos nós falávamos que a Internet, no futuro, seria como a eletricidade, e nós teríamos esta dependência desse tipo de infraestrutura, como nós temos da eletricidade, hoje em dia acho que não seja equivocado falar — pelo menos, para algumas regiões do País, onde o acesso é bastante universalizado, bastante disponível para grande parte da população — que o acesso é bastante importante.

O acesso é bastante importante em vários níveis: em termos econômicos, em termos de trabalho, em termos de eficiência. Vou trazer como único exemplo o que aconteceu quando nós tivemos uma pequena falha no serviço de governo eletrônico do eSocial. Quando nós tivemos alguns dias de indisponibilidade do serviço, gerou-se um caos que trouxe grande repercussão.

Essa infraestrutura toda é importante em vários níveis. É importante no nível econômico também. Nós temos estudos apontando sobre quanto um país pode crescer quando ele eleva em um ponto percentual a penetração da banda larga, quanto um país pode crescer em termos de emprego. Esse é um dado que eu achei aqui rapidamente: para cada ponto percentual de banda larga, há 0.2 ou 0.3 pontos percentuais em nível de emprego. Então, há alguns dados que mostram a importância de se ter esse sistema funcionando.

Agora, para esse sistema funcionar, nós precisamos que ele seja seguro e confiável. E, quando nós falamos de segurança e confiabilidade, não é só a estabilidade que nós temos, por exemplo, com a rede elétrica. Com esta, temos a certeza de que nós vamos apertar o botão, e a luz vai acender, o que permite que todos nós trabalhemos todos os dias, com a certeza de que vamos ter energia para

trabalhar. Significa também que nós vamos conseguir nos comunicar com o mínimo de segurança nessas nossas comunicações e com a certeza de que não vai haver interferências indevidas nessas comunicações.

Se nós olharmos de novo 10 ou 15 anos atrás, nós tínhamos um olhar para a Internet bastante utopista. Parecia que a Internet viria para resolver 90% dos problemas do mundo. Ela iria aproximar relação entre representantes e representados, ela iria democratizar as comunicações, ela iria permitir que os artistas falassem diretamente para o seu público, ela iria permitir que os governos prestassem serviços diretamente aos cidadãos. E muitas dessas coisas não se concretizaram ainda e, talvez, nem venham a se concretizar.

Nós temos um cenário um pouco distópico se desenhando no horizonte. E alguns fatos são emblemáticos deste cenário distópico, como cenários de espionagem em larga escala massiva dos cidadãos por governos estrangeiros — não só de um país, mas de vários países. Nós temos relato desse tipo de ação não só de países autoritários, mas também de países democráticos. Nós temos riscos à segurança e à confiabilidade dessas comunicações não só por atitudes de governos, mas também por atitudes de outras pessoas mal-intencionadas, como *crackers* — como já foi citado na fala de outro palestrante aqui.

Então, todo esse cenário hoje — e tentando não ficar nem no lado utopista nem no lado distópico da moeda — aponta talvez para um caminho em que nós vemos alguns direitos nossos que são fundamentais para uma democracia se erodindo bastante rapidamente. Toda a tecnologia que nos dá uma liberdade permite alguma forma de controle também. Se eu acesso um livro, eu deixo um rastro de que eu li aquele livro. Se eu acesso uma determinada informação, eu deixo o rastro de que eu acessei aquela informação. Se eu me comunico com alguém, eu deixo rastros de que aqueles são os meus contatos pessoais.

Então, tudo isso é importante quando, especialmente numa Casa Legislativa, nós vamos pensar qual é o regime legal que nós queremos adotar e quais são os poderes que nós queremos conferir aos nossos agentes de Estado, para investigar os cidadãos ou para investigar os crimes em geral. Nós temos que pensar se esses poderes vão ser excepcionais ou se esses poderes vão ser mais generalizados. Essas são algumas considerações de contexto.

Passando para considerações de ordem técnica, quando eu recebi o convite para falar sobre criptografia, este não é um tema no qual eu seja especializado. Mas a primeira coisa que eu pensei foi: bom, está bem. Se nós queremos ter um regime que permita a investigação de crimes, sempre eu sou daquela opinião de que nós temos que ter o caminho do meio, o moderado. Nós temos que ter uma exceção específica que permita que as autoridades acessem aquelas informações quando existir um crime, uma investigação.

O problema é que, quando se investigam os padrões técnicos que permitem a criptografia e que permitem a privacidade e leem-se os artigos acadêmicos que tratam a respeito, descobre-se que isso não é possível. Isso não é possível porque, se são criadas algumas exceções, cria-se um cenário de insegurança e de possíveis violações à privacidade, que é muito pior do que o cenário atual que nós temos.

Então, para dar um exemplo específico, nós falamos um pouquinho aqui, outros palestrantes falaram da questão das chaves criptográficas. Há um esquema de chaves criptográficas hoje em que cada transação é feita com uma chave criptográfica, que é imediatamente jogada fora. Fazendo uma analogia grosseira, que eu sei que não é a mais precisa, imaginem aquele *token* do banco, que nós temos. Para se autenticar aquela transação, precisa-se usar aquela chavezinha que aparece e que precisa ser digitada naquele momento. Ela funciona naquele momento; no próximo, ela já não funciona mais.

Então, nesta analogia grosseira que eu estou fazendo, o que isso quer dizer? Se alguém quiser interceptar a sua comunicação, precisa interceptá-la o tempo todo. Ele precisa pegar aquela chave uma vez para pegar aquele momento e violar a sua privacidade. Ele precisa interceptar aquela chave, novamente, para violar de novo, e assim sucessivamente. Essa é uma garantia das pessoas, é uma garantia de quem faz transações bancárias. É uma garantia minha, cidadão, que me comunico com outra pessoa, especialmente, quando eu faço isso legalmente.

Se eu criar uma exceção, que permita que alguém esteja vendo aquelas chaves o tempo todo, eu crio um ponto de vulnerabilidade extremamente importante. Aqueles que estão querendo, maliciosamente, ter acesso às minhas comunicações ou às minhas transações bancárias vão saber: existe um ponto aqui que guarda aquelas chaves.

Se eu atacar aquelas chaves, eu vou ter acesso, de uma vez só, a todas as comunicações do Luiz Moncau, ou a todas as transações bancárias, ou acesso à conta bancária de uma vez só. Se eu elimino esta forma rotativa das chaves, eu elimino uma segurança importante e, se eu dou acesso a alguém, a uma autoridade, eu crio uma forma importante de violação e de insegurança da privacidade dos cidadãos. Isso entrando um pouquinho na área técnica.

Se nós formos pensar na área técnica ainda, podemos pensar: está bem, mas ainda assim isso vale a pena. Então, quem é que faria a guarda desses dados? E aí nós teríamos que imaginar os enormes riscos e custos que, eventualmente, empresas teriam que ter para fazer a segurança dessas informações, e, eventualmente, quando o vazamento dessas informações ocorresse, o custo enorme que isso traria, porque obviamente, num Estado de Direito maduro, aqueles que tenham essas comunicações vazadas deveriam ser indenizados por isso, especialmente quando não dão causa a esse tipo de problema.

Então, a depender do tipo de solução que apontamos para esse problema, nós podemos elevar muito os custos e os riscos à inovação, especialmente nessa camada de aplicativos, a camada que essencialmente está sob disputa de concorrência mais ferrenha, já que ela exige as menores barreiras de entrada para inovação.

Por fim, uma coisa importante que temos de analisar é a privacidade por meio de flexibilização à criptografia. Nós podemos criar um cenário em que, ao invés de combater crimes, nós estamos dando margem para mais crimes, na medida em que permitimos mais violações à privacidade dos cidadãos.

Sabemos que as pessoas compartilham, por exemplo, fotos íntimas no celular. Numa comunicação criptografada, se nenhuma das partes fizer vazar essas fotos, elas não vão circular. Numa comunicação com uma criptografia violável, estamos certamente muito mais vulneráveis a que aquelas partes que estão se comunicando dentro de um acordo tenham a sua comunicação privada vazada para um grande número de pessoas.

Não precisamos pensar nesse cenário, que talvez seja um exemplo um pouco ruim, mas podemos pensar em comunicações privadas de sigilos comerciais.

Tivemos um exemplo recente aqui, inclusive em caso de espionagem em massa, de empresas brasileiras e missões diplomáticas brasileiras sendo espionadas. Então, temos de olhar para essa questão com bastante cuidado para não permitir que, ao buscar combater os crimes localmente, se abram as portas inclusive para serviços de contrainteligência de outros países que querem buscar informações importantes nossas.

Eu gostaria de terminar tentando imaginar algumas questões do ponto de vista jurídico. Do ponto de vista da privacidade, temos um cenário bastante claro desenhado. Acho que vale a pena refletir o quanto vale a pena flexibilizar a privacidade, as proteções, as garantias de privacidade de todos os cidadãos, em nome da busca e da repressão de crimes a alguns cidadãos, de alguns criminosos. Da questão do sigilo das comunicações e sigilos comerciais eu já tratei.

Por último, eu gostaria de mencionar — já foi mencionada aqui — a questão da liberdade de expressão. No cenário internacional, nós tratamos bastante da liberdade de expressão, dos *chilling effects* da liberdade de expressão e de como só podemos nos expressar muitas vezes se temos a convicção de que não estamos sendo, por exemplo, monitorados. A liberdade de expressão compreende não só aquilo que nós estamos falando, mas também, nos tratados internacionais, aquela busca por informações em que estamos interessados.

Eu tenho um exemplo aqui. Acho bastante interessante, quando pensarmos num contexto em que cada vez mais as empresas guardam muitas informações sobre nós, quando digitamos uma informação no mecanismo de busca, e essas informações possam ser acessíveis a autoridades, pensarmos nesse exemplo, que é o poema do Carlos Drummond de Andrade intitulado *Elegia 1938.* Eu não me lembrava do nome desse poema, tive de perguntar a um amigo meu, a única coisa que eu lembrava é que ele termina assim: *"Aceitas a chuva, a guerra, o desemprego e a injusta distribuição porque não podes, sozinho, dinamitar a ilha de Manhattan".*

Eu não me atreveria hoje, num ecossistema em que não exista segurança das informações, a dar um Google em "dinamitar a Ilha de Manhattan", porque eu não sei, sinceramente, o que isso pode me gerar de consequências negativas. Para quem acha que eu estou exagerando, sugiro assistir a um documentário que se chama *Terms and Conditions May Apply*, que mostra como coisas tão inocentes

como essa têm gerado consequências ruins para pessoas, cidadãos bastante comuns em países democráticos como os Estados Unidos da América.

Eram essas as minhas considerações.

O SR. PRESIDENTE (Deputado Paulo Henrique Lustosa) - Muito obrigado Luiz Fernando.

Passo a palavra agora para o nosso último orador, O Professor da Fundação Getúlio Vargas Pablo de Camargo Cerdeira.

O senhor dispõe de 20 minutos.

O SR. PABLO DE CAMARGO CERDEIRA - Tenho uma pequena apresentação breve. Vou ser bastante objetivo, com foco aqui hoje... apesar de o título ser “Privacidade”, eu queria trazer para os Deputados e para os colegas presentes, Deputado Silas Freire, a importância com que o cuidado que a gente tem com dados assumiu nessa nossa sociedade. Porque esse trabalho da Câmara de discutir, trazer especialistas, trazer pessoas de diversas áreas para discutir o tema é importante.

(Segue-se exibição de imagens.)

O SR. PABLO DE CAMARGO CERDEIRA - Malte Spitz, um político da Alemanha que trabalha muito a questão da proteção dos dados, a importância que os dados assumiram nessa sociedade. Ele começa narrando esse caso de como a política de retenção de dados estava enfrentando resistências na Europa naquele momento. Depois, posteriormente, ela foi inclusive julgada — eu acho que o Pedro Mizukami já falou aqui a respeito do julgamento sobre a política de retenção. E ele continua mostrando o que foi possível fazer com os dados que ele obteve.

(Exibição de vídeo.)

O SR. PABLO DE CAMARGO CERDEIRA - Achamos que essa realidade é algo muito distante ou teórico, mas de fato ela não é e pode ter aspectos positivos.

Eu queria mostrar essa mudança que a nossa sociedade está enfrentando. E eu acho que esse vídeo é bastante exemplificativo.

(Exibição de vídeo.)

O SR. PABLO DE CAMARGO CERDEIRA - É o caso da Juíza Patrícia Acioli.

Vou voltar para mostrar a vocês o começo. Prestem atenção, por favor!

(Exibição de vídeo.)

O SR. PABLO DE CAMARGO CERDEIRA - Então, quando estamos falando de dados da segurança e dos crimes eletrônicos nesta CPI, eu gostaria de trazer para vocês é uma provocação. Esses estudos de casos que levamos para as salas de aula para debate com os alunos mostram o quão é importante essa nova constituição de nossa sociedade. O nosso modelo de montar as redes na nossa vida, na nossa sociedade atual é relevante. Pode ser relevante para questões de controle em uma sociedade excessivamente controlada, pode ser relevante para solucionar crimes. O fato é que o nosso contexto, o modelo em que construímos relações hoje não é mais só nas conversas, naqueles encontros que tínhamos, hoje nós deixamos registro disso.

(Segue-se exibição de imagens.)

Vou dar outro exemplo externo para vocês da importância dos dados. Eu tive a oportunidade de trabalhar por 4 anos aqui no Conselho Nacional de Justiça, do outro lado da Praça, e lá nós publicávamos um relatório anual — publica-se ainda — , o relatório Justiça em Números. Em 2009, decidiu-se incluir os dados do Supremo Tribunal Federal no relatório do Justiça em Números. O Conselho Nacional de Justiça está abaixo do Supremo Tribunal Federal, pelo art. 103-B da Constituição, aprovado aqui na Emenda Constitucional nº 45, de 2004, e o Ministro Marco Aurélio entendeu e se manifestou dizendo que não concebe que o Supremo seja colocado no *site* do CNJ como se o Supremo fosse submetido a esse órgão. Mas a frase real dele, que aí saiu um pouco editada, foi essa que saiu no CONJUR: *"Não concebo que dados do Supremo sejam colocados (...)"* Reparem na importância de associação dos dados, da figura dos dados com uma instituição, o quanto os dados podem representar a instituição. O próprio Ministro Marco Aurélio viu, nessa submissão de dados de um órgão ao outro, a submissão de um órgão a outro, institucionalmente falando, não apenas dos dados.

Depois, na FGV, nós montamos um projeto chamado Supremo em Números, em que coletamos todos os dados do Supremo e fizemos um estudo semelhante àquele caso do telefone que vocês viram lá atrás, para tentar entender o Supremo Tribunal Federal, tentar fazer propostas para melhoria do Supremo Tribunal Federal, o que chamamos de ordenamento. Conseguimos entender a estrutura do nosso

Judiciário. Disso surgiu inclusive uma PEC, que chegou a tramitar nesta Casa, baseada em dados.

Vejam a importância dos dados nesse nosso novo modelo de democracia. Podemos usar os dados para entender a sociedade, para entender as instituições, para propor melhorias. Mas, para que isso aconteça, precisamos entender que dado não pode ser avaliado como se diz muito por aí: dado é o novo petróleo, *data is the new oil*, uma frase que tem sido dita a cada 14 minutos como uma expressão jocosa.

Quando dizemos que dado é igual a petróleo, estamos equiparando apenas o valor à dificuldade de extração, o valor de utilidade que aquilo tem para diversos usos distintos, estamos falando de como um mesmo dado pode ser aproveitado. Com petróleo se faz plástico, se faz remédio, até se faz doce, se reveste bala. Dado também tem essa multiutilidade, só que dado diz respeito à sociedade, diz respeito à gente. Dado diz respeito aos recursos humanos onde ele está sendo gerado. Ele não está dizendo de um dinossauro ou uma alga que viveu lá algum tempo atrás. Os dados servem para gerarmos conhecimento e não produtos.

Com essa visão de dados, eu costumo dizer que a nossa sociedade mudou bastante. Em 20 anos, deixamos de ser uma sociedade meramente consumidora de dados e de informação e passamos a produzir muitos dados e informação conectados no Facebook, no WhatsApp.

Quando se fala de segurança de dados, de criptografia, de segurança da informação, estamos falando não mais só da segurança de um indivíduo se comunicando com o outro. É óbvio que existe o risco de a pessoa ter a sua honra e a sua imagem afetada por um vazamento, mas esse é um dos riscos, uma das análises, que é a análise estritamente individual do valor que o dado tem. Nessa nossa nova sociedade, quando falamos de proteção de dados, estamos falando não só da proteção individual, que está nos arts. 5º, 10 e 12 da Constituição, mas também da proteção da nossa estrutura de sociedade. Uma sociedade que não pode se utilizar de criptografia, que não pode se utilizar de proteção nas suas comunicações afeta não só a relação entre indivíduos, mas a própria liberdade de comunicação dessa sociedade.

Eu exporia alguns outros casos de uso de dados que se faz hoje e o quanto isso pode ser importante para a administração pública, mas não vou me alongar.

Eu gostaria só de passar para vocês que eu coordeno o escritório de dados na Prefeitura do Rio de Janeiro também. Lá, temos usado muitos dados de redes sociais para desenvolver projetos que têm garantido ao Rio constantes prêmios de cidade inteligente. Usamos dados de Waze para identificar onde os engarrafamentos acontecem, onde acidentes vão acontecer, como a população se desloca, etc. — isso tudo porque temos dados, porque o cidadão se sente à vontade para produzir dados. São todos dados que não nos chegam criptografados, são dados que nos chegam seguros.

Eu gostaria de fazer uma sugestão à Casa. Nós temos aqui em tramitação o Projeto de Lei nº 7.804, de 2014, que trata da importância do acesso aos dados pela administração pública e da importância da proteção desses dados.

Era essa a mensagem que eu tinha para trazer e, se possível, enriquecer os debates que esta CPI tem promovido.

Obrigado.

O SR. PRESIDENTE (Deputado Paulo Henrique Lustosa) - Obrigado.

Tendo ouvido o último expositor, Sr. Pablo de Camargo Cerdeira, passo a palavra ao Deputado Delegado Éder Mauro, autor de um dos requerimentos.

A Mesa desta audiência foi formada a partir de três requerimentos: um requerimento de S.Exa., um requerimento do Deputado Sandro Alex e um requerimento meu.

V.Exa., Deputado Delegado Éder Mauro, tem a preferência, mas há uma lista de Parlamentares inscritos. Se V.Exa. preferir ouvi-los primeiro, fique à vontade.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Não, vamos aproveitar a oportunidade, Sr. Presidente.

Senhores palestrantes, sejam bem-vindos! Nós sabemos que a CPI deve ganhar uma prorrogação para que possamos trazer mais informações e, cada vez mais, criar caminhos para que tenhamos exatamente a condição de encurtar a questão das apurações com o fato criminoso e outras coisas que muitas vezes estão aí travadas em relação a essas apurações criminais.

O nosso requerimento, que eu acho que é o que deve estar fazendo parte, foi pela convocação das operadoras, que aqui estão representadas por praticamente um sindicato das operadoras, e da ANATEL, e ele dizia muito a respeito da questão

dos expedientes que são solicitados junto às operadoras para cumprimento de ordens judiciais e, em específico, de requerimentos de autoridades policiais, porque muitos deles, dependendo do departamento jurídico da operadora, eram entendidos que não poderiam ser cumpridos senão por ordem judicial. Foram citadas aqui duas leis que especificavam que teriam que ser atendidos.

Inclusive, dei entrada hoje a um requerimento solicitando ao Ministro que determine, junto a ANATEL, que se baixe uma resolução junto às operadoras para que seja dado o cumprimento imediato a essas operações, porque eu tenho certeza de que é o que vai ajudar muito nessa questão dos crimes para que eles sejam evitados, para que as autoridades policiais possam chegar também às suas autorias quando eles já aconteceram. Essas foram as questões dos requerimentos.

Nós esperamos que vocês que hoje estão aqui para palestrar sobre o assunto possam também falar um pouco sobre isto: a questão do WhatsApp que eu acredito que o colega ali estava colocando. Os dados que são grampados por ordem judicial — a questão do MSS, a questão do áudio — são repassados para autoridade policial, mas os do WhatsApp não, porque não há como a autoridade policial processar a identificação dos dados que a operadora repassa.

Nós insistimos em dizer isso porque foi colocado muito aqui que não fica no Brasil a fonte para que possa repassar. Se o serviço é utilizado aqui no Brasil, e amplamente, acho até que mais do que ligação, por que não há uma sede aqui no Brasil para que a polícia, para que a Justiça e as próprias operadoras possam fornecer esses dados? Essa seria a minha pergunta principal em relação a isso.

O SR. PRESIDENTE (Deputado Paulo Henrique Lustosa) - Obrigado, Deputado.

Só a título de esclarecimento — o Deputado Delegado Éder Mauro lembrou bem —, na verdade, esta audiência pública é fruto de um acordo de desmembramento de uma audiência pública que teria muitos membros compondo a Mesa. A primeira parte foi na semana passada, quando os representantes das operadoras de telefonia estiveram aqui. E aqui ainda está o Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal — SINDITELEBRASIL. Esta segunda parte é mais focada na questão da criptografia e nos questionamentos

que foram levantados em relação ao Facebook e ao WhatsApp. Como a Mesa ficaria muito extensa numa audiência só, ela acabou sendo desmembrada.

Não havendo aqui mais autores de requerimento, eu passo à lista de inscrição dos debates.

O Deputado Silas Freire tem a palavra.

O SR. DEPUTADO SILAS FREIRE - Sr. Presidente, primeiro, quero ressaltar a importância de um prazo maior para esta CPI. Nós estamos propondo à direção dos trabalhos desta CPI, através de um requerimento que ainda deve ser deliberado, que esta CPI deixe para esta Casa e para o Brasil um seminário que nós realizaríamos para saber da segurança cibernética brasileira, até porque nós vamos sediar uma olimpíada. Esta CPI deixaria como legado — é uma proposta minha — um seminário em que nós indicaríamos as autoridades, especialistas, para que, desse seminário, tirássemos um documento. Isso vai ser deliberado ainda.

O SR. PRESIDENTE (Deputado Paulo Henrique Lustosa) - Deputado, permita-me interrompê-lo.

O SR. DEPUTADO SILAS FREIRE - Pois não.

O SR. PRESIDENTE (Deputado Paulo Henrique Lustosa) - Tanto o Delegado Éder Mauro como V.Exa. falaram sobre a prorrogação da CPI. Então, já para antecipar, por informação da Presidente, a Deputada Mariana Carvalho, que tem feito gestões junto à Presidência da Casa...

O SR. DEPUTADO SILAS FREIRE - Sim, sim. Nós estamos aguardando.

O SR. PRESIDENTE (Deputado Paulo Henrique Lustosa) - A informação que ela tem é a de que o Deputado Eduardo Cunha se comprometeu a colocar... Há quatro Comissões Parlamentares de Inquérito na mesma situação da nossa, ou seja, somada à nossa mais três com os prazos vencendo até o dia 10. O Deputado Eduardo Cunha se comprometeu na reunião do Colégio de Líderes a colocar em votação o pedido de prorrogação por 60 dias na sessão ordinária de hoje ou de amanhã. De qualquer modo, apenas por uma medida de precaução, mantém-se a pauta da leitura do relatório para hoje.

A SRA. DEPUTADA MARIANA CARVALHO - Só uma correção.

O SR. PRESIDENTE (Deputado Paulo Henrique Lustosa) - Pois não, Deputada.

A SRA. DEPUTADA MARIANA CARVALHO - Eu acabei de sair de lá da Presidência, onde fui justamente falar sobre esse caso. Não vamos fazer a leitura do relatório. Há o consenso de todos os Líderes da Casa no sentido de que, para esta CPI, serão os 60 dias; para outras, 15 dias, e algumas já entrarão no seu final. Então, não faremos hoje a leitura — já conversei com o nosso Relator, Deputado Esperidião Amin —, mas vamos esperar Plenário para a votação do nosso pedido de mais 60 dias, para ampliar o prazo da CPI.

O SR. PRESIDENTE (Deputado Paulo Henrique Lustosa) - Foi melhor do que dito por mim: dito pela fonte original.

Por favor, Deputado Silas Freire.

O SR. DEPUTADO SILAS FREIRE - Aliás, a ampliação por 60 dias seria ótima para que nós realizássemos esse evento para deixar como legado da CPI.

Vamos lá! Eu tenho algumas perguntas a fazer, eu estive anotando, pesquisando: a primeira é sobre a possibilidade — pergunto até ao próprio representante do WhatsApp — da taxação do serviço de WhatsApp. O que os senhores acham? Aí eu estendo a pergunta à Mesa: o que os senhores acham da taxação dos serviços, de o usuário pagar a conta da regulamentação do WhatsApp? Essa é exatamente a pergunta que eu anotei.

De acordo com uma matéria da revista *Exame*, o presidente da operadora Vivo, falando de telefonia, disse que o WhatsApp é bem mais perigoso que o Netflix, é uma ameaça que precisamos entender melhor. É uma reportagem que eu guardei aqui também, com a minha assessoria. *"Na visão do executivo, o serviço de mensagens e de voz sobre o IP do Facebook é uma 'operadora pirata' e age na ilegalidade"*. Essa foi uma declaração que ele deu, pública. *"É pirataria no pior sentido, é um operador na Califórnia, usando nossos números e clientes e sem obrigações regulatórias, jurídicas e fiscais"*, comentou o executivo naquele momento da entrevista.

Eu gostaria que os senhores esclarecessem — e aí não só o pessoal do WhatsApp, mas todos — esses comentários de um executivo importante da telefonia, numa revista de âmbito nacional. Isso assusta o cidadão que usa a Internet no Brasil inteiro. De certa forma, é uma declaração forte.

Ainda a propósito do WhatsApp — pesquisei algo aqui —, o WhatsApp vai cumprir a legislação brasileira no que diz respeito ao marco civil, já que não guarda registro, não tem endereço de notificação? O WhatsApp irá cumprir a legislação brasileira? Essa é uma pergunta que nós precisamos fazer. Quantos empregados o WhatsApp tem no Brasil? Como o Brasil pode lidar com uma empresa que não tem nenhum representante em nosso País? Como as autoridades vão notificar o WhatsApp se não tem ninguém no Brasil? Há essa interrogação. E por que o WhatsApp não guarda os registros? Nós já tivemos algumas respostas, mas nada muito objetivo. Como é que as empresas de telefonia fazem para tarifar ou não tarifar as chamadas de voz pelo WhatsApp? Se o aplicativo é criptografado, isso não seria uma quebra de neutralidade? Por isso, eu perguntei. Vocês não têm o teor das conversas, mas vocês têm o tempo. Para tarifar, teria que ter o tempo.

Sr. Presidente, eu vou fazer inicialmente essas colocações, mas tenho outras, porque, senão, podemos abrir demais o leque e não obter as respostas objetivas a essas perguntas, já que há outros colegas que vão também participar.

Muito obrigado.

O SR. PRESIDENTE (Deputado Paulo Henrique Lustosa) - Se os membros da Mesa não se incomodarem, nós ouviremos os outros dois Parlamentares inscritos e faremos uma pausa para as respostas.

O SR. DEPUTADO SILAS FREIRE - Então, Sr. Presidente, se V.Exa. me permite, vou fazer uma última pergunta.

O SR. PRESIDENTE (Deputado Paulo Henrique Lustosa) - Não, mas eu lhe permitiria voltar.

O SR. DEPUTADO SILAS FREIRE - Eu queria falar com o pessoal do Facebook.

O SR. PRESIDENTE (Deputado Paulo Henrique Lustosa) - A Deputada Mariana Carvalho vai me substituir, e eu me coloco para perguntar também. Aí nós fazemos a última rodada. Pode ser, Deputado?

O SR. DEPUTADO SILAS FREIRE - Tudo bem. Muito obrigado.

O SR. PRESIDENTE (Deputado Paulo Henrique Lustosa) - Pela lista de inscrição, tem a palavra o Deputado Eduardo Bolsonaro.

O SR. DEPUTADO EDUARDO BOLSONARO - Sr. Presidente, confesso que eu vim aqui muito mais para aprender e ouvir os palestrantes do que para encaminhar-lhes questionamentos. Porém, foi impossível não relembrar uma operação da Polícia Federal, após ouvir o relato do Prof. Pablo Cerdeira, da FGV. Houve o estouro de um caixa eletrônico numa região perto da Avenida Paulista, em São Paulo, e o crime acabou sendo desmembrado da mesma maneira que ele disse, através do rastreamento das antenas de ERB — Estação Rádio Base. Quando você tem alguns suspeitos, fica mais fácil, você só checa os celulares dos suspeitos; quando você não tem suspeito, dá uma trabalheira de que o pessoal não tem noção. O que seja levantar os dados de todas as pessoas numa região tão central quanto a Avenida Paulista, realmente, as pessoas nem imaginam. Com certeza, as pessoas que foram pegas, tanto no caso da Patrícia Acioli, quanto lá em São Paulo, no estouro do caixa eletrônico, não sabiam que o celular transmitia tanta informação. Foi uma operação linda.

Sr. Presidente, o meu maior receio com relação ao relatório desta CPI é chegarmos a apontar alguma restrição à Internet. Eu fiz uma PEC recentemente, dei entrada a ela há pouco tempo, tentando colocar no art. 5º da nossa Constituição, ou seja, como direito fundamental, o acesso à Internet. Para quê? Para que ninguém consiga restringir esse acesso e, se alguém tentar fazê-lo aqui através do Legislativo ou do Executivo, para termos meios de encaminhar a questão através de uma reclamação ao Supremo Tribunal Federal. A Internet tem que ser livre. Eu não sei quem colocou — acho que foi o Prof. Pablo — uma manifestação em Berlim, falando que a pessoas não queriam o controle dos dados. Eu acho que essa é a melhor maneira.

Ouvimos muito questionamento falando da Internet, de xingamentos, etc., crimes contra a honra. No Código Penal, não há nenhuma restrição estabelecendo que os crimes contra a honra podem ser feitos só através de carta, ou pessoalmente. A Internet pode muito bem ser englobada nesse contexto.

Vou um pouco adiante, aproveitando o gancho do colega Deputado Silas Freire, que levantou questões com relação a como é feito esse controle de dados, principalmente através de WhatsApp. Salvo engano, a sede do WhatsApp é na Califórnia; senão, com certeza, ele é originário dos Estados Unidos. Só há uma

maneira, Deputado Silas: nós produzirmos aqui a nossa tecnologia Não importa quantas ferramentas de controle o próprio WhatsApp nos prove que existam, nós nunca vamos deixar de ter essa desconfiança.

Agora, se nós olharmos o currículo escolar das nossas crianças aqui no Brasil é um lixo: é Sociologia, é Karl Marx, é LGBT no MEC dizendo o que temos que fazer. Infelizmente, nós vamos cair nesse ponto de novo. Então, se nós quisermos realmente ser uma potência e tratar a tecnologia com respeito aqui, nós temos que investir em educação. Infelizmente, foi feito mais um corte no FIES, no Ciência sem Fronteiras, e cada vez mais as nossas crianças vêm crescendo muito mais atrás da merenda escolar, indo para escola, do que atrás do conhecimento.

Faço esse breve registro.

Aqui, algumas pessoas já consigo até reconhecer pelo rosto, não preciso nem ler a plaquinha, é o caso do Bruno Magrani, representante do Facebook. Não tive oportunidade de ouvir o senhor nem o Sr. Mark Kahn, do WhatsApp, mas vou ficar aqui para ouvir os esclarecimentos, as respostas às perguntas.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Deputado.

Com a palavra o Deputado Jhc.

O SR. DEPUTADO JHC - Meus cumprimentos, Sra. Presidenta, Sras. e Srs. Parlamentares, todos os convidados. Eu gostaria mais uma vez de saudar de forma especial o Mark, que pôde também estar no dia de hoje aqui na Comissão e que conheci lá nos Estados Unidos na missão em que fomos ao Vale do Silício. Nesta oportunidade, ele vai poder fazer os esclarecimentos devidos e necessários à Casa, especialmente a esta Comissão Parlamentar de Inquérito.

Falava-se falava muito na ideia do Estado controlando tudo, como na grande obra de George Orwell. Ele fala justamente do Big Brother, do Grande Irmão, que inspirou um *reality show* aqui no Brasil e mundo afora. Mas hoje estamos vivendo essa era realmente. A privacidade das pessoas é relativa.

Recentemente, eu estive conversando com diretores de alguns aplicativos também no mundo e eles me relataram coisas curiosas. O Google tem o sistema de tirar fotos das ruas, das cidades, o Google Street View. Eles foram processados na Europa, enquanto aqui no Brasil ocorreu o contrário, as pessoas queriam saber a

hora em que o carro do Google iria passar, para ir para a porta de casa, para poder aparecer na foto. Então, é também uma questão cultural.

Lá na obra de George Orwell era o Estado controlando, enfim. E aqui nós vemos empresas que têm o poder da informação desses dados. Mas fica a pergunta, especialmente ao Bruno e ao Mark, porque, na legislação dos Estados Unidos, ao que me parece, há a obrigatoriedade de, se solicitadas, todos esses aplicativos terem de passar essas informações. Então, quando essas informações ficam nos Estados Unidos, o Governo dos Estados Unidos estaria obrigado a passar todas essas informações. Na época do Snowden, quando houve aquele grande escândalo da NSA e o Brasil e outros países foram espionados, salvo engano, o Facebook também entrou com ação contra o próprio Governo dos Estados Unidos, porque acabou se utilizando dessas informações. O que mudou de lá para cá?

Há também informações — eu peguei algumas matérias — no sentido de que, em questão de proteção de dados, o WhatsApp, entre outros aplicativos, teria dificuldade em oferecer essas informações. Eu queria também que pudessem esclarecer, até para desmistificar alguns pontos, se realmente existe isso e como ela está se adaptando à nova legislação brasileira, em que os próprios delegados podem fazer a solicitação sem necessidade do pedido à Justiça.

Esta semana foi feito um protesto... Aproveito a oportunidade da presença do Mark aqui. A *hashtag* não calha ao WhatsApp. Hoje as operadoras travaram uma batalha muito grande com esses aplicativos de voz, e o WhatsApp hoje é um dos principais. Então, na linha de outros Parlamentares que aqui já falaram, o Ministério já foi notificado pela PROTESTE. Então, como fica? E na questão da proteção de dados?

Outro dado que eu quero destacar é essa aceitação de termo de uso. Hoje em dia, ele é muito complexo ainda, parece aqueles contratos com letras pequenas, de difícil transparência. Se nós tivéssemos esse termo de uso de forma mais clara, de forma que o consumidor pudesse saber efetivamente quais dados dele estariam sendo disponibilizados, eu acho que seria mais transparente e seria até mais ético. Uma coisa é você saber efetivamente o que você está oferecendo e outra é você tentar manipular para dar um arcabouço de legalidade. Aí, depois de aceitos aqueles

termos, você poder fazer o que quiser com os dados daquele consumidor, daquele cliente.

Eu estava observando esta semana... Eu nunca tinha feito essa identificação pelo smartphone ou pelo iPhone — eu acho que outros também devem ter o mesmo sistema —, mas eu acabei botando minha digital para desbloquear o iPhone. Então, eles têm todas as informações. Ou seja, os servidores, lá, eles vão ter, mundo afora, as informações. A digital, como eu falava com o amigo Deputado Eduardo Bolsonaro, é coisa que a nossa polícia tem no Brasil, e essas informações também são disponibilizadas às empresas particulares.

Então, como se dá essa relação de empresa e Estado? Pergunto aos Profs. Pablo e Luiz Fernando e ao Diretor Alexander.

O advento da Internet nos traz vários questionamentos e nós temos, claro, essa preocupação com a proteção de dados — isso em dimensões planetárias. Essa discussão está acontecendo em todo o mundo, não tenho dúvidas disso. Na semana passada, falávamos inclusive com a Presidenta Mariana Carvalho que agora o Estado Islâmico é digital. Antes, Al-Qaeda funcionava no analógico. Hoje, já recrutaram mais de cinco jovens, mais de cinco pessoas do Ocidente, inclusive brasileiros, que a mãe não sabe nem se morreram ou se não morreram, se estão vivos ou se não estão vivos. No próximo ano, nós estaremos já em ano de Olimpíada e é preciso saber como se pode harmonizar. Talvez não criar mais obrigações, mas como se pode ajudar o Estado Brasileiro e outros estados. Como o Eduardo falou também, nós temos que criar a nossa tecnologia. Essa questão de espionagem, acho que talvez isso esteja longe. Seria meio que utópico também achar que isso vai acabar. Desde quando o mundo é mundo que um está vigiando o outro para saber quais são as táticas, quais são as estratégias, quais são os planejamentos futuros, até como uma forma de proteção. Então, seria hoje uma utopia. Como harmonizar essas relações para que seja tudo isso feito de uma forma justa e que não prejudique o desenvolvimento tecnológico, o desenvolvimento científico e a inovação no País, no Brasil ou em qualquer lugar que seja.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Deputado Jhc.

Ainda temos dois inscritos, Deputado Paulo e Deputado Silas. Não sei se vocês preferem fazer nesse bloco...

(Intervenção fora do microfone. Inaudível.)

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Vou passar primeiro a palavra ao Sr. Mark Kahn, Vice-Coordenador Jurídico Geral do WhatsApp.

O SR. MARK KAHN - *(Exposição em inglês.)*

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada.

Concedo a palavra ao Sr. Bruno Magrani, Diretor de Relações Institucionais do Facebook Serviços Online do Brasil.

O SR. BRUNO MAGRANI - Obrigado pelas perguntas, Sra. Presidente e membros desta Comissão. Vou começar pela pergunta do Deputado Delegado Éder Mauro, em relação ao acesso das autoridades de investigação a esses dados.

Delegado, a gente tem um compromisso enorme com a segurança das pessoas e com a responsabilidade das polícias e das autoridades de investigação de efetivamente conseguirem combater a criminalidade *on-line*. Por isso, a gente criou um portal *on-line* por meio do qual qualquer autoridade de investigação pode enviar esses pedidos diretamente para o Facebook. Então, se ela tiver um pedido ou uma ordem judicial, ela poderá encaminhá-lo eletronicamente — nem precisa mandar por papel. Há um portal, que se pode acessar, encaminha-se o pedido através do portal e recebe-se a resposta diretamente a partir do portal. A gente tem uma equipe que funciona 24 horas por dia, 7 dias da semana, além dos canais de emergência que temos, como o Mark mencionou, para as situações em que há um eventual risco à vida da pessoa.

O Deputado Silas Freire disse que fará algumas perguntas específicas sobre o Facebook. Eu estou à disposição para responder às perguntas do Deputado.

O Deputado Eduardo Bolsonaro mencionou uma frase que eu anotei e que eu acho importante. Disse ele que a Internet deve ser livre. A liberdade e a abertura da Internet têm sido identificadas realmente como duas características fundamentais para a inovação na Internet. Eu acho que o senhor apontou muito bem que, se o Brasil quer efetivamente desenvolver a tecnologia local e ter empresas inovadoras, como existem em diversos lugares do mundo, o caminho é exatamente permitir a abertura e a inovação da tecnologia.

Por fim, quanto às indagações do Deputado JHC, queria lembrar que uma das primeiras audiências de que eu participei aqui no Congresso, em 2013, tratou exatamente da questão da espionagem. Eu trouxe uma frase que o CEO do Facebook disse na época: *"O Facebook nunca permitiu nenhum tipo de acesso backdoor aos servidores do Facebook por nenhum governo no mundo. Nunca. O Facebook só encaminha dados relativos aos seus usuários mediante lei, com relação à lei aplicável, e mediante ordens judiciais."* Então, essa é a maneira através da qual o Facebook dá acesso aos seus dados.

Portanto, esse mesmo portal que eu mencionei é o que as autoridades de investigação no mundo inteiro podem utilizar para submeter esses pedidos de acesso aos dados. Uma vez que esses pedidos são recebidos, o Facebook analisa detalhadamente cada um deles para ver se eles cumprem o devido processo legal, que é uma garantia importantíssima dos usuários e das empresas no Estado Democrático de Direito. Se o pedido atender todos os requisitos legais, especialmente o devido processo legal e a lei aplicável, o Facebook vai cumprir com a ordem judicial ou com o pedido a que eventualmente se relacionar.

Em relação ao tema das operadoras e aplicativos que V.Exa. mencionou — o Mark já falou sobre o WhatsApp —, eu quero dizer, em relação ao Facebook, que o ecossistema da Internet trabalha sempre em cooperação um com o outro. Quando V.Exa. contrata um serviço de telefonia para acessar dados, eu acredito que V.Exa. não contrata serviço para acessar o *site* da operadora, mas, sim, para acessar *sites* de outras empresas, seja o serviço do Facebook, seja o serviço do WhatsApp, seja o serviço de algumas outras empresas que inclusive já participaram desta CPI. A gente acredita que isso gera valor para as operadoras. A gente acredita que esse ecossistema em que você tem uma camada de conteúdo que tem uma inovação constante, uma variedade enorme de serviços e aplicativos que as pessoas podem acessar, é fator importante para gerar receita e aumentar o número de usuários da camada inferior de telecomunicações.

Só para completar os dois últimos pontos que V.Exa. mencionou, que têm a ver com a questão do acesso a dados, os termos de uso e transparência, o Facebook tem uma preocupação muito séria em relação a isso. O que nós fizemos, que outras empresas fizeram e têm adotado na indústria, é a publicação de um

relatório de transparência em que o Facebook traz todos os pedidos de acesso a dados que foram feitos à empresa ao redor do mundo inteiro, como no Brasil, nos Estados Unidos, na Índia. Eu posso encaminhar o *link* a V.Exa.

O SR. DEPUTADO JHC - Mas esse é o mesmo *site* que o senhor disponibilizou?

O SR. BRUNO MAGRANI - É outro *site*. Eu posso encaminhar para esta Comissão o *link*, as informações são públicas, estão disponíveis no *site*. É óbvio que esses dados são agregados, a gente não tem informações específicas. Mas ele tem o número de requisições que foram feitas, etc.

A gente tem um compromisso com o usuário em relação à transparência. Isso é parte importante do processo, que visa estabelecer uma relação de confiança com o usuário. A gente acredita que, se o usuário perder a confiança no nosso serviço, ele vai parar de usar o nosso serviço. Do ponto de vista comercial, também não faz o menor sentido se o usuário não tiver confiança no nosso serviço.

Por fim, no que se refere à questão do terrorismo, que V.Exa. mencionou, o Facebook tem uma política muito clara: não permitir na sua plataforma nenhum tipo de atividade relacionada ao terrorismo.

O SR. DEPUTADO JHC - Só para ter uma ideia, segundo matéria recente da revista *Veja*, salvo engano, são 200 mil *tweets* por dia a favor do Estado Islâmico — um número grande. Chega a ser assustador quando se fala em 200 mil *tweets*. Eles apagam contas, mas conseguem abrir outra conta muito facilmente. A guerra, portanto, tem que ser diária e permanente.

O SR. BRUNO MAGRANI - Nesse ponto, a gente tem, mais uma vez, alguns mecanismos que nós usamos para prevenir esse tipo de atividade. O primeiro mecanismo são, obviamente, nossas políticas contrárias a qualquer tipo de atividade relacionada ao terrorismo na plataforma do Facebook. A segunda ferramenta são exatamente os mecanismos de denúncia que existem no Facebook.

Eu creio que V.Exa. está familiarizado, mas qualquer pessoa pode denunciar qualquer conteúdo no Facebook por violação das políticas do *site*. Uma vez que esse conteúdo é denunciado, a gente conta com uma equipe que trabalha 24 horas por dia, 7 dias da semana, espalhada no mundo inteiro, que entende a língua e o

contexto brasileiro e que pode agir sobre esse conteúdo, não só aqui no Brasil, mas no mundo todo.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Concedo a palavra ao Sr. Alexander Castro, Diretor Regulatório do Sindicato Nacional das Empresas de Telefonia e de Serviços Móveis Celular e Pessoal — SINDITELEBRASIL.

O SR. ALEXANDER CASTRO - Eu gostaria de começar abordando as colocações do Deputado Delegado Éder Mauro com relação às operadoras e à disponibilização de dados e registros que as operadoras guardam nos seus *data centers* aqui no Brasil.

É importante que se deixe bem claro que as operadoras têm todo o interesse em contribuir para a apuração do ilícito, seja na Internet, seja na telefonia.

Eu gostaria de reforçar que durante todo o processo de discussão do Marco Civil da Internet as operadoras trabalharam no sentido de que o texto final da lei contemplasse a obrigatoriedade da guarda dos registros de aplicação. Nas primeiras minutas da lei, não estava prevista a guarda dos registros de aplicação.

Só para lembrar, os registros de aplicação são aqueles que dizem quem e que *site* o usuário acessou. Por vedação da própria lei do Marco Civil da Internet, as operadoras estavam proibidas de guardar essa informação, só podiam guardar o IP de origem, o início da navegação e o término da navegação. A quem o usuário acessou e que *site*, não. Nas primeiras versões do Marco Civil, não havia a obrigatoriedade de nenhum outro provedor de aplicação guardar essa informação. Num trabalho conjunto com o Ministério Público e a Polícia Federal, a gente participou de várias audiências, de debates e de seminários, no sentido de alertar para a necessidade de permitir que essas empresas guardassem essa informação, com o intuito de contribuir para o processo de apuração do ilícito.

Como outros colegas já apresentaram nesta Mesa, a liberdade de expressão foi algo extremamente defendido pelo SINDITELEBRASIL e pela categoria das operadoras, seja no serviço convencional de telefonia, seja através da Internet. A gente entende — a nossa própria Constituição garante — é que a liberdade de expressão é um direito fundamental e que é vedado o anonimato.

A facilidade na apuração dos crimes na Internet era também de interesse das operadoras. Ocorre que o Marco Civil da Internet só possibilita o fornecimento de

dados sem autorização judicial apenas para os dados cadastrais. Todos os demais dados que a gente é obrigado a armazenar só podem ser fornecidos mediante autorização judicial.

Então, para garantir a segurança e a privacidade dos nossos usuários, até pela responsabilização que as operadoras passam a ter no momento em que guardam os dados, existe mesmo uma preocupação das operadoras no sentido de caracterizar se a autoridade administrativa, conforme prevê o Marco Civil da Internet, tem competência para nos solicitar os dados cadastrais.

Finalmente, depois de longo tempo, porque a regulamentação do Marco Civil ainda não saiu, seria muito bem-vindo se esse esclarecimento viesse na regulamentação. Como a regulamentação não saiu e já se passaram aproximadamente 17 meses da aprovação da lei, a gente vem recebendo solicitações de diversas autoridades administrativas e acabou chegando, naquele eslaide que eu apresentei, a um consenso em relação àquelas duas leis. A gente está seguindo as duas leis que foram mencionadas.

Na verdade, a ideia da categoria das operadoras é trabalhar em conjunto e ajudar no que for possível. A gente vem buscando sempre melhorar as ferramentas, a automatização do processo e o atendimento no prazo mais rápido possível, que chega a ser de 2 a 24 horas — os processos mais complicados levam, no máximo, 24 horas. A gente vem trabalhando e investindo para facilitar o acesso a essas informações.

Eu gostaria de fazer um comentário sobre a manifestação do Deputado Silas Freire, que mencionou o Presidente da Telefônica, quanto à taxação dos serviços do WhatsApp e à eventual ilegalidade desse aplicativo.

É importante esclarecer que o setor não tem nada contra o WhatsApp ou qualquer provedor de aplicação. O setor de telecomunicações brasileiro sempre se orgulhou de promover competições no Serviço Móvel Pessoal (SMP) — o Brasil é o quinto maior país em termos de competição na área de SMP.

O setor de telecomunicações é sinônimo de tecnologia e de desenvolvimento e tem proporcionado aquilo que eu mostrei no meu eslaide: as telecomunicações são um caminhão que transporta uma série de serviços e aplicações que são

ofertados na Internet, chamados pela Lei Geral de Telecomunicações serviços de valor adicionado.

O serviço de valor adicionado é o serviço utilizado pelo *site* Climatempo, por exemplo, no qual alguém, usando as redes das operadoras de telecomunicações, fornece informações sobre o tempo. É o caso também das informações sobre as condições de tráfego, mapa das cidades, ou qualquer outra informação ofertada na Internet.

Mas é importante chamar a atenção para o que consta no art. 61 da LGT, que diz que os serviços de valor adicionado não se confundem com o serviço de telecomunicações, ou seja, com o serviço que lhe dá suporte.

Então, nós temos argumentado que existe uma infinidade de serviços e aplicações que não se confundem e que devem continuar sendo negociados com as operadoras de telecomunicações, como vêm sendo, e ofertando uma série de facilidades e possibilidades de melhoria de qualidade de vida para os nossos usuários de telecomunicações, que, no fundo, também são usuários desses aplicativos.

Existem algumas empresas cuja finalidade do serviço que elas oferecem é justamente ser um serviço paralelo de comunicação de voz, mas que apresenta uma enorme assimetria tributária e regulatória.

Nós temos procurado negociar com o Poder Executivo de forma geral, visando à sustentabilidade do setor de telecomunicações porque, sem telecomunicações, como foi mencionado nesta Mesa, não há Internet. Portanto, é importante que a sustentabilidade do setor de telecomunicações seja garantida para 2015, 2025, 2030.

Nós entendemos que, para o mesmo serviço, seja aplicada a mesma regra. Não somos contra o aplicativo A, B ou C. O que nós queremos é uma simetria regulatória e tributária.

Não é razoável que uma operadora de telecomunicações tenha de ter garantias de qualidade do serviço; que tenha de ter um *call center*; que tenha de garantir um tempo médio de reparo se o serviço sair do ar; que tenha de garantir bloqueio de sinal nos presídios; que tenha de garantir bloqueio de aparelhos terminais roubados; que tenha de garantir uma série de coisas referentes ao Custo

Brasil de operação, quando outros provedores de serviços e aplicativos de Internet não têm que assumir esses compromissos. Eventualmente eles nem estão no Brasil!

Dessa forma, nós entendemos que isso não é interesse apenas do setor de telecomunicações, mas do País, principalmente quando vemos a receita do Estado cair. O setor de telecomunicações contribui tremendamente nesse sentido: entre fundos e impostos, ele contribui anualmente com 80 bilhões de reais. Então, trata-se de um valor significativo, principalmente neste momento de crise que o País está vivendo.

Estamos demandando do Poder Executivo de maneira geral — Ministério do Planejamento, Ministério da Fazenda, Ministério das Comunicações, ANATEL — uma reflexão, um estudo.

Recentemente, o Ministério das Comunicações publicou uma consulta pública para discutir o modelo de telecomunicações brasileiro. Essa consulta pública vai até 23 de dezembro, e nela foi colocada uma série de perguntas para serem respondidas pela sociedade de maneira geral.

Assim, esperamos, a partir dessa ampla consulta à sociedade brasileira, lidar adequadamente com a atual distorção que entendemos existir em função dessa assimetria. Esse é o ponto que eu gostaria de esclarecer.

Deputado Silas Freire, se eu não tiver sido totalmente claro, estou à disposição para mais esclarecimentos.

Quanto à criptografia, gostaria de dizer que nós atendemos à demanda do juiz quando ele solicita que façamos uma interceptação e disponibilizemos a comunicação para o Ministério Público ou para um órgão policial de maneira geral. E nós o fazemos. No momento em que recebemos a comunicação, nós a interceptamos e a encaminhamos para o Ministério Público. Não se faz nenhum tipo de gravação ou registro daquilo ali, que passa a ser tratado pelo Ministério Público, pela Polícia Federal ou pelas autoridades administrativas.

Se aquela informação está criptografada e há uma dificuldade de acessar a informação propriamente dita, lamentavelmente, as operadoras de telecomunicações não têm como auxiliar, porque elas não têm acesso ao código-fonte da empresa que tem o conteúdo e que lhes mandou a informação para ser transmitida.

Volto a dizer: nós somos aquele caminhãozinho que transporta pacotes de forma transparente. E, como o próprio Marco Civil da Internet determina, não podemos monitorar, acessar ou manipular esses pacotes de dados. Então, nós simplesmente temos que transportá-los, utilizando para isso o modelo do melhor esforço, ou *best-effort*, que é um jargão comum na área de telecomunicações. Eu recebo o pacote num elemento de rede e o retransmito, recebo e retransmito, recebo e retransmito — é assim que isso funciona num processo normal.

Eu não sei se respondi a todas as perguntas, mas me coloco à disposição para, se houver algum questionamento adicional, esclarecê-lo.

Obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada.

Concedo a palavra ao Sr. Luiz Fernando Moncau, Professor do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas.

O SR. LUIZ FERNANDO MONCAU - Obrigado.

Vou tentar tratar de algumas questões aqui, a primeira delas referente à regulamentação do WhatsApp.

No Centro de Tecnologia e Sociedade, nos manifestamos numa linha razoavelmente parecida com a que o Alexander expôs aqui, apontando para as diferenças fundamentais que existem entre uma tecnologia que presta um serviço *over-the-top*, ou seja, uma tecnologia prestada pela Internet, e outra que presta um serviço de telecomunicações *stricto sensu*, que é regulado pela ANATEL e que tem todas as suas regras estabelecidas, ou seja, é um serviço regulamentado. Isso não afasta a necessidade da obediência a regras locais — direito do consumidor, direito trabalhista, direito tributário, etc.

Existe um desafio enorme no que diz respeito a como enquadrar não só esse, mas todos os outros serviços que são *over-the-top*, no sistema jurídico brasileiro. Então, nós temos discussões sobre como enquadrar e como tributar serviços de *streaming*, de *e-mail*, e assim por diante. Todos os serviços que surgiram com a Internet apresentam desafios regulatórios. Esse é um problema que nós vamos enfrentar não apenas nesse tipo de serviço, que presta serviços semelhantes ao de telefonia, mas também em outros tipos. Essa discussão é muito semelhante às disputas entre táxi e Uber, TV por assinatura e Netflix, telefonia e WhatsApp, e

outros serviços que pudermos imaginar. Então, essa é uma questão ainda não resolvida, que precisa de muito debate.

A princípio, no meu modo de olhar hoje — estou disposto a debater isto —, eu diria que não deveria haver uma equiparação. Fazer isso seria tratar duas coisas diferentes da mesma forma. Mas nós precisamos criar os incentivos corretos para fazer com que essas empresas tenham escritórios aqui, se adequem às regras locais, etc.

No que diz respeito aos termos de uso, esse é um ponto bastante importante. Nós temos uma pesquisa em desenvolvimento lá na FGV sobre esse assunto. Só citando alguns dados, há uma pesquisa da Carnegie Mellon University que aponta que, se fôssemos ler até o fim todos os termos de uso de *softwares* e aplicativos que usamos, que instalamos nos nossos computadores ou celulares, demoraríamos 2 meses ou mais apenas para fazer isso. Então, é absolutamente inviável para um ser humano normal fazer esse trabalho. Isso indica que há uma necessidade de simplificação desses contratos digitais, e isso aponta para a necessidade de se rediscutir esses contratos digitais de uma maneira bastante ampla.

Temos o Código de Defesa do Consumidor, que trata dos contratos de adesão e funciona de maneira bastante importante para esse ambiente digital, mas eu tenho a sensação de que, hoje, isso não é suficiente.

Por exemplo, hoje eu recebi uma mensagem de um dos aplicativos que eu uso dizendo que eu tinha que atualizar, aceitar os novos termos de uso — que eu fiquei sabendo que eram extremamente agressivos em relação à privacidade —, sob pena de ter que parar de usar o serviço.

Então, há algumas práticas de empresas extremamente agravadas no ambiente digital, e, neste caso que eu citei, estamos falando especificamente da alteração unilateral de contrato: ou você muda o contrato, ou o seu aplicativo para de funcionar. E as entidades de defesa do consumidor, que já têm que lidar com um universo muito grande de assuntos, não têm pernas, condições e capacidade técnica para encaminhar essas questões. É um desafio imenso essas mudanças, e problemas que têm acontecido o tempo todo.

Então, eu acho que é um desafio que o mundo inteiro está enfrentando, não é só o Brasil, e vale a pena ficar atento. Não sei se passa pela legislação, mas talvez

passe por sentar empresas e consumidores em uma mesa para discutir melhores práticas a fim de que o consumidor não fique tão exposto, principalmente às violações de privacidade.

E um último ponto em relação aos dados biométricos, à impressão digital: há um avanço de companhias em relação a alguns dados pessoais e também do Estado, e de companhias em relação a outros dados. Então, eu já fui forçado pelo meu banco a cadastrar a minha impressão digital, a contragosto, sob pena de não conseguir sacar mais dinheiro no caixa eletrônico, outra violação de direito do consumidor pela qual eu não gostaria de ter passado. Vai haver uma movimentação no sentido do cadastramento de dados biométricos, das digitais, para fins de votação nas urnas eletrônicas.

Parece que uma coisa não tem muito a ver com a outra, mas, no fundo, são os nossos dados sendo armazenados em imensos bancos. Os bancos de dados cada vez se comunicam mais, cada vez podem ser processados em uma velocidade mais alta, e cada vez dizem mais sobre quem nós somos e o que nós fazemos.

Então, todas essas questões... Há, cada vez mais, câmeras em todos os lugares, câmeras podem reconhecer facialmente quem nós somos. Então, se estamos em uma manifestação na rua, protestando contra ou a favor de alguém, podemos ser reconhecido. Tudo isso suscita uma série de questões importantes para a democracia, porque esses dados podem ser trabalhados.

O que vamos fazer? Precisamos ter alguma resposta, que, nesse caso, eu acho que é regulatória. Esses dados vão poder ser armazenados para sempre? O TSE, que outro dia quis passar os dados para o SERASA em troca de certificados digitais, vai poder passar os dados biométricos das pessoas, ou não? Isso não está claro.

Não há legislação de proteção de dados pessoais no Brasil. Isso está em discussão no âmbito do Ministério da Justiça, não chegou nesta Câmara, vai chegar em breve. Essa é uma questão extremamente importante, que vai precisar ser decidida e que mexe com muitos interesses, já que há muitas empresas e governos que querem explorar os dados apenas da ótica do dado como *(ininteligível)* e não como dados de seres humanos, como disse o Pablo aqui um pouquinho mais cedo.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada.

Concedo a palavra ao Sr. Pablo de Camargo Cerdeira, professor da Fundação Getúlio Vargas.

O SR. PABLO DE CAMARGO CERDEIRA - Obrigado. Eu vou ser bem breve. Eu tenho só alguns pequenos comentários.

Com relação à legislação brasileira, esse é um desafio, como o Moncau já comentou, e não só nacional. Já tivemos o nosso Legislativo se posicionando no Marco Civil sobre qual legislação se aplica quando se presta esse serviço no País; já tivemos os tribunais superiores se manifestando a respeito, mas há todo um trabalho de construção que faz parte desse trabalho. Quando o Legislativo debate, quando publica e aprova a legislação, envia uma mensagem para os outros atores da sociedade, inclusive externos — não só nacionais, mas do exterior. Isso aconteceu muito com o Marco Civil, que foi tomado como um exemplo fora do País; é um exemplo que está sendo discutido em outros países.

Então, independentemente da efetividade imediata que se consiga, é importante que esse debate continue, que a aprovação dessas normas continue, porque elas não só definem direitos e garantias, mas configuram nortes para nós.

Com relação aos termos de uso, de fato, já passamos de uma fase de contratos de adesão, em que tínhamos que aderir em massa a contratos. Agora, temos a massa dos dois lados. Antes, o contrato de adesão era um contrato que alguns poucos atores ofereciam para uma massa de pessoas, e agora temos uma situação em que uma massa de pessoas assina uma massa de contratos diferentes. De fato é preciso...

Esse é um ponto que pode ser refletido com relação à garantia de direitos. Pode ser debatido esse processo de simplificação. Já ocorre um pouco isso no anteprojeto de lei de proteção de dados pessoais, quando estabelece, especialmente com relação às garantias de proteção dos dados pessoais, que os termos têm que ser muito claros. Isso já vem do CDC, enfim...

Sobre criptografia, eu só queria alertar para um aspecto técnico. Fala-se muito da criptografia como uma forma de impedir totalmente a investigação, ou algo que é utilizado por criminosos. Essa figura de aparência muito. Mas eu acho que ficou muito claro aqui, nos outros depoimentos, que a criptografia é usada no dia a dia.

Quando fazemos uma ligação no celular, isso é criptografado para evitar clonagem de celular; não é uma criptografia para proteção exclusiva. Quando usamos o cartão de crédito, o cartão tem que ficar dentro da maquininha. Se você tirar o cartão e digitar a senha depois e ele não funciona, você está usando criptografia, está assinando digitalmente um documento.

Portanto, usamos a criptografia no dia a dia. É algo que já está presente, e nunca impediu os órgãos de controle de atuar quando necessário, inclusive com alguns exemplos, como o caso que o Deputado Eduardo Bolsonaro citou, dessas investigações que são feitas. É possível fazer.

Vai muito do trabalho desta Câmara definir os usos devidos e indevidos de criptografia, ou, de outro lado, das investigações. Uma vez garantidos os direitos individuais, as garantias da sociedade — e boa parte delas entraram no Marco Civil, outros já estavam na Constituição —, respeitados esses pilares que já foram definidos, é possível discutir flexibilizações, mas sempre olhando a criptografia como algo que vem ajudar a nossa sociedade muito mais do que atrapalhar, do que ser uma ferramenta para evitar a investigação.

A SRA. PRESIDENTA (Deputado Mariana Carvalho) - Vamos abrir um novo bloco de perguntas.

Com a palavra o Deputado Paulo Henrique Lustosa.

O SR. DEPUTADO PAULO HENRIQUE LUSTOSA - Obrigado, Presidente. Primeiro, quero parabenizá-la pela prorrogação. Eu estava dando a notícia que V.Exa. estava lá se empenhando em garantir a prorrogação. Então, vamos aproveitar esses 60 dias para produzirmos um relatório ainda melhor do que o que já estava aqui avançado.

Eu vou começar os questionamentos no sentido inverso, até porque nossa curiosidade aqui com o nosso caro Mark, do WhatsApp, faz com que se avolumem as perguntas.

Primeiro, eu perguntaria para Moncau e para o Cerdeira, já que estão discutindo, estão na academia, estão debatendo essa questão dos termos de uso, do termos de adesão...

Na verdade, o que está na pauta é a responsabilização. Na maior parte, nos termos de uso, aparece... Quando vamos ao médico para fazer uma cirurgia, nos

mandam assinar uma lista de coisas dizendo que, se acontecer tal coisa a responsabilidade é nossa; se não sei o quê... Ou seja, o médico quer se isentar ao máximo de qualquer coisa que possa acontecer no procedimento, e quem está pagando, quem está ali receber o tratamento, é o responsável.

Essa eu acho que é uma questão importante para esta Comissão de Crimes Cibernéticos, assim como não só apenas estabelecer quando o Estado pode acessar informação para o uso devido — e, aí, imagino que sejam os casos excepcionais. Ou seja, a regra é que o Estado não tem que ter acesso aos meus dados pessoais. Essa deve ser a regra. A exceção é que, caso eu cometa um crime, caso eu seja suspeito... Isso é exceção. Então, a regra é a preservação. Mas, no caso de vazamento de dados, de mau uso dos dados, de corrupção dos dados, a responsabilidade é de quem?

E eu pego carona no caminhão que o Alexander colocou aqui. Ou seja, eu tenho um caminhão, onde está todo mundo empilhado. Tem um motorista, tem um carona na boleia, tem um monte de gente. O caminhão derrapa, capota, e as minhas informações são espalhadas. A responsabilidade é de quem? É do dono do caminhão? É do motorista do caminhão? É do encaixotador que colocou a caixa com as minhas informações em cima do caminhão? Eu acho que nós ainda estamos longe disso, em termos de marco regulatório. Então, eu queria ouvir de vocês qual é o estado da arte, da discussão, em termos disso.

Com relação ao Alexander, concordamos fundamentalmente com a sua argumentação de que o papel central das operadoras é o de transportar, independentemente... Na verdade, não é independentemente, a lógica da neutralidade parte do pressuposto de que você não quer nem saber o que está lá dentro, para garantir a qualidade do serviço igual para todo mundo. Mas eu pego uma fala sua sobre a questão da vedação do anonimato.

E tem uma questão, talvez mais de natureza técnica, que é a seguinte: Nós temos o anonimato clássico, mas, no mundo virtual, temos o que chamamos de *spoofing,* ou seja, a possibilidade de se usar IPs falsos para acessar a rede e provocar seus atos, os atos que se queira. E, aí, existe um protocolo, um procedimento de prevenção desse uso anônimo, ou de falso anonimato, que é o BCP 38. Quer dizer, é uma solução, um protocolo para minimizar os riscos desse

tipo de anonimato. As operadoras estão usando isso. Como estão usando, não é responsabilidade delas. Na mesma lógica que, na audiência passada, estávamos discutindo o IP-6, ou seja, a versão para o IP-6 como mecanismo de prevenção ou de minimizar os riscos de mau uso das informações transitadas e aumentar a segurança da rede. Também aí eu pergunto: em que medida as operadoras têm trabalhado com isso ou se estão trabalhando com isso?

Para o Bruno e mais para o Mark, ficou claro em relação ao WhatsApp que o WhatsApp não guarda, não armazena a maior parte das informações que transita na plataforma, no aplicativo, como forma de dar maior celeridade, melhor qualidade. Há também questionamentos — e aqui também alguns que eu tinha discutido com a nossa Presidente — relacionados a como é esse procedimento de individualização do cliente. Quer dizer, se o fato de você usar o número do aparelho telefônico, ou da linha telefônica — não existe mais linha, mas usando esse jargão do STFC —, se você usar o número do telefone para identificar, se isso agrava essa disputa, que a gente já tinha visto aí, entre VoIP e as provedoras de serviços convencionais de voz, as operadoras de telefonia, ou se isso é indiferente.

E tem uma série de outras questões sobre os mecanismos de controle, as possibilidades de se ter acesso, do ponto de vista da Justiça, às informações do Facebook — a gente já conversou mais, Bruno —, mas, especialmente, do WhatsApp.

Então, eu queria fazer uma proposição contrafactual, na verdade. Suponha que nós estamos num ambiente em que não se tem a preocupação de preservar qualquer grau de privacidade. Essa é uma proposição contrafactual, ou seja, que o Estado pode, a seu bel-prazer e a qualquer momento, dispor de todas as informações sobre uma pessoa ou relativas a uma pessoa. Nesse ambiente, Mark, que informações o WhatsApp poderia entregar para o Estado, ou seja, livre de qualquer amarra de princípios de defesa de liberdades? Pense num ambiente em que o Estado tudo pode. O que é que pode a tecnologia do WhatsApp hoje entregar para o Estado, caso ele precise?

Bruno, com relação ao Mark, na fala dele, ele fez referência e remeteu você à questão dos cumprimentos de tratados internacionais, de convenções internacionais.

Eu queria que você fosse mais explícito a quais tratados e convenções ele se referia e como eles dialogam com a legislação brasileira, especialmente o Marco Civil da Internet.

Por fim — é curiosidade também, mas acho que serve para as várias perguntas que foram feitas aqui —, o Mark falou que o WhatsApp tem um canal dedicado para essas denúncias, inclusive em caráter emergencial, para algumas ações de polícia, ou ações de *law enforcement*, de exercício do poder de polícia do Estado. A pergunta é: como é que isso funciona e em que medida essa informação está à disposição dos agentes da lei nos vários países em que o WhatsApp funciona? Ou seja, você disse, Bruno, que o Facebook tem também um canal em que, no caso, o policial, ou o agente da lei, pode acessar se ele tiver um mandato, se ele tiver um questionamento. Ele pode enviar para vocês, e vocês respondem. Se tem, como é que funciona também esse do WhatsApp, até para que possamos, esta Presidência, disseminá-lo para os vários agentes da lei que reclamam da dificuldade de abordar o WhatsApp, o funcionamento desse canal.

Era isso, Sra. Presidente.

Obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Com a palavra o Deputado Silas Freire.

O SR. DEPUTADO SILAS FREIRE - Sra. Presidente, só para complementar a nossa participação: vi que o representante do WhatsApp nos deu uma declaração de que há um canal de fato para informação de autoridades, mas não falou da taxação, não falou da vinda desse aplicativo para o Brasil. Achei interessante aqueles que estão na academia dizerem aqui que nós não podemos limitar a Internet — o próprio companheiro Eduardo Bolsonaro. Quero dizer que não é a nossa intenção. Eu acho que a Internet é de livre acesso, tem que ser de livre acesso. Ela precisa ser uma comunicação de livre acesso. Agora, não pode servir de instrumento para crimes.

Depois que eu adentrei esta CPI, eu já me tornei usuário, ou pelo menos acessei, *sites* que não acessava. Conheci realidades da Internet, tipo *deep web*, das quais eu não tinha conhecimento. E lá, se você for me rastrear, vai ver *sites* adultos, *deep web*. E isso não é crime, é liberdade de Internet. Agora, se você usar esses

sites para crimes, você está usando a sua liberdade, a liberdade que a lei tem que lhe garantir, para cometer crimes.

Então, eu acho que nós temos que garantir a liberdade da Internet, garantir, inclusive, de certa forma, um anonimato não para as autoridades, mas para invasores. Temos — esta CPI é para isto mesmo — que dar andamento às garantias de liberdades da Internet, e encontrar meios e caminhos para aprimorar a lei brasileira contra crimes que venham da Internet.

Ver um *site* adulto não é crime. Agora, usar imagens de um *site* adulto, de alguém que não deu permissão, até para compartilhar, já é crime. Então, nós temos que deixar claro aqui que não estamos querendo delimitar direitos nem liberdade de Internet.

O que observamos entre as operadoras e o WhatsApp é uma briga comercial. Na qual esta Casa não pode, não deve e não vai entrar em hipótese nenhuma, embora haja, no meu modo pessoal de pensar, algumas injustiças, não tenham dúvida. Esse não é o nosso papel, não é o papel desta CPI.

E, aí, a pergunta vem ao pessoal da academia, aos dois professores: Em uma ordem judicial, vocês não concordariam que nós encontrássemos meios para acompanhar as pessoas na criptografia, por exemplo, a partir daí? Se alguém está cometendo crime cibernético, usando o sigilo da criptografia, vocês, que defenderam tanto essa forma de comunicação, a partir daí, nós não poderíamos interceptar, encontrar meios de interceptá-la, para combater o crime? Essa seria a pergunta.

Eu anotei outra aqui. Por exemplo: Seria possível copiar as informações de um usuário — pessoal do WhatsApp, por exemplo — a partir de uma ordem judicial? Parece-me que isso já foi feito nos Estados Unidos. O senhor responde sim ou não. Não seria possível separar, após essa ordem judicial, algumas conversas específicas de usuários? Nós temos a convicção de que há compartilhamento, WhatsApp, há ofensas em grupos de WhatsApp. Não seria possível nós, a partir dali, acompanhar? Seria uma das nossas colocações.

Eu queria falar também sobre o Internet.org que pertence ao Facebook. Eu gostaria de saber mais detalhes sobre a Internet, a possível limitação de acessos a conteúdos e o que está associado a essa oferta de Internet, questões que podem

afetar direitos fundamentais, estabelecidos no Marco Civil da Internet, como o direito ao fluxo de livres informações.

Ainda sobre o mesmo assunto, eu queria conectar o mundo. Não é uma meta muito ambiciosa. Exemplo: seria uma meta que está sendo divulgada. O Internet.org será um tipo de aditivo, uma força extra para o Facebook alcançar mais usuários? Também seria outra pergunta. São perguntas teóricas e técnicas que precisamos ter para formar o nosso conceito.

E, aí, volto ao WhatsApp. O WhatsApp, em tese, na criptografia de ponta a ponta, só dá as chaves de segurança para duas pessoas envolvidas na conversa. Mesmo que o WhatsApp seja pressionado... Por exemplo, nesse caso judicial, não tem como? Só dá a chave para essas duas pessoas? Seria basicamente isso.

Eu anotei algumas coisas aqui, mas o andar das falas foi se arrastando, e vamos perdendo aqui. Mas, de qualquer maneira, nos respondendo isso, vai nos ajudar a formatar a nossa ideia. Por favor.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Muito obrigada, Deputado Silas. Vamos voltar aqui para...

O SR. DEPUTADO EDUARDO BOLSONARO - Sra. Presidente...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Claro, Deputado Eduardo.

O SR. DEPUTADO EDUARDO BOLSONARO - Gostaria de fazer uma pergunta direcionada para o Sr. Bruno Magrani, do Facebook.

Quanto a essas falsas denúncias feitas no Facebook, há alguma maneira de controla-las? Por exemplo, aqueles perfis notadamente falsos, os *fakes*, feitos só para denegrir ou derrubar aquele *site,* existe uma maneira de controle nesse sentido?

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Aproveito e faço uma pergunta também para o WhatsApp.

Eu gostaria de saber por que não é disponibilizado para o WhatsApp uma ferramenta que também possa bloquear grupos. É apenas se pode bloquear pessoas e não grupos.

Vou deixar essa pergunta. Acredito que todas foram também contempladas aqui pelos nobres Deputados.

Então, concedo a palavra, para iniciar, ao Sr. Mark Kahn, Vice-Coordenador Jurídico Geral do WhatsApp.

O SR. MARK KAHN - *(Exposição em inglês.)*

O SR. DEPUTADO EDUARDO BOLSONARO - Sra. Presidenta...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Com a palavra o Deputado Eduardo Bolsonaro.

O SR. DEPUTADO EDUARDO BOLSONARO - Gostaria só de saber do Sr. Mark se ele teria os números de quanto o WhatsApp rende aos cofres públicos através de tributos. Se, por acaso, ele teria esse número com ele.

O SR. MARK KAHN - *(Exposição em inglês.)*

O SR. DEPUTADO EDUARDO BOLSONARO - Perfeito.

Indubitavelmente, o WhatsApp acelera a nossa economia. Qualquer coisa que acelere os meios de transporte ou os meios de comunicação também o faz.

Quero deixar claro que sou contra uma tributação de maneira 100% igualitária, como ocorre com as tradicionais operadoras telefônicas, até porque eu não quero que o consumidor pague a mais para ter esse serviço, porque, inevitavelmente, seria repassado a ele, mas começo a pensar que seria saudável, sim, um debate nesta Casa. Já vejo amigos meus deixando de usar a telefonia celular para usar as ligações através do WhatsApp. Além disso, com certeza, é interessante para o WhatsApp ter o aplicativo aqui no Brasil. Quero só deixar registrado este tema.

Como bem dito pelo Prof. Moncau, sobre WhatsApp, Airbnb, Uber, está na hora de esta Casa começar, sim, a debater esses temas e começar a regulá-los, porque tem havido muitos problemas nas Justiças locais.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Deputado Eduardo Bolsonaro.

Concedo a palavra ao Sr. Bruno Magrani.

O SR. BRUNO MAGRANI - Obrigado, Sra. Presidente.

Só aproveitando o gancho do que o Deputado Bolsonaro mencionou, mais uma vez, como representante do Facebook e de uma empresa de aplicação de conteúdos, quero reforçar que acreditamos que, conforme as pessoas contratam planos de dados para acessar Facebook, WhatsApp, Twitter, etc., criam-se

incentivos econômicos enormes para as empresas de infraestrutura oferecerem seus serviços. Então, achamos que o próprio fato de as pessoas acessarem a nossa plataforma gera um valor enorme para as empresas de telecomunicações.

Mas, indo às questões que me foram endereçadas especificamente, vou começar pelas questões do Deputado Paulo Lustosa. Primeiro, falarei sobre a questão dos tratados internacionais e do Marco Civil. Um dos grandes desafios com que empresas globais se deparam é a questão de potenciais conflitos de lei. Se você opera em diversas jurisdições e uma jurisdição diz que você tem que fazer X e a outra diz que você não pode fazer X, como é que você resolve essa questão?

Eu vou colocar para V.Exas. um exemplo bastante concreto que existe no Marco Civil. Esse foi um exemplo que trouxemos para diversos Parlamentares desta Casa na época: a questão da retenção de dados.

O Prof. Pablo Cerdeira inclusive mostrou um vídeo em que um ativista alemão se colocava de maneira contrária à diretiva de retenção de dados na União Europeia. Essa diretiva eventualmente foi considerada ilegal e, nesse ponto específico, o Marco Civil acabou criando uma obrigação potencialmente contraditória para empresas que têm operações nas duas jurisdições. Ou seja, a diretiva lá fora, hoje em dia, fala que você não pode guardar os dados ou que não tem a obrigação de guardar os dados. Mais do que isso, a diretiva de proteção de dados fala que as empresas têm a obrigação de deletar os dados, se assim for solicitado pelos usuários, enquanto aqui, no Brasil, existe a obrigação de retenção desses dados por até 6 meses. Então, você cria aí uma situação. Eu não tenho uma resposta de como se resolve isso, mas acho que, eventualmente, o Judiciário vai ter que se deparar com essa questão.

O que o Facebook tem feito nessa área de tratados internacionais, para diversos pedidos que são feitos, é: muitas vezes, quando as empresas só têm sede nos Estados Unidos, pode-se eventualmente ter que solicitar esses conteúdos através dos tratados de cooperação internacional de autoridade de investigação. Por exemplo, esses são os tratados que hoje em dia a autoridade policial brasileira usa para requisitar informações de bancos na Suíça ou de bancos em outras jurisdições. Então, é um mecanismo que tem sido utilizado. Não tenho a data de quando ele foi

efetivamente aprovado, mas tem sido utilizado por muito tempo, porque tem funcionado.

No caso específico da Internet, entendemos que alguns desses tratados ou a forma como alguns países têm implementado esses tratados tem criado dificuldades para autoridades de investigação. O Facebook, por exemplo, tem pressionado bastante o governo norte-americano, especialmente o Departamento de Justiça norte-americano, para acelerar eventuais análises de pedidos de dados e criar, eventualmente, mecanismos que possibilitem que determinadas jurisdições não precisem passar por processos burocráticos como os que existem hoje em dia, em diversos casos, para ter acesso a esses dados.

A segunda questão é sobre o que foi levantado pelo Deputado Eduardo Bolsonaro em relação às denúncias, ao controle dos *fakes* e às denúncias eventualmente falsas. Foi superimportante V.Exa. levantar essa questão, porque me permite esclarecer um ponto importante de como o Facebook funciona.

No Facebook, se você faz uma denúncia ou 5 milhões de denúncias é a mesma coisa. Isso não faz a menor diferença do ponto de vista de análise daquele conteúdo. Mais do que isso, potencialmente, se faz alguma diferença, a diferença é: se você denuncia o conteúdo uma vez, alguém do Facebook vai olhar aquele conteúdo e vai decidir se ele viola ou não as políticas. Vamos supor que essa pessoa da equipe de análise do Facebook tenha olhado aquele conteúdo e tenha determinado que aquele conteúdo não viola as políticas e que vai ficar no ar. Se ele é denunciado mais uma vez, a pessoa vai olhar mais uma vez. Se ele é denunciado pela terceira vez, talvez alguém vá olhar mais uma vez. Quando é denunciado 10, 20, 30, centenas, milhões de vezes, eventualmente, se aquele conteúdo está ali de maneira estática, se não houve nenhuma mudança, a lógica da empresa é: isso aqui já foi avaliado diversas vezes, pessoas diferentes analisaram e identificaram que esse conteúdo não viola as políticas do Facebook. Não tem por que ele ser avaliado novamente. Então, se faz alguma diferença, a diferença é: se o mesmo conteúdo é denunciado várias vezes, a partir de um certo número de denúncias, isso pode não servir para nada.

O SR. DEPUTADO EDUARDO BOLSONARO - E aquele selinho que vem na página, dizendo que o Facebook conferiu e, de fato, é uma página oficial, interfere em alguma coisa nessa análise?

O SR. BRUNO MAGRANI - Não. Na verdade, a única coisa em que pode eventualmente influenciar não é na análise propriamente dita, mas na questão de que o Facebook só dá aquele selo quando tem certeza de que aquela página pertence a uma pessoa que foi identificada. Por exemplo, parte do meu trabalho aqui, nesta Casa, é interagir com os Parlamentares e ter certeza, por exemplo, de que aquela página específica do Facebook pertence a determinado Parlamentar.

Esse selo de verificação possibilita que o usuário final saiba que está interagindo efetivamente com a página daquele Parlamentar, daquela celebridade ou daquela figura pública. Por exemplo, se houver uma denúncia de que aquele é um perfil *fake*, vamos saber que aquilo ali não procede.

Por fim, eu queria agradecer também ao Deputado Silas Freire pela pergunta que foi feita sobre o Internet.org. Esta Casa já promoveu inclusive uma audiência pública para debater o projeto. Eu tive a oportunidade de participar dessa audiência pública e quero esclarecer um pouco mais sobre ele. Acho que é sempre bom ter mais oportunidades para falar e explicar melhor um pouco o projeto. A melhor maneira de entender o Internet.org é pensar em um dos problemas que ele visa resolver. O problema que ele visa resolver é o da conectividade.

Quando o Facebook se deparou com os dados sobre conectividade, globalmente, o quadro que nós vimos foi o seguinte: existem 7 bilhões de pessoas no mundo, em torno de dois terços da população não estão conectados e somente um terço da população está *on-line*. Ou seja, estamos falando de em torno de 4 bilhões de pessoas que não têm acesso à Internet.

Quando você começa a analisar um pouco melhor, questiona por que essas pessoas não têm acesso à Internet. Você vê que, desses 4 bilhões — não tenho os dados específicos de cabeça —, uma grande parte não tem acesso porque não pode pagar e porque não conhece Internet, nunca acessou a Internet. Outra categoria dessas pessoas pode pagar, mas não vê o valor que a Internet tem para a vida delas.

Primeiro, nós detectamos esses dados, essa realidade, esse contexto no âmbito global. Quando começamos a analisar os dados, no Brasil, vimos, uma situação semelhante. Se V.Exas. virem a pesquisa de mídia da SECOM, que é feita todo início do ano, tem um dado lá, tem uma pergunta que foi feita para mais de 3 mil pessoas no Brasil. Para as pessoas que disseram não ter acesso à Internet a pergunta era a seguinte: "Por que você não acessa a Internet?" Razão nº 1: "Não vejo necessidade de acessar a Internet". Razão nº 2: "Não sei como usar o computador". Razão nº 3: "É muito caro acessar Internet. Eu não tenho dinheiro para acessar a Internet".

Então, se pararmos para analisar esses dados, os números 1 e 2 — "Não sei usar o computador" e "Não vejo necessidade de usar Internet" — podem ser categorizados nessa questão de que as pessoas não têm conhecimento ou não veem a importância da Internet para a vida delas. Eu não falei, na verdade, quais foram os percentuais, mas, nessa primeira pergunta, em torno de 43% das pessoas que não tinham acesso à Internet disseram que não viam necessidade. Essas perguntas não eram excludentes, eles poderiam assinalar várias delas. Em segundo lugar, com 37%, era essa de que não sabia usar o computador e, em terceiro, em torno de 20%, é que não tinha condições financeira para acessar a Internet.

Então, vimos que, no Brasil, também uma parcela significativa da população dispõe dos recursos para acessar a Internet, mas simplesmente não vê a necessidade de fazê-lo. Ou seja, não conhece os benefícios e o potencial de transformação que a Internet pode ter na vida dela.

Do ponto de vista negocial, para o Facebook, seria muito cômodo simplesmente manter os acordos ou manter a prática de algumas operadoras, de oferecer Facebook gratuito, de não debitar o Facebook do plano de dados das pessoas. Do ponto de vista comercial isso bastaria. Mas, o Facebook está interessado, mais uma vez, como eu falei, no ecossistema da Internet.

Então, acreditamos que as pessoas precisam descobrir o valor da conectividade da Internet. E a forma de fazer isso é ir além do que simplesmente acessar o Facebook. Achamos que o Facebook é uma parte importante disso. E o Internet.org dá esse passo adicional, oferecendo uma plataforma aberta em que qualquer desenvolvedor, principalmente brasileiro, pode desenvolver aplicativos para

serem oferecidos de maneira gratuita para essas pessoas. Aí, temos critérios técnicos somente que essas pessoas têm de utilizar.

Esses critérios técnicos são: você tem de ser eficiente do ponto de vista de dados. Ou seja, entendemos que as operadoras que oferecem esse serviço o fazem de maneira gratuita. O Facebook não paga às operadoras para fazer isso. As operadoras não pagam nada para o Facebook. Os desenvolvedores não pagam nada. Então, entendemos que ele tem de ser eficiente do ponto de vista de dados. Se começar ocupar muita parte da banda das operadoras, não vai fazer sentido comercialmente para ela.

O segundo critério é que, eventualmente, estimule o acesso à Internet como um todo. Ou seja, não queremos que o sujeito fique somente ali, naquele espaço gratuito. Queremos que ele efetivamente se torne um consumidor pago no futuro, porque estamos visando esse público do meio, esse público que tem capacidade econômica para pagar, mas que, eventualmente, não conhece os benefícios da conectividade.

Quer dizer, o projeto tem sido muito bem sucedido ao redor do mundo. Nós já o lançamos em torno 29 países. Os dados que vimos em conjunto com as operadoras parceiras foram surpreendentes. Nós vimos que as pessoas migram em torno de 50% mais rápido para o plano pago, quando elas acessam através do Internet.org. Mais do que isso, cerca de 50% dessas pessoas que têm o Internet.org também têm o plano cheio da Internet como um todo. Nem para o Facebook, nem para operadora faz sentido se o sujeito ficar naquela área livre, senão a operadora vai começar a perder os incentivos econômicos e não vai continuar oferecendo.

Para finalizar, a versão do Facebook que está disponível, dentro dessa parte que agora chamamos de Freebasic, novo nome desse serviço, não tem publicidade, e o Facebook tem uma coleta muito limitada dos dados. Só são coletados dados agregados para saber quais são os serviços mais populares. Então, mais uma vez, para o Facebook, do ponto de vista comercial, não faria nem sentido focar só no Freebasic. A ideia é o ecossistema mais amplo de acesso à Internet.

Com isso, encerro a minha fala.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Bruno.

Vou passar a palavra ao Sr. Pablo, em função do horário do seu voo. Ele tem uma pergunta para ser respondida.

Concedo a palavra ao Sr. Pablo de Camargo Cerdeira.

O SR. PABLO DE CAMARGO CERDEIRA - Obrigado.

Deputado Silas Freire, quanto à questão da violação pelo *man-in-the-middle*, aquela estratégia de a pessoa no *mail* conseguir interceptar comunicação criptografada, há modelos que permitem isso, mas se formos lembrar do modelo original que a nossa Constituição colocou no art. 5º, X e XII, estabelecendo a inviolabilidade da comunicação, especialmente da de dados — a telefônica tem a exceção, salvo em último caso, inclusive, tem a regulamentação específica para o caso de violação telefônica —, havia uma razão. Lá atrás, havia uma razão, que continua valendo até hoje. A telefônica, especialmente quando feita no STFC, no serviço analógico, lá atrás, através de pulsos elétricos no fio, não havia como se recuperar depois. Então, o modelo era esse. Precisávamos interceptar para poder fazer a prova, no caso específico.

No caso da Internet, essa relação se inverte, porque quase fica registrado. Mesmo a comunicação, no final, em uma das pontas, quando você tem dois comunicantes — um comunicante e um comunicado numa relação —, para alguém conseguir ler e aquilo efetivamente virar uma comunicação, enfim, virar um crime, virar uma foto que não deveria ter circulado, virar um texto ofensivo, alguém precisa decriptografar isso na ponta.

Então, é possível pegar na ponta, sim. O receio é a violabilidade da comunicação na Internet... Se fôssemos pensar no meio analógico antigo, se, de repente, de um mês para o outro, de um ano para o outro, alguém resolvesse interceptar todas as comunicações telefônicas de um país, não teria braço, não teria estrutura física para isso. Ele precisaria de pessoal, precisaria de equipamento, precisaria de uma infraestrutura. Enfim, não se consegue crescer dessa forma. No caso de uma violação de comunicação totalmente digital, nesse meio em que estamos, isso é muito mais fácil de acontecer, como vimos nos casos dos vídeos que passei.

Então, o risco para manutenção do nosso modelo de liberdade de expressão de comunicação, caso se viole, se permita com muita facilidade, a violação da

comunicação digital, é simplesmente a preocupação pelo potencial de escala. É o mesmo potencial que fez com que o Facebook, em 5 anos, saísse de um quarto de faculdade e tivesse bilhões de usuários no mundo. Essa mesma escala que a Internet permite crescimento econômico, aumento de base de clientes, d consumidores, de usuários, pode permitir também para o mal. Essa é a maior preocupação que eu tenho, uma preocupação minha, não necessariamente... Outras formas de ver a questão são absolutamente legítimas. E há quem diga que isso vai baratear muito o custo de investigação. Amplia para casos que não poderiam ter sido descobertos antes, acelera a investigação, também. Esses casos da Paulista, enfim,... Há argumento para os dois lados. Eu, particularmente, neste caso, prefiro ficar com a preocupação em manter a liberdade de comunicação.

Com relação à questão do Deputado Lustosa, de responsabilidade civil, os casos mais simples são complicados. Quando envolve Internet, em que questões que ultrapassam fronteiras, empresas que não estão no Brasil, mas que prestam serviços, porque prestam globalmente, dificilmente vamos conseguir uma resposta que se aplique a todos os casos. Enfim, acho que isso vai muito de uma construção jurisprudencial, uma construção com o Judiciário, caso a caso, em cima de uma legislação que já temos que é bastante boa, bastante moderna, nesse aspecto.

Essa era a minha contribuição. Eu queria agradecer muito, pedir desculpas e licença, porque meu voo já parte logo mais. De qualquer forma, estou à disposição desta Casa sempre que preciso. Por favor, precisando de qualquer suporte nosso, estou à disposição.

Muito obrigado. Boa noite!

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Muito obrigada. Nós é que agradecemos.

O SR. PABLO DE CAMARGO CERDEIRA - Enfim, eu estou à disposição aqui, caso algum Deputado precise de algum esclarecimento. Se não, eu vou indo.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Mais uma vez, muito obrigada.

O SR. PABLO DE CAMARGO CERDEIRA - Muito obrigado, Presidente.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Concedo a palavra ao Sr. Alexander Castro.

O SR. ALEXANDER CASTRO - Eu só tenho uma pergunta, a do Deputado Paulo Henrique Lustosa, sobre o BCP 38. O BCP 38 é um padrão de filtragem de pacotes, padronizado pelo Internet Engineering Task Force — IETF, que é uma solução para evitar ataques nas redes, para se poder tirar um acesso. Tira-se do ar, às vezes, um *site* ou um determinado serviço ou aplicação, usando-se um grupo de endereços IP. Usando essa técnica, consegue-se eventualmente derrubar alguns serviços.

O que eu posso dizer agora, Deputado, é o seguinte: na discussão com o CGI — Comitê Gestor da Internet, quando o CGI estava preparando o seu documento com as recomendações para a quebra de neutralidade — porque filtrar pacotes é a quebra de neutralidade — como a lei dizia que havia a possibilidade de um decreto da Presidenta regulamentando as exceções à neutralidade e que o CGI seria ouvido na discussão — e nós temos assento no CGI, o Presidente do Sindicato, Eduardo Levy, faz parte do Conselho do CGI —, nas discussões ficou colocado como uma regra básica, um princípio básico, que qualquer situação notória de agressão à rede, à segurança, à estabilidade e à integridade das redes, é passível de quebra de neutralidade. E foram citados alguns exemplos. Não eram exaustivos, mas foram colocados no documento. Um deles foi o DDOS, que é uma solução, é o BCP 38. E foi colocado claramente: *"São exemplos de situações notórias de segurança de rede em que serão permitidas práticas de discriminação"* de rede *(...): "Filtragens de endereços IP específicos para mitigação de DDOS"*, que é essa solução.

Agora, se de todas as empresas de telecomunicações estão usando essa técnica, eu não sei lhe dizer agora. Eu sei que, na verdade, a responsabilidade pela segurança, estabilidade e integridade das redes é das empresas. Então, elas têm o maior interesse. Agora, de repente, se há uma empresa que entende que há outro padrão, outra ferramenta que pode usar, pode fazê-lo.

Mas, de qualquer forma, nós do sindicato, junto com todas as empresas, tivemos essa preocupação de colocar para discussão no CGI, entre os conselheiros do CGI, a possibilidade — e acabou passando — de inserir essa possibilidade, como um caso claro de exceção à neutralidade de rede.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada.

Concedo a palavra ao Sr. Luiz Fernando Moncau.

O SR. LUIZ FERNANDO MONCAU - Obrigado.

Tirando o que o Pablo já endereçou aqui, acho que ficou faltando uma última questão, que é referente à questão de os termos de uso frequentemente se isentarem da responsabilidade e de quem é a responsabilidade no caso de vazamento de dados e no tratamento de dados, etc. e tal.

O Brasil está num processo de construção do seu marco regulatório sobre proteção de dados pessoais. Temos algumas regras esparsas que tratam do assunto, mas não uma norma específica que cuide disso e que valha não só para o ambiente digital, mas também para o ambiente *off-line*, porque o Anteprojeto de Lei para a Proteção de Dados Pessoais vale também para aqueles dados que são coletados muitas vezes em relações *off-line*, dados, por exemplo, da operadora de plano de saúde, que tem muitos dados sobre nós, como consumidores.

O fato é que nesse anteprojeto de lei há algumas categorias importantes. Em primeiro lugar, define o que é dado pessoal e o que não é, quem é o responsável pelos dados pessoais, quem é o operador dos dados pessoais. E prevê uma série de hipóteses e situações que já se tornaram corriqueiras no dia a dia ou nas práticas comerciais de hoje em dia, e que merecem atenção. Por exemplo, temos um custo para fazer armazenamento de dados aqui no Brasil. Então, podemos imaginar uma empresa brasileira que capture dados dos consumidores *on-line* e não queira armazenar esses dados no Brasil; e queira armazenar esses dados em países onde esse armazenamento seja mais barato, e não necessariamente tenha regras de proteção à privacidade tão boas quanto as do Brasil. Esse é um debate muito grande entre Estados Unidos e Europa, e você tem algumas regras específicas sobre transferência internacional de dados nesse anteprojeto de lei.

Então, acho que tudo isso vai ficar mais claro quando conseguirmos ter um marco regulatório sobre proteção de dados pessoais. Lá, por exemplo, está escrito que o responsável pelo tratamento de dados pessoais responde pelo vazamento ou qualquer outro dano que venha a causar, quando ele for fruto da sua atividade comercial, etc. e tal.

(Não identificado) - Essa responsabilidade não pode ser transferida.

O SR. LUIZ FERNANDO MONCAU - Exatamente, essa responsabilidade não pode ser transferida. Houve até um novo texto que foi liberado agora pelo Ministério

da Justiça para esse fim, para fins de debate público, também. Então, esse é um debate bastante atual da agenda.

Sobre a questão da criptografia, acho que o Pablo mencionou algumas alternativas. Eu gosto de usar o raciocínio da Lei de Interceptação Telefônica e me alio ao Pablo um pouco em relação a onde estão as minhas preocupações. A Lei de Interceptação Telefônica trata de quais são as hipóteses em que você pode quebrar o sigilo telefônico e fazer uma interceptação. Então, ela fala:

> *"Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:*
>
> *I – não houver indícios razoáveis da autoria ou participação em infração pena;*
>
> *II – a prova puder ser feita por outros meios disponíveis;*
>
> *III – o fato investigado constituir infração penal, punida, no máximo, com pena de detenção.*

Então, temos alguns critérios aqui para dizer: não vamos invadir as comunicações dos cidadãos, a não ser que seja um crime, um crime com uma pena alta, em que existam fundados indícios de que seja aquela pessoa específica e que a prova não possa ser feita por qualquer outro meio.

Eu acho que esse *framework* que está desenhado aqui para a Lei de Interceptações, ele poderia nos orientar. Às vezes, muito pouca coisa do mundo analógico, do mundo dos anos 90, pode ser utilizada para o mundo digital, mas eu acho que isso aqui é uma das coisas que podemos aproveitar. Não deveríamos usar toda essa capacidade que a tecnologia dá de se imiscuir na vida dos cidadãos para buscar solucionar qualquer problema, às vezes até um ilícito civil, utilizar esse tipo de expediente para solucionar esse tipo de questão. Então, é um pouco de como eu vejo essa situação.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Muito obrigada.

Com a palavra o Deputado Paulo Henrique Lustosa.

O SR. DEPUTADO PAULO HENRIQUE LUSTOSA - Sra. Presidente, só a título de sugestão, aproveitando muito do que nós ouvimos aqui, e para V.Exa.

avaliar, na condução aqui da Comissão, há dois aspectos que me chamaram atenção e que eu acho que a Comissão poderia, de alguma forma, avaliar a possibilidade de se engajar nesse processo.

Um deles, como o Moncau acabou de mencionar, é o Ministério da Justiça estar em pleno processo de discussão dessa regulação da questão dos dados pessoais, e eu acho que isso dialoga diretamente com parte do que é discutido e que gerou preocupações aqui na Comissão. Talvez pudesse sair uma recomendação para o Presidente da nossa Comissão de Ciência e Tecnologia, para que, no próximo ano, nós tivéssemos uma subcomissão ou um grupo de trabalho dentro da CCTI que acompanhasse essa discussão, para que, quando a matéria chegasse à Casa, não nos pegasse de surpresa ou desinformados quanto ao andamento.

A outra questão também a avaliar é que muito da discussão de hoje rodou em torno do fato de o WhatsApp não ter sede no Brasil e das dificuldades que isso gera para que os operadores do direito consigam cumprir suas missões. E foi informado pelo representante da empresa que eles estão num processo de diálogo com operadores de direito para melhorar esse diálogo.

Eu também sugeriria, para a avaliação de V.Exa., se esta Comissão — e, aí, como um resultado prático do trabalho desta Comissão — não poderia também participar e acompanhar esse processo para manter os nossos pares... Porque essa preocupação que foi levantada aqui pelos vários colegas não é restrita aos membros desta CPI. Vários colegas no plenário, ao discutir essa matéria, levantam essa mesma preocupação. Então, talvez isso fosse interessante, para que nós pudéssemos dar um retorno para os nossos pares sobre os avanços e dificuldades, o que acaba sendo, de certa maneira, um resultado concreto da presidência de V.Exa. nesta Comissão.

Obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Eu que agradeço. Muito obrigada, Deputado Paulo Henrique Lustosa. Agradeço a todos os Deputados também.

E quero agradecer aos nossos convidados, que vieram somar com esta Comissão; ao Sr. Mark Kahn, que não mediu esforços para estar aqui, já tinha

procurado esta Comissão mesmo no mês de outubro, esteve sempre dando a atenção devida; ao Sr. Bruno Magrani. Quero agradecer também ao Sr. Alexander Castro, ao Sr. Luiz Fernando Moncau e também ao Pablo de Camargo Cerdeira, que teve que se retirar.

Quero agradecer, ainda, a todos os Deputados, que não mediram esforços para conseguirmos ampliar os trabalhos por 60 dias, a todas as pessoas que vêm trabalhando, aos nossos consultores, funcionários da Casa, que conseguiram, juntos, esse adiamento por 60 dias.

Quando a CPI teve início, Deputado Paulo, vimos que eram tantos assuntos... Acabamos criando essas condições de formar sub-relatorias, para poder falar e abranger um assunto que é tão novo, relacionado à Internet. V.Exa., que já participou de outros debates aqui nesta Casa, sabe bem disso. Cada vez que estamos discutindo, novos assuntos vêm. E nós não imaginamos a velocidade que a Internet tem.

Então, estou feliz de saber um pouco mais sobre esse assunto, que, confesso, também é muito novo para mim. A cada dia mais, nós aprendemos mais sobre ele. Eu acho que, principalmente na vida pública, temos que ter humildade para poder aprender. E aqui temos um grande aprendizado, com as pessoas que se colocam à disposição para vir aqui falar um pouquinho sobre esse assunto. E agora, Deputado Silas, vamos ter condição de poder trazer mais assuntos para serem debatidos. V.Exa. tem ideias fantásticas!

No decorrer desta CPI, conseguimos fazer algumas denúncias. Houve casos até mesmo em que pessoas foram presas pela Polícia Federal, com denúncias até de dinheiro público sendo investido em alguns *sites* piratas, que não tinham essa divulgação. E foi dada ampla divulgação, e até mesmo foi feita a denúncia aqui, através desta Comissão Parlamentar de Inquérito.

Nós vemos que os assuntos são tantos... O Deputado Silas Freire hoje foi bem feliz em sua fala, quando disse que a pessoa tem a liberdade de expressão e de uso, mas que não pode também chegar ao momento de cometer um crime contra a sociedade e de trazer riscos.

E hoje vemos a preocupação tanto do Facebook quanto do WhatsApp em relação a ter uma segurança maior, a dar uma privacidade aos dados das pessoas.

Vemos que, cada vez mais, o Facebook também tenta criar mecanismos para tentar facilitar. Então, nós ficamos felizes por isso. Eu acho que nós temos que ter liberdade de expressão, mas, sem dúvida alguma, também dar segurança aos nossos usuários.

Então, agradeço. Vamos aguardar essa votação no Plenário. Como deram palavra o Presidente e todos os Líderes desta Câmara, nós aguardamos que se leve esta votação ao Plenário, para aprovarmos os 60 dias e podermos debater esses temas durante esses 60 dias. Então, mais uma vez, muito obrigada a todos.

Nada mais havendo a discutir, declaro encerrada esta audiência, já convocando reunião para a próxima quinta-feira.

Muito obrigada a todos. Boa noite.

TEXTO ESCRITO E EM PORTUGUÊS DO DISCURSO PROFERIDO PELO SR. MARK KAHN — VICE-COORDENADOR JURÍDICO GERAL DO PROVEDOR WHATSAPP, ENCAMINHADO AO DEPARTAMENTO DE TAQUIGRAFIA, REVISÃO E REDAÇÃO PELA COMISSÃO PARLAMENTAR DE INQUÉRITO DE CRIMES CIBERNÉTICOS. O TEXTO NÃO É DE RESPONSABILIDADE DO DETAQ.

Depoimento WhatsApp (português)

Obrigado pela oportunidade de conversar com vocês hoje sobre o WhatsApp. Meu nome é Mark Kahn e sou Vice-Diretor jurídico do WhatsApp. Hoje eu quero tratar sobre como o WhatsApp funciona, como as pessoas no Brasil o utilizam para se conectar com seus amigos e familiares, e quais medidas adotamos para proteger a segurança e a privacidade dos nossos usuários.

Introdução

O WhatsApp foi fundado em 2009 com o objetivo de oferecer um serviço global de troca de mensagens através de diferentes plataformas móveis. Nossa aplicativo permite que pessoas que nunca estiveram *on-line* antes possam se comunicar com outras pessoas que são importantes para elas.

O WhatsApp oferece uma forma rápida e fácil para as pessoas enviarem massagens uma para as outras e para se comunicarem com pequenos grupos familiares e amigos. Atualmente, a partir do nosso escritório em Mountain View, na

Califórnia, o WhatsApp oferece o seu serviço a mais de 900 milhões de usuários ativos em todo mundo e possibilita a transmissão de mais de 30 bilhões de mensagens por dia através dos nossos aplicativos em diversas plataformas móveis incluindo dispositivos Android, IOS, Windows Phone, BlackBerry e Nokia. Recentemente, começamos a oferecer às pessoas a capacidade de fazer chamadas de voz gratuitas entre usuários do WhatsApp, quer eles sejam vizinhos ou vivam em países diferentes.

O WhatsApp não requer que os usuários tem alguma assinatura para usar o serviço e não há publicidade em seus produtos. A oferecer o WhatsApp gratuitamente para os nossos usuários, acreditamos que facilitamos a comunicação em tempo real com amigos e familiares para um vasto número de pessoas. Mais à frente neste meu depoimento, vou tratar em mais detalhes como no serviço funciona.

O WhatsApp foi adquirido pelo Facebook em 2014, mas opera de maneira independente tanto do Facebook Inc. quanto do Facebook Serviços Online do Brasil. O WhatsApp tem em torno de 110 funcionários, todos alocados em Mountain View, na Califórnia.

O WhatsApp no Brasil

É uma honra para o WhatsApp oferecer seu serviço para dezenas de milhões de usuários todos os dias no Brasil, um serviço que está definindo a forma como milhões de brasileiros se comunicam e interagem.

A fim de servir aos brasileiros da melhor forma possível, traduzimos todos os nossos serviços para o português. Também dispomos de uma equipe de atendimento aos usuários que fala português do Brasil para dar suporte aos usuários do seu país.

À medida que mais e mais pessoas passam utilizar o WhatsApp do Brasil, nós ficamos cada vez mais fascinados ao perceber a maneira criativa, inovadora como elas têm usado o serviço. Quanto nossos fundadores criaram o WhatsApp, não acho que eles poderiam imaginar as maneiras fantásticas como os brasileiros utilizam o WhatsApp.

Milhões de brasileiros usam WhatsApp principalmente para se comunicar com seus amigos, familiares e pessoas queridas. Um exemplo que ilustra esse tipo de

uso é o projeto desenvolvido pela unidade de oncologia pediátrica do Hospital Amaral Carvalho, no Estado de São Paulo. Reconhecendo que um dos maiores desafios enfrentados por seus jovens pacientes é a solidão por estarem desconectados de seus amigos e familiares durante tratamento, o hospital começou a oferecer às crianças hospitalizadas ursos de pelúcia equipados com o WhatsApp, apelidados de “Elos”. Pais, parentes e amigos que de outro modo estariam distantes podem gravar e enviar mensagens de voz ao urso de pelúcia através do WhatsApp, e assim os pequenos pacientes em tratamento contra o câncer no hospital podem se sentir mais reconfortados ao ouvir vozes familiares com mensagens de carinho e apoio.

O WhatsApp também tem sido utilizado para ajudar no combate à epidemia de dengue. A Secretaria de Saúde do município de Itaberaba estabeleceu uma conta de WhatsApp através da qual os cidadãos são estimulados a utilizar para informar a Secretaria de Saúde sobre a existência e a localização de terrenos baldios e focos de água parada que podem estar servindo de criadouro para os mosquitos que transmitem a dengue.

O WhatsApp também tem trabalhado com empresas brasileiras para criar mais valor para as pessoas no Brasil. Especificamente, o WhatsApp tem firmado parcerias com operadoras de telefonia móvel para tornar os planos de dados e consequentemente o acesso a serviços de Internet mais acessíveis para as pessoas no Brasil e no mundo. Sem planos de dados acessíveis, as pessoas podem permanecer relutantes para utilizar seus aparelhos celulares, o que dificulta o contato entre elas.

Mais de 130 operadoras de telefonia móvel ao redor do mundo já firmaram parceria com WhatsApp para oferecer pacotes de dados que incluem acesso ao WhatsApp, o que mostra como essas parcerias são favoráveis tanto para os usuários quanto para as operadoras. O WhatsApp e as operadoras de telefonia móvel não pagam uns aos outros qualquer quantia em dinheiro como parte destes acordos.

Essas operadoras parceiras nos dizem que como resultado da nossa parceria elas são capazes de manter mais dos seus clientes conectados por mais tempo. E essa melhor conectividade significa mais receitas por usuário para os seus negócios.

Por exemplo, no trimestre seguinte à parceria da TIM com o WhatsApp, eles tiveram um aumento de 4% nas receitas sobre os dados por usuário e um aumento no número de usuários ativos por dia. Essas parcerias beneficiam todos os envolvidos— as operadoras, o WhatsApp e, o que é mais importante, os brasileiros.

Segurança

Agora eu gostaria de abordar como protegemos a segurança e privacidade das pessoas que utilizam o WhatsApp.

O WhatsApp está profundamente comprometido com a segurança das pessoas que usam os nossos serviços. Reconhecemos que questões de segurança, incluindo bullying e outras formas de assédio e perseguição que ocorrem *off-line* estão se movendo para o mundo *on-line*. Gostaria então de destacar três aspectos do nosso programa de segurança.

Em primeiro lugar, um elemento chave do nosso programa de segurança é a educação. Temos o prazer de anunciar que acabamos de lançar uma nova Central de Segurança que oferece ferramentas e estratégias que as pessoas podem adotar para ter uma experiência de uso mais seguro no WhatsApp, incluindo instruções sobre como bloquear um usuário que utilize o serviço para assediar ou perseguir e como entrar em contato com o WhatsApp a respeito de uma situação específica de abuso. Incluímos na Central uma sessão específica para estimular os usuários a refletir sobre o que eles compartilham antes de enviar uma mensagem através do WhatsApp. Também contamos com uma versão em português da Central de Segurança. E o WhatsApp continuará buscando maneiras de aprimorar a Central de Segurança à medida que novos desafios se apresentarem.

Em segundo lugar, o WhatsApp não permite o uso inapropriado ou para fins ilícitos do nosso serviço. Desabilitamos contas de usuários quando tomamos conhecimento de que eles estão envolvidos neste tipo de atividades.

Em terceiro lugar, nós trabalhamos com autoridades de investigação para manter as pessoas seguras. Por exemplo, quando tomamos conhecimento de um caso de exploração infantil na nossa plataforma, seja por meio de uma denúncia feita por um usuário ou por outros meios, nós encaminhamos as informações que tivermos para o National Center for Missing and Exploited Children. Esse centro, também conhecido como NCMEC (“nick-meck”), é internacionalmente reconhecido

por trabalhar com polícias e autoridades da investigação de todo o mundo, inclusive brasileiras, para levar à justiça indivíduos que exploram explorem crianças.

Também reconhecemos a importância de trabalhar mais próximo de autoridades de investigação no Brasil. Apesar de sermos uma empresa muito pequena, estamos priorizando nossos espaços educacionais e de engajamento no Brasil. Em outubro deste ano, eu estive em Brasília e me reuni com parlamentares, incluindo alguns dos membros desta Comissão. Foram reuniões muito valiosas para mim e para o WhatsApp porque nos possibilitou aprender em primeira mão sobre as suas preocupações, as quais estamos trabalhando ativamente para endereçar. Esperamos continuar nosso diálogo para que possamos compreender melhor os problemas que brasileiros estão enfrentando e como podemos resolvê-los da melhor maneira possível.

Segurança e privacidade

Ao mesmo tempo, construímos nossos serviços para colocar a privacidade e segurança dos nossos usuários como prioridade. O WhatsApp desenhou seu serviço com um forte conjunto de princípios de privacidade em mente. Nós coletamos pouquíssimas informações sobre as pessoas que usam o WhatsApp. Apenas um número de telefone móvel é necessário para o registro. As pessoas têm a opção de fornecer um nome e foto do perfil para se identificarem mais facilmente para o seus contatos, mas isso não é necessário e nós não verificamos o nome que nos é fornecido.

Não armazenamos as mensagens que as pessoas enviam umas às outras, e uma vez que a mensagem é entregue aos seus destinatários, ela é armazenada apenas nos aparelhos telefones das pessoas — não retemos cópias ou registros de mensagens entregues em nossos servidores. Isto nos permite oferecer uma experiência mais rápida e mais confiável para as pessoas.

Ameaças de segurança *on-line* representam um enorme e crescente desafio para indivíduos e para empresas. O WhatsApp tem investido de maneira significativa em tecnologias que incorporam tecnologias de criptografia e anti-spam para ajudar a manter os nossos serviços mais seguros.

Criptografia

Gostaria de falar um pouco mais sobre criptografia. Ao longo dos últimos anos, as pessoas começaram a usar a internet para mais e mais coisas — serviços bancários, compras, comunicação, compartilhamento de arquivos — e, com isso, a demanda por mais segurança, incluindo tecnologias de criptografia, também aumentou. Em resposta ao desejo das pessoas por uma segurança digital mais forte, os bancos agora usam a criptografia para proteger os ativos financeiros das pessoas, empresas de cartão de crédito usam criptografia para proteger transações, *sites* de comércio eletrônico usam a criptografia para garantir que as pessoas possam comprar produtos de forma segura, fabricantes de aparelhos usam a criptografia para proteger dispositivos móveis caso eles sejam perdidos ou roubados. A criptografia tornou-se uma maneira comum de proteger a nossa privacidade e segurança na era digital.

A criptografia também se tornou comum em serviços de mensagens e a maioria dos serviços existentes hoje em dia implementaram alguma forma de criptografia como uma medida de privacidade padrão em seus produtos. Como a maioria dos principais aplicativos de mensagens, o WhatsApp utiliza criptografia forte durante a transmissão de mensagens das pessoas para ajudar a garantir que elas não sejam interceptadas ou comprometidas por criminosos. A implementação de criptografia forte significa para o WhatsApp ajudar a garantir que as mensagens enviadas apenas serão lidas por seus reais destinatários. Especificamente, estamos implementando criptografia de ponta-a-ponta, o que significa que apenas o emissor e o receptor dessas mensagens no WhatsApp podem vê-las. Nem o WhatsApp nem qualquer outra pessoa podem ver essas mensagens.

Hoje em dia, ouvimos o tempo todo exemplos de como indivíduos mal-intencionados exploram vulnerabilidade nas redes de comunicações e produtos de consumo. As pessoas podem comprar *malware* e outras ferramentas tecnológicas prontas que permitem a invasão por esses indivíduos mal-intencionados da privacidade das pessoas e que prejudicam a capacidade das pessoas de usar os serviços que elas valorizam.

É por isso que criptografia forte é tão essencial para segurança cibernética e a prevenção dos crimes *on-line* — pois facilita comunicação segura e confiável mesmo frente a essas ameaças. As pessoas no Brasil e no mundo têm demandado

produtos que usem a criptografia necessária para protegê-las de criminosos *on-line*, da vigilância indesejada e de outras ameaças à sua privacidade e segurança.

Formuladores de políticas públicas têm reconhecido o papel importante que a criptografia tem. Michael Chertoff, ex-Secretário de Segurança Nacional dos Estados Unidos, afirmou enfaticamente em um artigo no Washington Post que “o maior bem público é uma infraestrutura de comunicações segura, protegida por criptografia ubíqua em termos de dispositivos, servidores e empresas”.

E recentemente um Ministro de outro grande país explicou publicamente como ele usa o WhatsApp para governar e porque a criptografia do WhatsApp é tão importante: “Eu administro meu Ministério no WhatsApp. Eu aprecio o modelo de criptografia ponta-a-ponta do WhatsApp... Ser um reformista pode ser um pouco intimidante. Você fica na mira de interesses escusos. Você está indo contra máfias. Boa parte de nossa indústria sofre de oligopólio e formação de cartel. Essas pessoas se vingam.”

Nós entendemos que isso é apenas uma de muitas razões pelas quais as pessoas escolhem usar o WhatsApp, mas é importante lembrar que governos, empresas e pessoas são beneficiados quando usam comunicações são privadas e seguras.

Investigações policiais

Como mencionei, o WhatsApp foi inventado para assegurar a proteção e a segurança das pessoas que utilizam nosso serviço, e estamos comprometidos em trabalhar com as autoridades de investigação para ajudar a proteger os cidadãos brasileiros. Nós priorizamos solicitações de emergência e envidamos todos os esforços para responder imediatamente quando há uma situação envolvendo risco imediato à vida de uma pessoa. Na maioria dos casos, como o WhatsApp coleta pouquíssimos dados de seus usuários, isso significa basicamente que conseguimos fornecer o número do telefone. Mesmo nos casos em que temos informações específicas, podemos trabalhar com as autoridades para verificar se existe uma conta.

Nós também respondemos a pedidos feitos por autoridades através de tratados internacionais que permitem a um país solicitar informações de outros países. O Judiciário brasileiro tem reconhecido esse sistema como um mecanismo

válido à luz do Marco Civil para fazer pedidos a empresas norte-americanas. Reconhecemos que às vezes esse não é o jeito mais rápido e eficiente, como as autoridades precisam que seja. É por isso que o Facebook tem trabalhado com outras empresas de tecnologia para melhorar esses sistemas e fornecer mais recursos, mais pessoal e processos mais eficientes e somos fortemente favoráveis a esses seus esforços. Conclusão

Obrigado pela oportunidade de estar aqui hoje. O WhatsApp se orgulha de disponibilizar seu serviço para as pessoas no Brasil e temos o compromisso de garantir a segurança e privacidade dos brasileiros que utilizam a nossa plataforma.

Também estamos comprometidos a continuar a inovar e a desenvolver um produto que contribui para a vida das pessoas. Temos o prazer de oferecer uma forma gratuita, rápida e confiável para que brasileiro se comuniquem com amigos. Seja quando você envia mensagem para seu familiares ou quando uma secretaria de saúde disponibiliza um canal de comunicação com cidadãos, o WhatsApp é parte integrante da forma como os brasileiros se comunicam todos os dias. Por exemplo, há também uma escola na Vila Canária, em Salvador, que desenvolveu um uso realmente inovador do WhatsApp. A escola envia desafios e problemas de matemática através WhatsApp e os alunos respondem com propostas de soluções aos problemas também via WhatsApp. Mas o projeto vai além disso, já que os alunos com dificuldade em encontrar as soluções para os desafios podem enviar perguntas aos seus professores por meio do WhatsApp e receber uma resposta deles rapidamente. Isso tem permitido que a escola identifique quais alunos precisam de mais auxílio pedagógico e quais conceitos têm se mostrado mais desafiadores para a compreensão dos alunos.

Exemplos como este mostram o impacto do WhatsApp no Brasil e esperamos que, conforme a empresa continua a crescer e a inovar, possamos aumentar nossa capacidade de melhorar a vida das pessoas no Brasil. Esperamos continuar a ver as pessoas usarem nossos serviços de maneira criativa e inovadoras para melhorar suas vidas e a vida de suas comunidades. Mais do que isso, esperamos poder continuar a aprender como melhor servir os milhões de brasileiros e brasileiras que utilizam o WhatsApp. Estou à disposição para responder suas perguntas.