SENADO FEDERAL
SECRETARIA-GERAL DA MESA
SECRETARIA DE REGISTRO E REDAÇÃO PARLAMENTAR

REUNIÃO
13/06/2018 - 27ª - Comissão de Educação e Cultura

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Bom dia! Bom dia a cada uma e a cada um!

Havendo número regimental, declaro aberta a 27ª Reunião, Extraordinária, da Comissão de Educação, Cultura e Esporte desta 4ª Sessão Legislativa Ordinária da 55ª Legislatura.

A presente reunião atende aos Requerimentos nºs 20, 36 e 38, de 2018, de minha autoria, junto com o Senador Pedro Chaves, para a realização de audiência pública destinada a debater o tema "A educação digital como meio de prevenção aos crimes cibernéticos".

Dando início à audiência pública, solicito ao Secretário da Comissão que acompanhe os convidados para tomarem assento à mesa, por favor.

Vou chamar os convidados: Dr. Emilio Simoni, Diretor do Laboratório de Segurança da PSafe Tecnologia; Thiago Tavares Nunes de Oliveira, Presidente da SaferNet Brasil; Carlos Oliveira, Ministro-Conselheiro da Delegação da União Europeia no Brasil; Cristhiane Andrade França, Delegada da Delegacia Especial de Repressão aos Crimes Cibernéticos; Paulo Rená, Professor de Direito e Pesquisador de Cultura Digital e Democracia do nosso UniCeub e do nosso Iesb; e Fabricio da Mota Alves, advogado e professor em Direito Digital, Vice-Presidente do Inova Digital e também Vice-Presidente da Comissão Especial de Inovação da OAB/DF.

Eu vou passar a palavra na ordem das chamadas, agradecendo a presença de cada um de vocês.

Quero dizer que esta audiência se insere em algo fundamental no mundo de hoje, que é a descoberta dos crimes digitais, que não existiam 30 anos atrás - talvez, alguns dos senhores especialistas possam identificar mais atrás, mas não existia isso -, e como combatê-los, sobretudo, e como combatê-los em todos os níveis.

Num desses dias, eu vi uma matéria sobre o Enem, e, lá, por trás, havia crime cibernético tentando burlar as provas. Felizmente, o Ministério da Educação tem tido um sistema muito rigoroso para evitar esse tipo de coisa.

No caso do processo eleitoral, nós temos não só na campanha o risco das manipulações, que chamam hoje de *fake news* , mas até mesmo suspeitas, que continuam a existir - devo dizer que não sou um desses -, de que os resultados podem ser manipulados na contabilização dos votos que chegam pelas urnas eletrônicas. Há pessoas que não confiam no sistema, tanto que muitos requerem cada vez mais que haja também o voto impresso, como forma de controle.

O sistema de cobrança de impostos é um lugar onde poderá, sim, haver crimes digitais. No sistema financeiro, tem havido isso bastante. Cada um de nós, de repente, de vez em quando, é vítima desses crimes quando penetram nos nossos cartões de crédito.

Então, esse é um tema que já é muito importante e que vai crescer cada vez mais. Nós escolhemos um grupo de pessoas que, creio, poderão trazer sugestões, análises e respostas a esse problema.

Como sabem vocês, essas audiências têm a cobertura da TV Senado, da Agência Senado, do *Jornal do Senado* e da Rádio Senado e contam com os serviços de interatividade com o cidadão que o Senado mantém, o chamado Alô Senado, através do telefone 0800-612211 e do endereço e-Cidadania, por meio do portal www.senado.gov.br/ecidadania.

Essas reuniões, em alguns momentos, podem ser transmitidas ao vivo, dependendo das outras comissões em andamento, e por outros canais que não são muitas vezes o principal. E vocês que estiverem assistindo a esta reunião podem mandar perguntas, sugestões e comentários.

Eu tenho uma lista de perguntas que deixarei para fazer ao longo do processo em que formos fazendo a audiência. Passo a palavra inicialmente a Emilio Simoni, dizendo que, como são seis, vamos limitar o tempo em dez minutos, mas, quando tocar uma campainha automaticamente, não se assustem nem parem. Continuem elaborando o pensamento. Não vou ficar aqui cortando a palavra. É apenas por uma questão de organização que vamos colocar dez minutos, flexíveis.

Por favor, Dr. Emilio.

O SR. EMILIO SIMONI - Bom dia a todos!

Primeiramente, muito obrigado ao Senador Cristovam pelo convite.

Vou falar um pouco hoje sobre os desafios da área de cibersegurança, muito focada no Brasil.

Sou Diretor do Laboratório de Segurança da PSafe, uma empresa de segurança com foco em *mobile*, brasileira, e todos os números que eu falar aqui hoje estão baseados na proteção dos nossos 21 milhões de usuários ativos.

Eu comecei nessa área profissionalmente em 2003, justamente na época em que se estava estruturando o cibercrime no Brasil. Até então, os cibercriminosos tinham um foco muito grande em invadir servidores e em desfigurar *sites* e se contentavam em somente colocar o seu protesto, o seu manifesto. Aí, em 2003, aconteceu algo muito interessante, que foi a percepção por parte desses cibercriminosos de que eles poderiam fazer enormes quantias em dinheiro se direcionassem seus ataques a instituições bancárias e financeiras. Aí, começou a surgir a estruturação do cibercrime brasileiro.

Justamente nessa época, eu comecei a atuar com foco em segurança digital. Então, eu sou especialista em criação de tecnologias de proteção ao usuário final, contra ataques de cibercriminosos, como, por exemplo, páginas falsas, vírus, *malwares* e até monitores de teclado e *mouse*.

A partir desse momento, então, até 2008, chegando a hoje, o que a gente tem é uma completa estruturação do cibercrime brasileiro, em que há uma área que a gente chama de *underground*, onde esses cibercriminosos se comunicam. Existem verdadeiros mercados negros por trás disso, onde todo tipo de informação é compartilhado, desde dados bancários a credenciais de *e-mails*, de redes sociais, até informações confidenciais, inclusive de políticos e entidades públicas. A informação, conforme sua raridade e o valor que ela tenha agregado, costuma ser mais cara nesse submundo *hacker*. Também são comercializados ali códigos-fontes de ameaças. Quando descobrem uma forma de fraudar um banco novo, essa informação é muito cara e também é vendida.

Então, a gente tem hoje, aqui no Brasil, um dos cenários de cibercrime mais bem organizados do mundo.

E, para entender o que a gente tem hoje, é importante falar um pouco do nosso cenário de conectividade. Quando a gente fala de número de pessoas conectadas à internet, baseados nos números do IBGE do ano passado, há 116 milhões de brasileiros conectados, o que, percentualmente falando, dá um número muito baixo. Somente 65% da população estão conectados hoje, e a gente vai ver que, apesar disso, há números de bloqueios e de ameaças exorbitantes, assustadores, porque, caso se projete esse número que a gente tem hoje na população total do Brasil, haverá números muito maiores.

A população brasileira hoje, em sua totalidade, utiliza serviços de internet praticamente para redes sociais e trocas de mensagens instantâneas, e, em terceiro lugar, vem crescendo, ano a ano, a utilização para serviços bancários, principalmente com aplicativos bancários, já que a gente está em processo de migração dos serviços bancários para os dispositivos móveis, principalmente pela sua facilidade de integração. E o *hacker*, por sua vez, acaba indo atrás disso. O que o *hacker* mais gosta é de dinheiro. Então, o *hacker* vai atacar onde ele vai ganhar dinheiro.

Quando a gente comenta, por exemplo, que, na minha plataforma, não há ataques é porque o *hacker* não tem a percepção de que vai fazer dinheiro naquela plataforma. O *hacker* vai sempre focar onde ele pode ganhar dinheiro.

E, para falar um pouco do nosso cenário atual, baseado nos últimos três anos, a gente começa com 2016, quando a gente teve um total de 66 milhões de bloqueios de ciberataques, e aí estou falando ataques de páginas falsas e ataques de aplicativos maliciosos focados em ambiente androide. Vou explicar daqui a pouco como funciona esse tipo de ataque.

Um fator bem interessante em 2016 é que nasceu um tipo de golpe novo aqui no Brasil. Não sei se vocês sabem, mas o Brasil é um grande exportador de ciberataques - vários deles nascem no Brasil -, justamente pelo avanço tecnológico da nossa área financeira e bancária, o que forçou o nosso *hacker* a também evoluir. Então, em 2016, houve o nascimento de um novo tipo de golpe, que é o que a gente chama de golpe de WhatsApp, golpe de páginas falsas do WhatsApp, e o reflexo disso é que, de 2016 para 2017, a gente teve um crescimento de quase 200% no número de ciberataques no Brasil, fechando o ano de 2017 com 191 milhões de ciberataques. E houve um ataque bem expressivo, que foi o ataque

envolvendo o saque das contas de FGTS inativo, em que, sozinho, a gente teve a marca de dez milhões de bloqueios. Esse foi um dos maiores golpes da história que a gente atingiu atrás desses monitoramentos de golpes, e ele foi um dos responsáveis por esse número bem alto.

Quando a gente fala já de 2018, um pouco mais atual, até maio, a gente teve um total de 97 milhões de bloqueios de ciberataques. A gente projeta que, até o final do ano, será atingido o número de 250 milhões de bloqueios. Esse crescimento se deve a dois fatores principais. O primeiro deles é um número crescente de notícias falsas que vêm sendo disseminadas, e algo que a gente considera importante é considerar uma notícia falsa como algo prejudicial ao usuário, a manipulação da opinião pública como algo prejudicial ao usuário. E esse bloqueio é um dos responsáveis por esse crescimento de número.

A partir do segundo semestre, há outro fator interessante: em novembro, há a Black Friday, uma época em que os *hackers* e os cibercriminosos costumam intensificar os seus ataques, tendo como alvo principal as grandes marcas de *e-commerce*, os grandes varejistas. Eles têm como objetivo o roubo de credenciais bancárias e de números de cartões de crédito.

Falando de forma geral, todos esses ciberataques têm um mecanismo em comum, têm uma estrutura em comum; eles são baseados fortemente em engenharia social. O primeiro passo é o convencimento da vítima da veracidade daquela informação, e esse convencimento é muito intrínseco ao tipo de golpe, à natureza do golpe. Quando a gente fala de golpe de páginas falsas bancárias, são páginas que tentam convencer o usuário de que aquele *link* que ele recebeu é o *link* da instituição bancária ou é o *link* de um *e-commerce*, de forma que, quando o usuário acessar, ele vai acabar tendo prejuízos financeiros.

Quando a gente fala de golpes de WhatsApp, entra algo aí que também veio e que é perceptível com relação ao cibercriminoso: ele entendeu que pode transformar a vítima em um vetor de disseminação do golpe. Isso é algo muito interessante, e é o principal responsável pelo grande número que a gente tem de bloqueios nesse tipo de golpe. O *hacker*, percebendo que a vítima pode ser um vetor de disseminação do golpe, passou a trabalhar no convencimento da vítima de que ela tem de divulgar aquele conteúdo para mais pessoas para que ela tenha acesso a uma suposta vantagem.

Então, no início deste ano, por exemplo, a gente teve vários golpes de WhatsApp envolvendo falsas vagas de emprego. O usuário recebia um *link* de uma suposta vaga de emprego, mas, para se candidatar ou garantir sua vaga, ele teria primeiramente de compartilhar aquele *link*, aquela suposta vaga, com dez pessoas ou com cinco grupos. Aí o que acontece? De um dia para outro, há milhões de acessos em um golpe, e essa foi a grande sacada do *hacker* brasileiro, que passou, inclusive, a exportar, a vender esse *kit* de ataque para outros países.

A partir do momento em que a gente tem um ponto de convencimento, em que o *hacker* tem o assunto, tem o contexto, tem o conteúdo, ele vai cuidar de disseminar aquele golpe, de espalhar aquele golpe. E aí a gente tem dois pontos em comum. O primeiro deles, quanto a gente fala de golpes de WhatsApp e de *fake news*, notícias falsas, o ponto de partida são grupos de WhatsApp, porque hoje pode haver até 250 pessoas em um único grupo. Então, o *hacker*, o cibercriminoso está inserido nesses grupos chaves, joga esse conteúdo lá, e as pessoas que estão lá, sem saber da veracidade ou não daquele conteúdo, acabam repassando esse conteúdo para outros grupos e para outras pessoas. E o espelho disso é o que a gente pode citar: por exemplo, meus grupos de família e de amigos quase sempre compartilham golpes de WhatsApp, porque se tornou muito comum no dia a dia do Brasil esse tipo de golpe.

Por outro lado, a gente tem as redes sociais, que acabam, sem querer, ajudando os cibercriminosos. E como isso funciona nas redes sociais? Os cibercriminosos acabam criando perfis falsos, páginas falsas, onde eles colocam esse conteúdo fraudulento. Normalmente, eles colocam páginas iniciais de banco, utilizam nomes de grandes bancos, também costumam colocar essas supostas vagas de emprego na rede social, notícias falsas, e se aproveitam do próprio mecanismo de divulgação da rede social, de propaganda incentivada da rede social, para espalhar aquele conteúdo, porque hoje eles têm conhecimento de qual o perfil da vítima, de qual a segmentação da sociedade que está na rede social que é mais suscetível àquele conteúdo. Então, eles segmentam até o início do golpe. Eles mandam diretamente para as pessoas que eles sabem que vão consumir, que vão divulgar aquele golpe.

E, a partir do momento em que esse golpe se espalhou, em que as pessoas nele caíram e acreditaram, em que elas forneceram seus dados pessoais e suas credenciais bancárias, a gente tem o ponto final do golpe, que também é muito intrínseco ao tipo de golpe. Quando a gente fala de golpes bancários, o ponto final é o fornecimento das credenciais de acesso ou o cartão de crédito da vítima por cibercriminoso. E aí ele passa a acessar a conta daquela vítima, passando-se por ela junto à instituição bancária, e vai transferir a maior quantidade possível de dinheiro daquela conta, inclusive solicitando empréstimos pessoais, pagamento de contas e de boletos. Isso é muito comum no cibercrime brasileiro. No cenário do cibercrime, eles fazem bancos de dados de boletos para serem pagos e, a partir do momento em que eles têm acesso a uma conta, pagam todos aqueles boletos até esvaziar por completo a conta da vítima.

Quando a gente fala de ataques de WhatsApp, a gente tem dois pontos finais nesse tipo de golpe. Esse ponto final varia conforme a conexão da vítima. Se a vítima tiver uma conexão 3G, é muito comum que ela seja direcionada a um serviço

premium ou pago de SMS, onde ela vai ter a conta dela atrelada ao serviço pago, e ela vai ter um prejuízo semanal financeiro. Além de ter caído no golpe e de ter fornecido os dados pessoais para o atacante, ela acaba tendo seu celular registrado no serviço pago de SMS. Já se ela estiver numa rede *wi-fi* - isso também é detectado -, ele é direcionado para o *download* de *malware*, de um vírus para celular, e aí ela passa a ter seu celular comprometido, muitas vezes dando acesso ao *hacker*, que pode, remotamente, controlar aquele celular ou roubar mais dados confidenciais.

E, para dar um pouco mais de detalhe desses tipos específicos de golpes de que a gente vai falar aqui hoje, que são golpes bancários, páginas falsas de WhatsApp e notícias falsas, começo falando um pouco dos golpes específicos que têm como alvo roubar credenciais bancárias.

Somente no primeiro trimestre deste ano, a gente registrou 2,44 milhões de tentativas de ataque. E, quando a gente fala desses números, é importante relembrar que estou falando de números relativos aos 21 milhões de usuários ativos que a gente tem hoje. Então, a gente bloqueou esses ataques 2,4 milhões de vezes. E, se a gente projeta esse número para toda a população brasileira, é um número preocupante, é um número catastrófico. Esse ataque tem um impacto financeiro muito grande. A vítima tem sua conta esvaziada.

Então, a gente pode ver um reflexo disso inclusive no número de reclamações do Banco Central, que somente do ano passado para este ano cresceu quase 300%, reclamações específicas de golpes bancários no Brasil.

Há outro número preocupante que a gente percebeu. Quando a gente fala de mensagens SMS, muito comuns no Brasil, uma, em cada 20 mensagens SMS, é um *link* para uma página falsa de banco, é um conteúdo que chega falando para o usuário que a conta dele foi bloqueada ou que ele pagou um boleto com um valor altíssimo e que, para cancelar aquela ação, para não ter aquele prejuízo, ele vai ter de clicar naquele *link* e fornecer seus dados pessoais. Aí, o que acontece é que ele cai nesse tipo de página que tende a imitar com perfeição o *site* verdadeiro do banco ou o aplicativo do banco, de forma que a olho é impossível identificar se é verdadeiro ou não, já que ele é visualmente perfeito, igual ao verdadeiro.

Outro tipo de golpe mais comum no Brasil, quando a gente fala de golpes de WhatsApp, são esses golpes em que o *hacker* utiliza a vítima como um vetor de disseminação do golpe. A gente registrou, no primeiro trimestre, 37 milhões de bloqueios desse tipo de golpe, sendo que, nos seis primeiros meses, os principais conteúdos utilizados para a engenharia social eram supostas vagas de emprego.

Algo também importante e muito peculiar do Brasil é a parte contextual. O *hacker* brasileiro, além de ser muito criativo, é muito contextual. Ele vai sempre aproveitar algo que está em alta naquele momento. Assim como ele fez em 2017, com relação ao FGTS, ao saque das contas inativas, ele fez também neste ano. Fez durante a época da Páscoa, prometendo supostos ovos gratuitos, pois a vítima teria de dar dados pessoais e, depois, compartilhar, e aí ela receberia um ovo em casa.

A gente teve um caso recente agora, no Dia dos Namorados, que prometia um *kit* de uma empresa famosa de perfume, mas, para poder receber o *kit*, ela teria de, primeiro, compartilhar com cinco grupos, além de fornecer seus dados pessoais. E, somente em dois dias, a gente atingiu a marca de dois milhões de bloqueios.

(Soa a campainha.)

O SR. EMILIO SIMONI - Então, esse tipo de golpe é muito rápido.

Falando um pouco de notícias falsas, a gente fala de *fake news*, que é algo também recente, somente de 2017 para cá, cresceu mais de 30%, atingindo a marca de três milhões de bloqueios. E, quando a gente fala de *fake news*, de notícias falsas, é importante lembrar que existem dois grandes grupos de *fake news*, não é algo genérico; elas são específicas. No primeiro grupo, o principal objetivo é o ganho financeiro. Então, são notícias falsas que têm por trás um *site*, uma URL ou um *link* e que têm como objetivo levar o usuário para aquele conteúdo, para aquela página, e essas páginas, normalmente, são repletas de publicidade, de *banner*, justamente para gerar a maior quantidade de dinheiro possível. Normalmente, elas são mal escritas, contêm uma série de erros de português. A gente pode perceber que elas têm um tom alarmista. Elas falam, por exemplo, "compartilhe agora", "ajude a divulgar", "compartilhe com seus amigos", "você tem de divulgar isso", normalmente no título, e, muitas vezes, têm conteúdos, inclusive, fora da realidade. Um caso recente, da semana passada, por exemplo, foi uma *fake news* dizendo que a vacina da febre amarela poderia causar gravidez. Então, é algo praticamente impossível, e houve cinco milhões de bloqueios em uma semana. Então, a população consome esse tipo de conteúdo. Por mais fora da realidade que seja, a população acaba consumindo. Mas isso tudo só é válido para as notícias falsas que têm como objetivo o ganho financeiro, que esse é um grande grupo.

Por outro lado, há um segundo grupo de notícias falsas, que têm como principal objetivo a manipulação da opinião pública, e é aí que mora realmente o perigo. E a gente estima que ele vai ter um grande crescimento agora principalmente devido às eleições. Vai haver um crescimento muito grande de notícias falsas tendo como alvo as eleições.

Qual o problema desse tipo de notícias falsas? Elas são muito bem estruturadas. Existem grupos de manipulação por trás que escrevem bem, sabem o que escrever, como divulgar aquilo. Muitas vezes, não há um *site* por trás, não há um *link* por trás, e, então, é difícil bloquear. Elas utilizam meios alternativos como uma imagem ou então um áudio de WhatsApp, como aconteceu num caso recente envolvendo o diretor do sindicato dos caminhoneiros, um suposto áudio gravado por ele, convocando a população para uma série de coisas, e até mesmo vídeos editados.

Então, é muito difícil para as empresas de segurança identificar de forma automática esse tipo de golpe nessa categoria e fazer um alerta, fazer um bloqueio, justamente por essa diversidade, que é proposital, para identificar o seu alerta, a sua identificação.

Por que há esse crescimento muito grande, esse total de acessos? A gente foi analisar mais a fundo para entender por que isso acontece aqui no Brasil e percebeu algo muito grave. Foi aí que a gente viu como a educação e a conscientização são importantes nesse tipo de combate. A gente viu que somente 3% das pessoas que passam *fake news* ou golpes de WhatsApp abrem aquele conteúdo e leem o que está escrito antes de compartilhar. Aí você pensa: "Caramba, somente três, em cada cem pessoas, abrem aquele conteúdo de notícia falsa e leem o que está escrito." A grande maioria, 97%, repassa aquela notícia falsa para a frente sem sequer ler aquele conteúdo. E aí a gente percebeu o quanto é importante a conscientização, o trabalho cultural em cima disso, para checar aquele conteúdo.

Quando a gente projeta esses tipos de golpe realizado por cibercriminosos, sejam notícias falsas, sejam páginas falsas de banco ou páginas falsas de WhatsApp, a gente percebe algo alarmante, que é o quê? Um, em cada quatro brasileiros, pode ter sido vítima de ataque de cibercriminosos no Brasil hoje e, muitas vezes, nem sequer se dá conta disso. O reflexo disso tudo é o prejuízo financeiro que a gente teve no ano passado, em 2017, chegando à casa de US$22 milhões de prejuízo. E, se você considerar ainda que a maioria das vítimas não faz a denúncia, não dá queixa daquele crime, ou por vergonha ou por medo, esse número é muito maior. É por isso que a gente foca que é importante a parte da educação, o trabalho de conscientização e de divulgação de como os cibercriminosos trabalham e de como funciona essa dinâmica.

Em cima disso, dessa magnitude de ataques que existem hoje, existe uma série de iniciativas. A própria PSafe trabalha bastante junto a grandes veículos de comunicação, divulgando golpes, alertando a população, explicando como esses golpes funcionam, dizendo como você deve fazer se cair em um golpe, o que você tem de fazer, como você tem de agir.

Há iniciativas de grandes redes sociais, como é o caso do Facebook, que passou agora a marcar notícias que foram checadas ou não, trabalhando em conjunto com empresas de checagem de fatos aqui no Brasil. Houve o caso do WhatsApp, que passou a marcar notícias, *links*, conteúdos em geral que foram encaminhados, justamente para a pessoa ter ciência de que aquilo é algo novo ou se está somente sendo repassado. E até mesmo é o caso do Twitter, que passou a melhorar seus algoritmos e identificação de *bots*, porque um dos fatores de espalhamento de notícias falsas, de conteúdo inverídico, é a utilização em massa de *bots* e de perfis falsos.

E temos também grandes exemplos na esfera pública como a Lei Carolina Dieckmann, de 2012, e o que está sendo discutido agora, no momento, que é o projeto de lei geral de proteção a dados pessoais, muito importante aqui no Brasil. Eu não sei se vocês sabem que o brasileiro é um dos povos que menos se preocupam com os dados pessoais. Então, é muito comum, no Brasil, postar suas rotinas diárias em uma rede social, postar dados confidenciais em redes sociais. O brasileiro ainda não tem a consciência de que aquilo é perigoso, de que aquela exposição em excesso é perigosa e de que o *hacker* pode aproveitar todos esses detalhes para comercializar, podendo até roubar a identidade dele. Um tipo de crime que tem crescido muito no Brasil é o roubo de identidade, que a gente chama de *scammers*, que são os perfis falsos em redes sociais. E, principalmente, as delegacias especializadas em crimes cibernéticos também têm feito um trabalho muito bom em cima disso e contribuído bastante.

Mas a gente acredita que trabalhos isolados não trazem o efeito esperado. E é por isso que a gente...

(Soa a campainha.)

O SR. EMILIO SIMONI - ... traz aqui hoje o que a gente acredita que é a proposta que pode solucionar esse problema, que é uma ação conjunta. Na área de legislação, através de leis atualizadas, categorias mais específicas para combater o cibercrime; através da tecnologia, principalmente pesquisas, envolvendo as universidades, ferramentas de tecnologia de ponta. A gente tem que utilizar muito tecnologias baseadas em inteligência artificial para acompanhar a evolução dos *hackers*, já que a gente tem aí milhões de *hackers* para poucas pessoas protegendo, poucos pesquisadores, poucos estudantes. Então, a gente tem que ter um cérebro eletrônico capaz de ajudar o pesquisador a identificar esses tipos de ataque, esses padrões de ataque, e combater o cibercriminoso brasileiro.

Outra coisa muito importante: proteção em tempo real. Identificou algo novo, identificou um ataque novo, um padrão novo, tem de haver uma rede de comunicação, de divulgação, para levar essa informação muito rápido a outras empresas,

ao governo, à sociedade, para que eles possam se proteger dos cibercriminosos, afinal eles crescem de forma muito rápida, e a gente tem que acompanhar isso, para segurar esses ataques.

E, acima de tudo, o principal é a educação, como a gente está fazendo aqui hoje, que é um ótimo exemplo: a ampliação dos debates, a conscientização da população sobre como os cibercriminosos no Brasil agem, como esses ataques se apresentam, o que é a engenharia social. Porque, se a engenharia social não funcionar, o cibercriminoso não tem sucesso. Se a possível vítima perceber que aquilo lá não pode ser verídico, se ela tiver um senso crítico, pesquisar a marca envolvida - se eu recebi uma vaga de emprego, vou checar junto à empresa se aquilo é verdadeiro ou não; se eu recebi um SMS do banco, eu vou ligar para o banco consumar se aquilo é verdadeiro ou não -, o senso crítico vai ajudar muito a combater esse crime.

E o principal, que eu acredito pessoalmente que é o mais importante, é envolver as crianças e adolescentes nesse processo, porque hoje a conectividade acontece cada vez mais cedo. Eu tenho um exemplo muito próximo disso, que é o meu filho, que começou a navegar na internet com dois anos. Na época, eu tinha um iPad, mas com dois anos e meio ele o destruiu, e hoje ele acessa através do meu *notebook* e do meu celular. E algo que me chamou a atenção recentemente, especialmente ontem: na hora em que acabou a bateria do meu celular, em que ele estava navegando, ele falou um palavrão que a gente nunca tinha falado em casa. Eu falei: "Ô filho, onde você aprendeu isso? Foi na escola?" Ele: "Não, pai. Eu vi num vídeo do YouTube o cara que faz vídeo de *minecraft* falando". E eu percebi o quanto que ele está exposto. Se ele aprendeu um palavrão num vídeo do YouTube, imagina se uma pessoa mal-intencionada o induz a instalar um *malware*, um vírus. Inclusive, a gente teve casos recentes de *hackers* que acessaram aqueles *smart toys*, brinquedos inteligentes que ficam conectados à internet, e passaram a se comunicar com as crianças, perguntando detalhes das rotinas da casa, quando saíam, quando não tinha ninguém em casa, inclusive induzindo as crianças a fazer ações maliciosas, como agredir os irmãos, agredir os pais.

Então, é muito importante a conscientização, a divulgação de como os *hackers* funcionam, do que pode ser feito, e principalmente o trabalho conjunto. A PSafe hoje se dispõe a trabalhar em conjunto com todas as áreas interessadas, para garantir que a gente tenha a liberdade de navegação na internet, mas de forma segura, garantindo a nossa privacidade.

É isso que eu tenho para falar aqui hoje.

Muito obrigado a todos e em especial ao Senador por esta oportunidade.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Nós é que agradecemos, Emilio, e eu espero que a sua mensagem fique.

Eu passo a palavra agora ao Dr. Thiago.

O SR. THIAGO TAVARES NUNES DE OLIVEIRA - Muito bom dia a todos e todas. Cumprimento os meus colegas da Mesa na pessoa do Senador Cristovam Buarque, a quem desde já agradeço pelo convite. É uma honra muito grande para mim e para a SaferNet Brasil poder participar desta audiência pública, a convite de V. Exª, cuja história parlamentar está indissociavelmente ligada à luta pela qualidade da educação e pela universalização da educação, de modo que eu fico muito feliz.

Tomo emprestadas as suas palavras iniciais para remetê-las a Émile Durkheim: onde há sociedade, há crime. Crime é um fato social. E, se existe crime na internet, é porque a internet é sobretudo uma rede de socialização. Ela é um espaço de socialização, é um espaço onde a sociedade manifesta as suas angústias, as suas aspirações, as suas ideias, as suas propostas. É uma grande praça pública, é uma grande ágora pós-moderna. Então, se a sociedade está presente na internet, é também previsível que nesse espaço ocorram atos ilícitos e crimes.

E a outra premissa, mais contemporânea, mas igualmente importante, é essa do criador da internet, do inventor do protocolo TCP/IP, o Vint Cerf, que disse exatamente isto: que a internet é um espelho da sociedade, ela é a imagem refletida nesse espelho; e, se nós não gostamos da imagem que vemos refletida no espelho, não adianta quebrar o espelho, nós temos que mudar a sociedade, nós temos que procurar atingir as causas do problema, e não apenas olhar para os sintomas.

Então, a internet é essa caixa de ressonância, é essa imagem refletida. E é evidente que, numa sociedade desigual como a nossa, profundamente marcada por desigualdades sociais, econômicas, de gênero, étnicas e todo tipo de assimetria, essas assimetrias e essas desigualdades muitas vezes vão resultar em conflitos, e esses conflitos vão encontrar na internet essa caixa de ressonância.

Desse modo, uma outra premissa - essa mais antiga ainda e que se conecta a esse debate que nós estamos travando hoje - é o papel da educação. O Cesare Beccaria, lá no século XVIII, dizia que é melhor prevenir os crimes do que ter de puni-los e que o meio mais seguro, mas ao mesmo tempo mais difícil, de tornar os homens menos inclinados a praticar o mal é aperfeiçoar a educação. Isso foi dito há mais de 250 anos, mas continua extremamente atual. E foi com esse objetivo que, lá em 2005, eu decidi fundar a SaferNet Brasil, que é uma organização não governamental, sem fins lucrativos, sem

qualquer tipo de vinculação político-partidária, sem financiamento público de qualquer natureza, e que tem o objetivo, atua há mais de uma década no Brasil com o objetivo de defender e promover direitos humanos fundamentais.

Nós acreditamos que a educação para boas escolhas *on-line* é um dos pilares que devem estruturar não só as políticas públicas, mas também a ação empresarial e também a ação do terceiro setor, e por uma razão muito simples: a educação promove o conhecimento; o conhecimento proporciona escolhas; quem tem escolhas tem liberdade; e navegar com segurança é navegar com liberdade, é, sobretudo, fazer boas escolhas *on-line*.

Então, segurança e liberdade andam juntas, não são polos opostos que se repelem; pelo contrário, eles andam juntos e devem andar juntos. Não se trata de fazer uma escolha entre liberdade ou segurança, ou entre segurança ou privacidade. Trata-se de garantir o equilíbrio entre esses direitos fundamentais, que são indivisíveis, que são mutuamente reforçadores, que são universais e que devem ser respeitados e implementados na sua integralidade.

Então, nós criamos lá em 2005 um canal de denúncias. Lá nós recebemos, Senador, denúncias anônimas referentes a todos aqueles crimes e violações de direitos humanos; casos que vão desde abusos e exploração sexual de crianças pela internet, racismo, xenofobia, homofobia, neonazismo, intolerância religiosa, tráfico de pessoas e, mais recentemente, violência e discriminação contra mulheres.

E nesses anos a população tem colaborado e participado nesse esforço de identificar esses atos ilícitos que são praticados pela rede e tem denunciado milhares de páginas, centenas de milhares de páginas, com conteúdos dessa natureza. E nós atuamos em parceria com as empresas privadas, sobretudo as empresas de internet, mas também algumas empresas de telecomunicações, para detectar esses conteúdos ilícitos, removê-los e preservar as provas para que o Ministério Público e a Polícia Federal possam investigar e identificar a autoria e responsabilizar esses criminosos na forma da lei.

Nós também temos um termo formal de cooperação com a Procuradoria-Geral da República, para centralizar o recebimento dessas notificações e permitir que os Procuradores da República no País possam usar as informações que nós coletamos e armazenamos na nossa base de dados para instruir as suas investigações e o seu processo criminal.

Também oferecemos um canal de suporte às vítimas - de suporte emocional e de orientação a vítimas como crianças, adolescentes e também adultos que vivenciam alguma situação de risco ou de crime na internet. Então, situações que vão desde o *ciberbullying* até vazamento de *nudes*, "sextorsão" - lançamos recentemente uma campanha em parceria com o Facebook e com o Twitter sobre o tema da "sextorsão" - e vários outros temas, que vão desde o vazamento de dados, questões de privacidade, até questões mais sérias, incluindo suicídio.

Para esta audiência... Eu li no requerimento que um dos objetivos do Senador é discutir o tema *fake news* e o papel da educação na prevenção da disseminação de conteúdo fraudulento de desinformação *on-line*. Então, eu resolvi incluir alguns eslaides sobre esse tema. Esse é um assunto em que a SaferNet tem-se aprofundado bastante, sobretudo no último ano. Nós temos o privilégio de compor o conselho consultivo sobre a internet e eleições, que foi instituído pelo TSE no final do ano passado, e temos levado contribuições concretas sobre essa temática.

A primeira advertência que eu preciso fazer em relação a esse assunto é de que não há um conceito definido do que vem a ser *fake news*. *Fake news* é um *hype*, é um chavão, uma palavra da moda que é apropriada por diferentes atores, em diferentes perspectivas, com diferentes interesses e diferentes objetivos. Eu vou falar um pouco disso e trazer um pouco do que existe de pesquisas de ponta no exterior sobre o assunto.

Usando um exemplo prático, se alguém perguntar ao Donald Trump o que é *fake news* para ele, ele vai dizer que é tudo que o *The New York Times*, o *Washington Post* e a CNN publicam contra ele e que ele não gosta; é isso que ele vai dizer que é *fake news.* Um dos maiores propagadores de *fake news* nos Estados Unidos chama-se Donald Trump.

(Soa a campainha.)

O SR. THIAGO TAVARES NUNES DE OLIVEIRA - Bem, vou ter que avançar aqui.

Aqui no Brasil, em janeiro deste ano, um dos pré-candidatos declarou numa entrevista que tudo o que a *Folha de S.Paulo* publicar contra ele ou sobre ele, ele dirá que é *fake news*, porque a *Folha* fez uma série de reportagens mostrando uma evolução patrimonial incompatível com a renda desse pré-candidato, e ele não gostou dessa apuração jornalística. A imprensa, quando imprensa, incomoda, e quem se sente incomodado tenta deslegitimar, tenta desacreditar o trabalho jornalístico e o trabalho de apuração jornalística. E uma das formas de fazer isso é dizer: "É *fake news*, é *fake news*, é *fake news*, é *fake news*".

Então, esse debate sobre *fake news* se insere num contexto mais amplo, que internacionalmente os acadêmicos, os cientistas que estão estudando a matéria chamam de desordem informacional. Esse é o conceito mais aceito na academia e na comunidade internacional para enquadrar esse fenômeno, que se batizou de *fake news*, de desinformação *on-line* - questões aí que envolvem vários outros temas, como conteúdos fabricados, boatos, etc. e tal.

Essa desordem informacional pode ter uma intenção de causar dano, e existem aí classificações que nos ajudam a compreender um pouco mais a dimensão desse fenômeno. Então, ela pode ter a intenção de causar dano, por exemplo, a uma candidatura, como foi o caso da invasão dos servidores da campanha do Partido Democrata nos Estados Unidos durante as eleições presidenciais. Houve um grande vazamento de *e-mails*, de dados do comitê de campanha, e isso gerou um constrangimento para a campanha e também um dano para a própria candidata Hillary Clinton lá nos Estados Unidos. Isso é *mal-information*; está classificado ali, naquela categoria que inclui também assédio, que inclui intimidação, que inclui discurso de ódio, mas também existe conteúdo manipulado, existe conteúdo fabricado, existe conteúdo que é retirado do contexto e colocado em outro contexto, existem conexões falsas, existem conteúdos não verdadeiros, e assim por diante. Então, existe uma complexidade aí que precisa ser levada em consideração.

A First Draft é, sem sombra de dúvidas, a mais importante e reconhecida iniciativa internacional nessa área. É um consórcio com mais de 70 instituições, incluindo grandes universidades, como Harvard; grandes empresas, como Google - o próprio Facebook também participa -; grandes veículos de mídia, como a BBC, como a CNN, o *The New York Times*, o *Washington Post*. É uma grande coalizão com mais de 70 instituições.

Ela classifica a desinformação *on-line* em sete tipos, que são aqueles ali: vão desde sátira e paródia, que não têm intenção de causar nenhum dano, mas têm um potencial de repercutir, de causar repercussão e de influenciar; conteúdo fabricado, em que o conteúdo é 100% falso e tem o objetivo de causar um dano ou de manipular a percepção do eleitor, ou mesmo de gerar lucro para quem está fabricando aquele conteúdo de monetização; falsas conexões; falso contexto; contexto manipulado, quando uma informação genuína ou uma imagem é manipulada para mudar o contexto. Então, existe uma granularidade enorme desse tipo de conteúdo, que é criado com esses objetivos.

Uma outra organização vai além e classifica em dez tipos de categorias diferentes isso que vem se chamar de desordem informacional ou desinformação ou, como é mais popularmente chamado aqui, *fake news*.

Dentre as motivações, pode ser a motivação financeira, pode ser a motivação política, pode ser uma motivação de humor, de causar humor, de provocar humor, de causar reações apaixonadas e também de desinformar - desinformar o receptor dessa mensagem.

Dentre, ainda, essas classificações, percebam a complexidade, quando você começa a olhar o fenômeno com mais profundidade, e a necessidade que há de se ter... Antes de se tirar uma conclusão sobre que tipo de conteúdo fraudulento é esse de que estamos tratando, que tipo de *fake news* é essa que nós estamos discutindo, é preciso você ter pelo menos aquelas informações, ter uma resposta para aquelas informações sobre o agente que está produzindo o conteúdo, a mensagem que foi produzida e, também, o intérprete dessa mensagem.

Aqui entra o famoso viés de confirmação, que é muito comum em sociedades polarizadas como a nossa, em que as pessoas não querem e não estão muito preocupadas em saber se um determinado fato é verídico ou não, se procede ou não. Elas simplesmente leem a manchete e interpretam aquela manchete de acordo com o seu viés de confirmação.

Então, se aquela manchete é aderente ao que eu penso previamente sobre um determinado político, sobre um determinado fato, sobre uma determinada situação, eu já me dou por satisfeito e repasso aquela informação. Crio ali câmaras de eco, repercuto aquela informação em grupos, em redes sociais, única e exclusivamente porque eu acho que aquilo é o que eu gostaria que fosse verdade; é aquilo que confirma a minha percepção ou a minha ideia sobre aquele determinado fato, pouco importando se aquilo foi apurado, se aquilo foi verdade, se aquilo procede ou não.

Então, existe uma granularidade, e é preciso olhar atentamente a esses critérios, que incluem questões até mesmo de automação - foi mencionada aqui a questão dos robôs -, a intenção da audiência, a intenção de causar dano ou não e vários outros critérios.

Não vou me alongar porque o tempo é bastante restrito.

Este aqui é o *modus operandi* de como esses conteúdos fabricados, de como a desinformação se retroalimenta e gera esses processos que influenciam, sobretudo, a percepção das pessoas sobre fatos, que desinformam pessoas sobre fatos e que podem, evidentemente, influenciar também o próprio processo eleitoral. Então, esse é um pouco do *modus operandi* de como a coisa acontece. Sempre há a necessidade de se fazer esta pergunta, nós temos que fazer a nós mesmos esta pergunta: isso é real ou é um conteúdo inventado?

Estou aqui apenas trazendo alguns eslaides que mostram que esse é um problema real, isso não é ficção científica, nem é hipótese de que vai acontecer. Não; já está acontecendo. Se a gente olha a experiência dos últimos processos eleitorais nos Estados Unidos e Europa, a gente vê claramente que essa foi uma estratégia utilizada por muitos atores para influenciar o processo.

Mas não é preciso ir muito longe. Na base de dados da SaferNet, nós temos registros de conteúdos fabricados e usados em processos eleitorais já na eleição de 2012. Em 2012, começam os primeiros *sites* com conteúdos fraudulentos, inventados, com o objetivo de gerar algum tipo de engajamento, sobretudo em redes sociais.

Em 2014, isso ganha mais relevância, mais vulto, entra definitivamente no radar, sobretudo a utilização de robôs em redes sociais. E, em 2016, esse processo continua, muitas vezes financiados pelos próprios partidos políticos, que contratam pessoas para fabricar conteúdos e administrar perfis que gerenciam redes de robôs e *bots* para poder impulsionar esse conteúdo.

Desse modo, esse tipo de estratégia, que ganhou uma repercussão internacional com a eleição americana de 2016, já é conhecido e está fartamente documentado, inclusive pela imprensa, no Brasil, desde 2012. Os primeiros registros começam em 2011 e vem à público no final de 2011 e em 2012.

(Soa a campainha.)

O SR. THIAGO TAVARES NUNES DE OLIVEIRA - Nós temos um levantamento sobre isso. Então, é um problema real, que vem crescendo ao longo do tempo.

Esse tipo de conteúdo fraudulento nos Estados Unidos mostra que as pessoas perdem a noção do que realmente é verdadeiro e do que é falso. Então, há uma disputa de narrativas sobre a própria realidade, e isso, claro, tem um impacto.

Estes são alguns dados estatísticos a partir da experiência americana. Então, há alguns exemplos de notícias... De notícias, não; de conteúdos falsos, conteúdos fabricados apresentados no formato de notícia e que foram utilizados na eleição de 2016 do Trump. Manchetes que diziam que o Papa Francisco teria endossado a candidatura do Donald Trump; notícias falsas dizendo que um agente do FBI encontrou um *e-mail* e que, este agente, supostamente, teria cometido suicídio; e outros dizendo que o Donald Trump teria usado o próprio avião para transportar 200 marines. Ou seja, conteúdos absolutamente fabricados com o objetivo de manter o nome do candidato na mídia e na memória dos eleitores.

Aqui temos alguns outros dados também estatísticos a partir da percepção desse fenômeno - não vou me alongar muito. Apenas para destacar que, em uma recente pesquisa da BBC, o Brasil foi apontado como o País mais preocupado com o fenômeno da desinformação *on-line*, vulgarmente chamada de *fake news*.

Um outro risco real é a possibilidade de fabricação desses conteúdos, em uma estratégia de *marketing* comportamental, *marketing* político comportamental, para impulsionar conteúdos falsos para segmentos específicos da população. Então, se eu sei que um determinado eleitor tem um perfil conservador e se mobiliza em temas que envolvem questões morais, questões de família, questões que envolvem valores morais e familiares, eu posso fabricar um conteúdo contra um determinado candidato e direcionar aquele conteúdo especificamente para esse eleitor. E, esse eleitor, quando receber, vai, certamente, atuar como replicador desse conteúdo, salvo se ele estiver vacinado por um bom vírus, que é o bom vírus da educação, ou seja, se ele tiver uma postura crítica de checar aquela informação antes de repassar. E, para isso, o papel da educação é realmente fundamental.

Isso aqui não é novidade. Houve o escândalo da Cambridge Analytica, que todos acompanharam. Então, era exatamente esse o *modus operandi* que essa empresa de *marketing* político usava. E ela não era a única; existem vários filhotes da Cambridge Analytica por aí, inclusive no Brasil, e nós precisamos ficar atentos a isso.

Aqui um outro dado, também a partir do contexto americano, que mostra que o engajamento em relação a esses conteúdos fraudulentos é maior do que nos conteúdos verdadeiros. Então, os conteúdos falsos repercutiram mais nos Estados Unidos do que os conteúdos produzidos pela imprensa tradicional. Isso mostra que a produção desse tipo de conteúdo é rentável, ou seja, *fake news* é rentável, dá dinheiro, e muita gente produz isso porque é rentável.

Diante desse contexto - e aí eu já concluo Senador -, o que nós fizemos? A SaferNet, como membro do Conselho Consultivo do TSE, encaminhou formalmente - eu vou deixar uma cópia dessa contribuição com a assessoria de V. Exª - uma série de 14 sugestões ao TSE para lidar com essas questões. São questões que envolvem transparência e *accountability*, isonomia econômica na precificação de anúncios e, sobretudo, o item 3, *media literacy* - *media literacy*, *fact-checking* e jornalismo colaborativo. E essas recomendações do eixo três conectam-se diretamente com o propósito desta audiência pública, que procura discutir o papel da educação.

Então, nós dissemos ao TSE que deveriam ser estimuladas iniciativas educativas, com foco na conscientização do eleitor, para reconhecer e não compartilhar conteúdos fraudulentos e desinformação.

Também sugerimos ao TSE que deve ser estimulado o engajamento do próprio tribunal, da própria Justiça Eleitoral nas iniciativas multissetoriais voltadas a promover a checagem em tempo real de informações, ou seja, o *fact-checking*, como também o jornalismo colaborativo, a exemplo das iniciativas da First Draft, que eu já mencionei, e também da

Electionland, que se revelaram muito bem-sucedidas em eleições recentes nos Estados Unidos, no Reino Unido, na França e na Alemanha.

Eu não tenho tempo de entrar em detalhes, mas esse documento é público. Nós divulgamos essa contribuição publicamente, e nas notas de rodapé ali existem *links* para mais informações sobre essas duas iniciativas, First Draft e Electionland, que foram, realmente, bem sucedidas e consideradas exemplos de boas práticas no contexto internacional.

E chamamos atenção para o perigo de se enveredar pela abordagem criminal. Isso me preocupa muito, Senador, porque, dos 20 projetos de lei apresentados no Congresso Nacional, a grande maioria procura seguir por essa linha de criminalizar a veiculação ou criminalizar o compartilhamento de conteúdos fraudulentos.

Eu vou até mencionar, rapidamente, um eslaide sobre isso.

Então, aqui um exemplo concreto...

(Soa a campainha.)

O SR. THIAGO TAVARES NUNES DE OLIVEIRA - ... do que é feito pela rede pública de TV norte-americana em relação à educação de crianças e adolescentes para *media literacy*, ou seja, para educação de mídia. É um exemplo do que poderia ser feito, por exemplo, pela TV Senado, que é uma TV pública e poderia desenvolver campanhas similares, e por outras TVs públicas no Brasil em relação à *media literacy*. Essa é uma sugestão concreta que eu já faria a V. Exª.

E o debate no Congresso, como eu mencionei. Se a gente faz uma busca por *fake news* na Câmara, nós temos 18 resultados, em 2017, e 92 resultados em 2018. Aqui, no Senado, se nós fizermos a mesma busca, nós tivemos dois pronunciamentos de Senadores no plenário do Senado, em 2017, e 48 pronunciamentos de Senadores no plenário do Senado em 2018, o que mostra que esse é um tema muito presente no debate parlamentar, no debate aqui no Congresso.

Apenas para iluminar esse debate, que está a todo vapor aqui no Congresso Nacional, eu trago duas referências que eu julgo da maior importância. A primeira delas, a do Ministro Louis Brandeis, que foi um Ministro da Suprema Corte Americana, que, ao julgar um caso célebre nos Estados Unidos, em 1927, disse que, quando há exposições, há conteúdos, há discussões que são falsas ou falaciosas, nós temos que aperfeiçoar os processos educacionais - educação, o que V. Exª está propondo aqui nesta audiência pública - e que o remédio a ser aplicado é *more speach*, ou seja, mais liberdade de expressão, e não o silêncio forçado. Então, o remédio para conteúdos falsos, narrativas falsas ou falaciosas é mais expressão, e não silêncio imposto. Isso foi o que um Ministro da Suprema Corte dos Estados Unidos disse em 1927.

E, aqui, o nosso Ministro Luiz Fux, em artigo agora na *Folha de S. Paulo*, no domingo, disse:

> *Contra notícia falsa, mais jornalismo.*
>
> *[...]*
>
> *Países com democracias sólidas e textos constitucionais robustos conseguem garantir a liberdade de expressão e, ao mesmo tempo, um jornalismo político-eleitoral combativo, crítico e investigativo. Nos Estados Unidos, por exemplo, mais de 40 plataformas de checagem de dados trabalharam durante as eleições de 2016. Outras cinco participam hoje da iniciativa de verificação do Facebook. Não houve registro de agressões a seus jornalistas.*

E o Ministro, nesse artigo de domingo, nesse lúcido artigo de domingo, chamava atenção para as agressões que os jornalistas têm sofrido no Brasil única e exclusivamente por exercerem a sua profissão de jornalistas. E ele se referia, sobretudo, aos jornalistas que trabalham nas várias agências de *fact-checking* - não são só duas: a Agence France-Presse está fazendo *fact-checking*...

(Soa a campainha.)

O SR. THIAGO TAVARES NUNES DE OLIVEIRA - ... *O Estadão* está fazendo *fact-checking*; a Globo, o G-1 está fazendo *fact-checking*. Vários outros veículos de imprensa tradicionais estão se mobilizando para isso, e aqueles que estão produzindo conteúdos fraudulentos e tentando usar as mesmas táticas usadas em eleições anteriores para influenciar e fraudar o processo eleitoral estão incomodados com isso e passaram, inclusive, a agredir esses jornalistas.

Este é o último eslaide.

É apenas um convite para um seminário internacional que ocorrerá no Auditório do TSE, no próximo dia 21 de junho, na semana que vem. As inscrições estão abertas, são gratuitas e podem ser feitas pelo site do próprio TSE. É apenas para divulgar o evento, porque certamente é mais uma oportunidade de nós continuarmos aprofundando essa discussão.

Muitíssimo obrigado, Senador.

Peço desculpas por ter estendido o tempo.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Nós é que agradecemos por suas sugestões, suas análises.

Eu passo a palavra ao Ministro Conselheiro da Delegação da União Europeia no Brasil, Sr. Carlos Oliveira.

O SR. CARLOS OLIVEIRA - Muito obrigado.

Sr. Presidente da Comissão de Educação, Cultura e Desporto do Senado, Sr. Senador Cristovam Buarque, Srs. Senadores, membros do painel, minhas senhoras e meus senhores, eu gostaria de começar por agradecer o convite que foi endereçado à União Europeia para participar deste interessante debate, que aborda um tema de indiscutível relevância. Nós estamos perante uma transformação daquilo que é a visão tradicional da sociedade, das relações de confiança, daquilo que é a confiabilidade das fontes de informação e também do papel dos cidadãos nesse novo mundo, que, de fato, requer uma reflexão muito aprofundada sobre a forma como podemos superar conjuntamente esses desafios, sem pôr em causa aquilo que são os fundamentos de uma sociedade democrática.

Bem, se eu disser que atualmente existem mais telefones celulares do que número de pessoas no Brasil, contando com os recém-nascidos, isso é de fato uma evidência. Uma outra informação que pode ser interessante é que estão licenciadas no mundo dois bilhões de contas no Facebook. Isso dá aproximadamente uma conta para cada quatro pessoas.

Um aspecto também interessante é que, quando nós analisamos a lista das dez maiores empresas do mundo, seis são empresas que, de uma forma ou de outra, estão associadas àquilo que se convencionou chamar economia digital.

Por outro aspecto, vemos primordialmente empresas que gerem informação sobre pessoas, que gerem dados sobre pessoas, que trabalham, digamos, todo esse manancial quase inesgotável de informação e de novos negócios, novas atividade lucrativas.

Se eu estou a citar esses dados, é só, digamos, para ilustrar as implicações que essas transformações têm nos gestos mais simples do nosso cotidiano. Elas têm a ver com a forma como nós trabalhamos, têm a ver com as nossas atividades de lazer, têm a ver com a nossa relação com entidades institucionais, como governos, Ministério da Fazenda, mas também - e não podemos esquecer esse aspecto muito importante - com os nossos hábitos como consumidores, e mesmo com a forma como interagimos com os nossos amigos, com as pessoas que fazem parte do nosso círculo de relações. Isso mostra que, na realidade, é fato que, a par da visão tradicional que foi instituída há algumas décadas, em que se apresentava a internet como um espaço de liberdade, há também que se equacionar a internet como um espaço de responsabilidade.

É importante, essencial que as pessoas tenham consciência das implicações que existem naquilo que são atividades ilícitas, atividades ilegais e atividades criminosas. Portanto, uma parte essencial, digamos, da nossa vivência, do nosso cotidiano é perceber que o processo de transformação digital tem também que assegurar condições de um novo tipo de cidadania, adaptado àquilo que é o ambiente da sociedade de informação. Uma cidadania tem que ser inclusiva, uma cidadania tem que ser responsável, mas uma cidadania também tem que ser informada.

Na União Europeia, nós temos nos preocupado muito com essa temática, não só porque isso é essencial para preservar aquilo que são os aspectos fundacionais do projeto europeu, mas também porque esse é um desafio que não vai ser exclusivamente resolvido pela confiança no livre arbítrio e na mão invisível. É uma preocupação coletiva, em que o Estado, a coletividade no seu todo tem que ter um papel essencial no sentido de facultar a cada cidadão a oportunidade para ser um membro consciente e ativo desse processo e evitar criar novos fatores de exclusão e mesmo, em alguns casos - como foi, aliás, mencionado por alguns dos oradores que me precederam -, que isso funcione como um fator acelerador desses comportamentos perversos e disruptivos no sentido mais negativo do termo.

Há um conceito a que eu gostaria de me referir, que é do meu ponto de vista e do ponto de vista da União Europeia um conceito central, que é o conceito da literacia digital e, podemos falar mais genericamente, de competências digitais. Uma boa parte dos fundamentos da democracia representativa se assenta no fato de as pessoas terem criado, digamos, acesso à capacidade de ler, escrever e compreender o discurso falado e escrito como um fator de participação nas decisões coletivas.

Quando nós passamos para o mundo digital, o que se passa é que o leque de atividades em que o cidadão é chamado para participar é de tal forma lato e abrangente que nós temos que investir fortemente na criação e no desenvolvimento desse conceito mais abrangente a que eu chamei de literacia digital.

Todos nós lidamos cotidianamente com dispositivos e artefatos digitais no nosso computador pessoal, no *tablet*, no celular, no *smartphone*, se quisermos.

E é essencial facultar aos cidadãos confiança para usarem de forma crítica aquilo que são essas ferramentas com as quais eles lidam cotidianamente. E quando falo em utilizar isso conforme a crítica, significa dar-lhes a capacidade de avaliar a seriedade da informação que lhes é facultada através desses meios. Isso significa equipá-los com as capacidades de análise

que lhes permitam, por exemplo, quando vier uma informação, ser capazes de confrontar e comparar essa informação com outras fontes, ter uma apreciação sobre o grau de confiança que a origem dessa mensagem pode ou não inspirar.

Da mesma forma, um dos fatores que marcam a diferença face àquilo que é da nossa experiência tradicional é que, enquanto antigamente nós, no meu português lusitano chamaríamos isso de boca a boca, ou seja, passávamos a informação para o nosso pequeno círculo de amigos, as redes sociais têm um efeito acelerador absolutamente avassalador. Aquilo que no fundo poderia fixar-se em um grupo de dez, quinze pessoas rapidamente chegam a centenas, a milhares de pessoas. E a apreciação é: "Ah! Isso me foi passado pelo fulano que eu até conheço". E aqui, sim, há um efeito um bocado perverso, porque o contato humano e o conhecimento pessoal funcionam um pouco como acelerador dessas notícias, dessa informação de caráter duvidoso. E eu estou um pouco...

A apresentação do Thiago anteriormente focava muito na questão das f*ake new*s. Mas isso também é verdade e é um canal difusor importantíssimo para tudo aquilo que são mecanismos de destruição, mecanismos fraudulentos que promovem pessoas, atraem pessoas para negócios fantasiosos, que são geralmente falsos. Sem querer fazer um comentário muito longo, é conhecidíssima a história, há 20 anos passados, de que essas informações eram enviadas por fax e geralmente envolviam sempre um homem riquíssimo, numa posição significativa, portanto, uma pessoa politicamente exposta, num país num recôndito da África, normalmente conhecido como sendo um país com grandes riquezas naturais. Depois se dizia: "Eu preciso da sua ajuda porque tenho que exportar não sei quantos milhões do meu país para o outro". Extraordinariamente, isso continua a ser um veículo de promoção da fraude nos tempos da internet, com alguma sofisticação original, mas continua a ser um veículo importante.

Nós podemos imaginar que as pessoas com uma educação mais aprofundada são capazes de distinguir e identificar isso como sendo um mecanismo claramente fraudulento. Quando nós falamos em 200 milhões de utilizadores de *smartphones* ou de telefones portáteis, telefones móveis, no Brasil, eu não estou seguro de que todas as pessoas sejam capazes de fazer essa distinção. Da mesma forma, mesmo na Europa, esse problema também existe. E a educação média das pessoas é que quase toda gente tem o nível secundário.

Portanto, esse é um desafio que se coloca para nós desenvolvermos uma sociedade inclusiva e responsável no que diz respeito à utilização da internet e naquilo que é a cidadania digital.

Antes de mim, os dois oradores presentes falaram muito sobre aquilo que é a essência do cibercrime e da cibersegurança. Eu não vou repetir tudo aquilo que foi mencionado, mas há um leque vastíssimo. Nós falamos muito sobre as questões de usurpação de identidade, que funcionam como um vetor para depois interferir naquilo que é o acesso a coisas tão simples como não só sua conta bancária, mas também, de repente, uma pessoa descobrir que, magicamente, alguém fez um contrato em seu nome em coisas tão simples como a venda de um imóvel, a aquisição de um telefone celular, a celebração de um contrato com um prestador de serviço qualquer. Essas são questões que interpelam o cidadão no seu cotidiano e para as quais é necessário que ele esteja atento, que ele tenha consciência desses riscos.

Isso significa também um trabalho notável daquilo que é a conscientização, a educação, que começa seguramente nas gerações que estão agora a chegar às escolas, mas que abrange todos os cidadãos. Eu posso dizer, por exemplo, a propósito de um fenômeno que teve lugar há alguns anos na Europa por ocasião da instalação do euro, com a mudança de todas as notas, que uma das coisas mais importantes foi acompanhar esse processo, porque havia muitas pessoas que enviavam notícias assim: "Agora seu dinheiro não vale nada. Passe para cá o seu dinheiro que é para a gente depois vir aqui trazer as notas novas". São coisas que parecem óbvias, mas que, na realidade, eu acho que, se isso é verdade num universo como a União Europeia, em que as pessoas têm até proteções de proximidade, porque a cidade mais próxima está a apenas 10 quilômetros, e as pessoas se conhecem muito, eu penso que esse é, de fato, um problema muito mais generalizado e que se coloca provavelmente em todos os países. Portanto, é importante nós pensarmos coletivamente nessas matérias porque, como foi muitas vezes mencionado antes, o cibercrime, os ciberataques, a cibersegurança são questões que extravasam aquilo que são as fronteiras tradicionais.

Há ainda outros aspectos que não foram mencionados aqui, mas que são igualmente importantes. Estamos a falar da proteção em relação a conteúdos obscenos e ofensivos. Toda gente sabe do que estou a falar quando falo de pornografia infantil. Toda gente sabe do que estou a falar quando me refiro, por exemplo, ao aliciamento de jovens e menores nas redes sociais. Há um aspecto que, às vezes, aparece associado também às camadas mais jovens da população, que é a utilização ilegal de conteúdos que ultrapassam aquilo que são as regras tradicionais dos direitos autorais. Há de fato uma noção de que isso não é crime.

(Soa a campainha.)

O SR. CARLOS OLIVEIRA - Mas, na realidade, há muitas pessoas cujo cotidiano, cuja sobrevivência econômica depende criticamente do respeito a um conjunto de regras. E no mundo dos negócios, em que eles estão estabelecidos, esses

modelos podem ser revistos, mas isso não pode servir, digamos, de álibi para se fomentar essa desregulação descontrolada desses aspectos. Eu acho que isso é também um aspecto muito importante e muitas vezes o cidadão comum não tem perfeita consciência da gravidade desse tipo de mudanças.

Eu gostaria de, muito brevemente, citar algumas iniciativas da União Europeia. Na realidade, há um leque tão vasto que eu não vou conseguir ser exaustivo, mas também não é esse o meu objetivo. Vou só citar algumas que são especialmente relevantes.

Uma delas tem a ver com o plano de ação sobre aprendizagem e letramento digital. Trata-se, por um lado, de trazer as técnicas de informação para o cotidiano das escolas, das universidades. Isso tem que ser não só uma ferramenta que permita um empoderamento por parte dos atores da escola, estamos a falar dos professores, estamos a falar dos alunos, e requer, digamos, uma redefinição daquilo que são as relações sociais no processo de aprendizagem nesses ambientes. Estamos a falar também em redefinir aquilo que é o leque de competências com que as pessoas devem sair daquilo que são os órgãos de educação institucionais para enfrentar a vida no nível do ensino secundário, do ensino universitário, mas também, e é muito importante, do ensino vocacional, do ensino profissional. E isso é muito importante porque muitas vezes se pensa nisso focando apenas as novas gerações, muito com a ideia de que é necessário que eles fiquem familiarizados com aquilo que são os computadores pessoais, os *smartphones*, o *software*. Isso é de fato importante, mas eu até me atrevo a dizer que, para as crianças, os nativos digitais, como às vezes se convenciona falar, isso é de alguma forma intuitivo. Uns começam a aprender aquilo com facilidade por ter uma plasticidade cognitiva que as pessoas que já têm uma experiência de vida mais longa têm dificuldade em desenvolver. Por isso é muito importante focar muito naquilo que a população adulta tem mais dificuldade em assimilar, essas mudanças que, de alguma forma, desafiam aquilo que é o seu conhecimento estabelecido.

A Comissão Europeia desenvolveu, em colaboração com os Estados-membros, uma inciativa que é o quadro de competências digitais para os cidadãos. Só para citar alguns pontos que eu há pouco mencionei: a capacidade de procurar informação na internet, ajuizar a sua credibilidade, combinar várias fontes de informação e dados para poder, em função disso, tomar decisões informadas, saber interagir com os outros, respeitando regras de etiqueta apropriadas. As pessoas, no cotidiano, normalmente não se insultam de uma forma aberta e frontal. Basta ver, por exemplo, aquilo que é o exemplo das caixas de comentários dos meios de comunicação social para se perceber que há, de fato, coberto de um suposto anonimato, às vezes, comportamentos antissociais que são inadmissíveis naquilo que é uma sociedade que se rege por princípios, digamos, de cordialidade e respeito pelos outros.

Naturalmente, todos os aspectos têm a ver com identidade digital. É uma coisa essencial, de fato, não diria ter, mas pelo menos controlar o acesso ao anonimato nas redes sociais, o acesso ao anonimato na internet. Uma questão essencial é que, no cotidiano, nós não aceitamos pacificamente que as pessoas apareçam, digamos, de cara vendada. A sua identidade é uma forma também de elas se sentirem responsáveis por seu contributo para um advento coletivo. Se a pessoa chegar a um banco com a cara vendada, está obviamente a fazer um assalto. Isso é uma coisa que ainda não foi totalmente conscientizada quando falamos nas redes sociais e na internet.

Importantíssimo proteger a segurança minha e dos outros, porque cada vez mais as nossas fragilidades...

(Soa a campainha.)

O SR. CARLOS OLIVEIRA - ...são fragilidades que abrangem o coletivo; salvaguardar a privacidade, a nossa e a alheia; respeitar a propriedade e, também, porque isso é um espaço de fruição coletiva, promover um uso criativo e inovador das tecnologias da informação. Isso é um plano geral que se tenta pôr em desenvolvimento em muitas outras políticas públicas europeias em áreas como a cibersegurança. Esse é um debate que preencheria quase toda a minha intervenção, de forma que eu manifesto a minha disponibilidade de aprofundar essas matérias. Mas há um conjunto de diretivas e políticas em nível europeu sobre segurança de informação na rede. Há uma entidade, que é o centro europeu de segurança informática, a Enisa, que dá orientações que são extensivas ao conjunto da União Europeia.

Proteção de dados. Eu também não vou me alongar, mas a entrada em vigor do regulamento geral de proteção de dados é uma medida muito específica nesta área, que está associada - porque falamos aqui em questões de cibersegurança - a ações específicas sobre polícia e cooperação judiciária, em que um País como o Brasil também está empenhado.

Estamos a falar em questões também de pesquisa e inovação, em que há todo um conjunto de ferramentas. Toda gente agora fala de inteligência artificial. Isso também serve para tornar as redes mais resilientes e menos vulneráveis a esses aspectos. Há um conjunto de atividades de pesquisa e inovação que também se focalizam em questões como, por exemplo, *fake news*, em questões de segurança, em questões de privacidade. Falamos em questões, por exemplo, agora é muito habitual, como cibermoedas. Mas, de fato, a tecnologia que está por trás das cibermoedas é também algo que permite

uma melhoria das cadeias de confiança que existem sobre as notícias e sobre a informação. O *blockchain* tem como base, digamos, um aspecto importante disso.

Um aspecto que foi mencionado anteriormente e que eu gostaria de citar, até servindo de cumprimento ao Thiago, são as atividades ligadas ao Safe Internet Day, que tem expressão não só na Europa, mas com colaborações a nível mundial, nomeadamente no Brasil. Tudo isso, digamos, faz parte de um edifício que está a ser construído e que nós designamos como mercado único digital. Nosso objetivo é, de fato, criar um quadro regulatório que abranja seguramente os países europeus, mas que tenha cada vez mais pontos com aquilo que são o quadro regulatório e as medidas de proteção que sempre ficam nos países com os quais existem particulares afinidades, como é o caso do Brasil.

Nós temos vindo colaborar com o Brasil nessas matérias desde longos anos. A parceria estratégica entre União Europeia e Brasil completou, em 2017, dez anos. E este é também o ano em que nós tivemos o 10º Diálogo em Sociedade da Informação, precisamente entre a União Europeia e o Brasil. Isso tratou de um conjunto de atividades muito vasto. Eu não vou entrar nos detalhes, mas estamos a falar em mais de 50 milhões de euros que foram coletivamente investidos em pesquisa e inovação sobre essas matérias. Estamos a falar também em aspectos que são essenciais quando falamos de cibersegurança, que é quando nos referimos geralmente como internet das coisas, computação de nuvem, aspectos de segurança que são absolutamente cruciais e centrais para viabilizar esses desenvolvimentos. E também das aplicações dessas tecnologias em domínios de relevância social e econômica, manufatura avançada, gestão da água, cidades inteligentes, governo digital. Essas coisas não vivem se nós não tivermos uma visão sistêmica de como a transformação digital está a se processar e abrange, como foi muito bem mencionado, os aspectos da segurança e da cibersegurança, os aspectos da cidadania, os aspectos da educação.

(Soa a campainha.)

O SR. CARLOS OLIVEIRA - Eu gostaria de terminar reiterando a minha saudação ao Senado por tomar essa iniciativa e de manifestar, naturalmente, a minha disponibilidade para facultar informação mais ampla sobre as iniciativas europeias. Vou oportunamente fazer chegar a lista dos *links* com essa informação, sendo que uma boa parte desses documentos estão exclusivamente em português, que é uma das línguas oficiais da União Europeia.

Muito obrigado por vossa atenção.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Obrigado, Dr. Carlos Oliveira.

Passo a palavra a Cristhiane Andrade França. Ela é delegada da Delegacia Especial de Repressão aos Crimes Cibernéticos.

A SRª CRISTHIANE ANDRADE FRANÇA - Em nome da Delegacia Especial de Repressão aos Crimes Cibernéticos, eu gostaria de agradecer o convite para falar a esta Casa e de ressaltar a importância de falarmos acerca da educação digital como prevenção aos crimes cibernéticos. O empirismo do nosso dia a dia como policiais tem demonstrado que esse é um fator essencial na prevenção desse tipo de crime, uma vez que é um fator determinante a ocorrência desse tipo de crime quando a pessoa não tem nenhuma noção de tecnologia, ou, se tem noção de tecnologia, não sabe como lidar com aquela tecnologia de forma adequada.

A DRCC, que é a Delegacia Especial de Repressão aos Crimes Cibernéticos, foi criada pelo Decreto distrital nº 38.098, de 30 de março de 2017, atendendo a uma necessidade premente da Polícia Civil do Distrito Federal, uma vez que a quantidade de crimes cibernéticos tem aumentado anualmente em cerca de 40%.

Quando nós falamos de crimes cibernéticos, não houve ninguém que tenha feito essa classificação aqui, mas dizemos que os crimes cibernéticos podem ser: crimes cibernéticos próprios, crimes cibernéticos impróprios ou, então, crimes cibernéticos propriamente ditos ou aqueles que são cometidos por meios cibernéticos. Os próprios são aqueles que necessitam da tecnologia para serem cometidos, e os outros, que são os impróprios, são os diversos tipos de crimes que nós temos no Código Penal e em toda a legislação especial, em que o meio utilizado é a internet, o meio tecnológico para cometimento desses crimes.

A Lei 12.735, de 2012, impôs que os órgãos de polícia judiciários estruturarão, nos termos de regulamentos, setores e equipes especializados no combate a ação delituosa em redes de computadores, dispositivos de comunicação ou sistema informatizado. Portanto, uma delegacia que apure esse tipo de crime só está atendendo ao imposto, a uma exigência social e a uma determinação legal. A DRCC, que é a sigla pela qual nós chamamos a Delegacia Especial de Repressão aos Crimes Cibernéticos, tem uma equipe especializada tanto de investigadores quanto de delegados que atuam especificamente na apuração desses crimes.

É importante ressaltar que, na maioria das vezes em que qualquer crime ocorra, no andamento das investigações, pode acontecer alguma quebra de sigilo. No entanto, isso ocorre no andamento das investigações. No caso das nossas investigações, em quase 100% dos casos é necessário uma representação ao Poder Judiciário. Então nós produzimos representações sistematicamente, quase todos os dias representamos ao Poder Judiciário, pedindo alguma quebra de sigilo.

Quando se fala em educação digital, na prevenção dos crimes cibernéticos, esses crimes devem ser abordados sob dois aspectos. O primeiro aspecto deles é a educação digital como forma de impedir e desestimular o indivíduo ao cometimento de crimes e também a educação digital como forma de prevenção à vitimização a esse tipo de crime. Muito vemos na doutrina uma produção sistemática de trabalhos a respeito do comportamento das vítimas nesses crimes. No entanto, é importante ressaltar que nós devemos produzir uma educação digital com vistas a aumentar uma consciência de que a internet é uma ferramenta criada essencialmente para ser usada de forma lícita. Sendo assim, somente se deve fazer na internet o que a lei permite.

Ademais, é importante demonstrar que o anonimato proposto pela rede não é eterno, é apenas temporário. Muitas vezes a polícia não consegue descobrir o autor de determinado crime naquele primeiro momento. Entretanto, no andamento das investigações, em quase 100% dos casos é possível se descobrir a autoria dos crimes.

Tratando-se da educação digital como meio de prevenção à vitimização nos crimes cibernéticos, é relevante dizer que a internet é um meio no qual todos estão anônimos e são iguais. Então ela é um meio extremamente democrático. Entretanto, o que a um usuário comum é permitido? Uma vastidão de possibilidades lícitas, como pesquisas diversas, ou observações de locais a milhares de distâncias, ou comunicação de pessoas em qualquer lugar do Planeta.

Para um usuário com intenções maliciosas, a internet se torna um meio, um instrumento poderoso para lesão de bens jurídicos diversos. Diante de tal constatação, pode-se perceber que no meio virtual o comportamento das pessoas é destituído de muitas cautelas. Elas julgam que, por estarem em suas casas, por terem um antivírus, por utilizarem algum *software* de segurança, elas estão totalmente seguras e não vão ser lesadas em seus bens jurídicos. Só que muitas vezes as pessoas, na vida comum, deixam de frequentar determinados locais para não serem vítimas de diversos crimes. Na internet, não; elas se comportam de forma descuidada, visitam *sites* não confiáveis, acessam *links* que desconhecem, conversam com pessoas que nunca viram pessoalmente e muitas vezes compartilham seus dados pessoais, imagens e vídeos com essas pessoas.

É claro que muitas pessoas que são diligentes no meio cibernético também podem ser vítimas desse tipo de crime, uma vez que muitos criminosos buscam sempre explorar as vulnerabilidades dos sistemas operacionais e dos *softwares* de segurança. Apesar disso, o tipo mais comum de vítima que nós vemos na delegacia é aquela vítima descuidada e muitas vezes solitária, gananciosa, curiosa e que também desconhece as ferramentas digitais.

Os crimes que mais geram registros de ocorrência da DRCC e nas delegacias do Distrito Federal são os seguintes: crimes de estelionato, a internet oferece possibilidades diversas para o cometimento de todo tipo de crime de estelionato, mas o que nos chama muito a atenção e o que ocorre com frequência, chegam muitos casos desse tipo lá na delegacia, são os *love schemers*. Eu acho que algumas pessoas já devem ter visto isso na televisão. São golpistas que procuram mulheres solitárias e exploram essa vulnerabilidade delas. Eles criam perfis falsos de homens entre 40 e 50 anos que sejam divorciados, ou com filhos, ou viúvos. Eles conseguem atrair a confiança dessas mulheres e, a partir do momento em que conseguem atrair a confiança delas, começam a contar histórias mirabolantes para essas mulheres, inventam uma história a respeito de um pacote que vai ser enviado, e esse pacote é enviado para elas. Dizem que nesse pacote vai constar uma documentação, joias e pedras preciosas. E essas mulheres, por acreditarem que essa história é verdadeira, acabam fazendo depósito para pagamento de taxas de alfândega. Nós tivemos um caso lá de uma mulher que pagou cerca de R$200 mil. Ela acreditou que aquela pessoa realmente existia, que eles tinham um relacionamento amoroso, e acabou fazendo um pagamento de R$200 mil para essa pessoa.

Nós temos também os crimes de extorsão. Geralmente esses crimes acontecem da seguinte forma: o criminoso obtém da vítima imagens e vídeos íntimos, de alguma forma, ou consegue adicionar essa pessoa na rede social ou invade o computador dessa pessoa e consegue essas imagens, e começa a ameaçá-la, solicitando que ela pague determinada quantia. Em alguns casos, a pessoa fica tão... A pressão é tão grande sobre ela que... Nós tivemos um caso em que uma pessoa cometeu suicídio depois de tanta pressão.

Temos ainda a modalidade de crimes de extorsão denominada *ransomware*, que é um código malicioso que sequestra os dados dos indivíduos, e eles podem ou codificar esses dados - codificar, não, criptografar esses dados - ou impedir o acesso da pessoa àqueles dados, aí o criminoso solicita o pagamento de uma quantia em *bitcoins*, geralmente esse pagamento é feito em *bitcoins*. Esse tipo de crime vitima principalmente pessoas jurídicas cujo banco de dados contém informações sobre clientes, funcionários e projetos.

Nós temos também, com muita frequência, os crimes contra a honra, já que a internet se mostrou um terreno vasto para o cometimento de crimes dessa natureza, porque muitas pessoas acreditam que não serão descobertas. Destacam-se nesses crimes alguns casos em que as pessoas querem se vingar de antigos relacionamentos e espalham imagens e vídeos íntimos dessas pessoas. E também os casos das injúrias raciais, que são grupos no Facebook ou no Twitter que se organizam para fazer ataques a determinadas pessoas, geralmente pessoas famosas - nós tivemos o caso da Taís Araújo e da Maria Júlia Coutinho. E também os crimes cometidos no âmbito das eleições - nesse caso, os crimes acabam se tornando de ação penal pública incondicionada.

Foi dito aqui a respeito das *fake news*. É bom lembrar que o art. 323 do Código Eleitoral prevê que divulgar na propaganda fatos que sabem inverídicos em relação a partidos ou candidatos e capazes de exercer influência perante o eleitorado tem uma pena de detenção de dois meses a um ano. Então, não é simplesmente espalhar essas notícias falsas. Isso constitui também um crime do Código Eleitoral.

São muito frequentes também na delegacia os crimes de furto mediante fraude, principalmente com o *modus operandi* de envio de *phishing* por meio de WhatsApp e de SMS. A pessoa recebe aquela mensagem, acaba clicando em um *link* e aquele *link* infecta o sistema operacional do aparelho dela ou o computador dela e, quando ela tenta acessar a sua conta do banco, é aberta uma página falsa na qual ela digita a sua senha. Aí o criminoso acaba obtendo aquela senha da pessoa e todas as suas credenciais, entra na conta e consegue realizar diversas transações bancárias como empréstimos, transferências etc.

Há várias outras modalidades criminosas também, principalmente as de falsa identidade, de invasão de dispositivo informático. Nós temos muitos casos lá também de venda de drogas pela internet ou de comercialização de diplomas falsos. No entanto, nós esbarramos muito na análise da tipicidade. Fica até um alerta sobre a produção legislativa a respeito desses crimes, porque muitas vezes, por exemplo, o art. 154-A, quando fala de dispositivo, não está se referindo à invasão de redes sociais. Muitas vezes se acredita que a invasão da rede social seria um crime, mas, na verdade, se você analisar a tipicidade daquilo ali, o que seria dispositivo informático, não seria possível encaixar a rede social ou o *e-mail* como um dispositivo a ser invadido.

Apesar de muitas pessoas acreditarem que só são vítimas dos crimes cibernéticos aqueles que têm desconhecimento tecnológico a respeito desses crimes, a respeito da tecnologia, é importante ressaltar que muitas pessoas que têm conhecimento a respeito disso acabam se tornando vítimas. Nós temos muitos casos de pessoas que chegam à delegacia, têm conhecimento, utilizam objetos de alta tecnologia e sabem mexer com aqueles objetos, no entanto, acabam clicando em alguns *links* suspeitos, muitas vezes simplesmente porque a vida é tão corrida e tão cheia de informações que elas acessam aquelas informações de forma rápida e efêmera. Às vezes, de modo açodado e descuidado, elas acessam aqueles *links* porque não têm um cuidado especial, não fazem uma análise minimamente crítica a respeito daquilo.

Ultimamente, aproveitando-se desse clima de Copa do Mundo, nós recebemos lá, na delegacia, um *phishing*...

(Soa a campainha.)

A SRª CRISTHIANE ANDRADE FRANÇA - ... que trata das camisas da seleção. Eles pedem para a pessoa clicar e acrescentar os seus dados e ela vai acabar ganhando uma camisa da seleção.

Quando se fala do tema educação digital na prevenção da vitimização, deve-se entender que tal educação não se relaciona somente ao conhecimento técnico a respeito das tecnologias digitais, mas que é necessário um comportamento responsável e analítico diante da rede mundial de computadores. Sendo assim, não é exagerado dizer que todos nos comportemos na internet da mesma forma como nos comportamos na vida real, tendo cuidado com os nossos dados, tendo cuidado com as informações que repassamos para as outras pessoas. Quando o indivíduo ingressa na internet, ele deve ter a consciência de que, ao mesmo tempo, ele é uma vítima em potencial e até - em uma conversa com os colegas aqui isso foi dito - um criminoso em potencial. Então, é necessário criar uma conscientização de que deve haver um comportamento e até regras de etiqueta na internet, o que tornaria a vida mais harmoniosa e segura para todos os usuários.

Infelizmente, jamais chegaremos a um índice zero de criminalidade, uma vez que o crime realmente é um fato social, como já foi dito aqui, é impossível reprimir e chegar a um índice zero nesse tipo de crime. No entanto, para a prevenção efetiva dos crimes cibernéticos, a educação digital é essencial, devendo estar aliada a um aparato repressivo composto de uma polícia investigativa especializada e uma legislação que consiga atender às especificidades da investigação e punição de crimes dessa natureza. Então, é necessário que as delegacias especializadas sejam realmente criadas e que os policiais sejam qualificados para o atendimento desse tipo de crime e para a investigação desse tipo de crime, porque é uma investigação muito especializada, totalmente diferente da investigação convencional.

Obviamente, o assunto sobre o qual estamos tratando não se esgotará em uma discussão de apenas um dia dedicado a esse tema. No entanto, a abertura do debate é extremamente válida e muito importante.

Nós da Delegacia Especial de Repressão aos Crimes Cibernéticos da Polícia Civil do Distrito Federal agradecemos a oportunidade de contribuir com a construção dessa discussão.

Obrigada, Senador, pelo convite.

Boa tarde a todos.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Muito obrigado, Delegada Cristhiane.

Eu passo a palavra agora ao Professor Paulo Rená.

O SR. PAULO RENÁ - Senador, só para constar, além dos 13 minutos iniciais, qual é tempo que está sendo dado na prorrogação.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Eu falei 10, mas tenho dado 15 e tem sido mais do que 15. Fique tranquilo que você vai ter o mesmo que os outros ou mais até se for preciso.

O SR. PAULO RENÁ - Obrigado.

Pergunto até pelas instigantes falas que me precederam, todas elas gerando aportes aqui para poder acrescentar ao meu planejamento. Mas vou tentar me ater ao tempo.

Então, boa tarde a todos os presentes a esta audiência pública da Comissão de Educação, Cultura e Esporte.

Agradeço o convite do Senador Cristovam, historicamente ligado ao tema da educação.

Agradeço ao Senado por realizar o evento. É muito importante que a gente esteja aqui não debatendo um projeto de lei apresentado de forma de fundamentada, mas, sim, o tema, para propiciar uma alimentação, um debate para, então, a gente poder pensar sobre a temática. Eu acredito no Parlamento como um espaço de convencimento mútuo. O marco fundador da democracia é pensar que a lei é legítima quando é feita pelo povo e para o povo, de modo que o real debate e a discussão, com atenção e cuidado, são um pressuposto.

Viabilizar o encontro de argumentos sobre um tema tão importante como a educação, cibercrimes, com essa centralização nas *fake news*, é um esforço parlamentar que merece não apenas aplausos e agradecimentos, mas uma participação, então, da minha parte, à altura desse desafio.

Quero cumprimentar as pessoas da Mesa na pessoa do Senador Cristovam, que preside a Mesa; cumprimentar ainda quem está aqui acompanhando, o pessoal do Facebook e outras representações presentes; cumprimentar também quem está nos acompanhando *on-line* e, eventualmente, quem tenha participado por telefone - vou tentar acompanhar, ver se alguém fez alguma contribuição.

Bom, eu estou aqui apresentado como professor e pesquisador. Sou profissional contratado pelo UniCeub, também anualmente dou aulas no Iesb e mantenho o grupo de pesquisa Cultura Digital e Democracia, em que a gente pretende analisar quais os desafios que essa mudança tecnológica traz para as exigências políticas de participação. Além disso faço parte da ONG Instituto Beta: Internet & Democracia. A nossa proposta é fazer com que a internet se torne cada vez mais democrática, ao mesmo tempo em que a gente quer que a democracia cada vez mais reconheça a internet como um espaço público produtor de significados politicamente relevantes, partindo do pressuposto de que não necessariamente a internet vai ser mais democrática e não necessariamente a democracia vai usar a tecnologia da forma correta.

Nós do instituto temos uma participação em diversos momentos. Destaco aqui a nossa presença, no ano passado, falando na audiência do STF a respeito dos bloqueios do WhatsApp. São duas ações que tratam de combater crimes de tráfico. Foram determinados bloqueios no uso de um programa de comunicação instantânea entre pessoas que não têm nada a ver com a história. Será que isso é democrático? Então, o debate no STF migrou para a questão da criptografia, mas está obviamente dentro do que a gente trabalha na ONG.

Quero destacar também que o Instituto Beta, em conjunto com 40 outras organizações, pesquisadores e ativistas, compõe a Coalizão Direitos na Rede, que tem algumas campanhas, alguns projetos também relacionados à ideia de que os nossos direitos hoje dependem de uma atuação cuidadosa, de um olhar bastante atencioso à internet como um possível, um efetivo espaço de novas violações de direitos, mas também como um espaço de construção conjunta de uma sociedade melhor. Então, é para a gente não criminalizar o uso da internet, primando pela liberdade de expressão e pela privacidade.

Meu roteiro aqui é falar de educação digital e cibercrimes, pontuando como a educação digital pode ser utilizada, a partir das perguntas que o Senador colocou, como assegurar aos internados que seus dados sejam preservados, como tornar a sociedade mais preparada e consciente em relação aos crimes cibernéticos, como proteger crianças e adolescentes. E aqui eu destaco a minha atuação em sala de aula. Fui professor de direitos da criança e do adolescente, sou professor de

responsabilidade civil. E os casos que chamam mais a atenção dos alunos são os relacionados às questões *on-line*, que têm lugar nas manchetes dos jornais.

Ao mesmo tempo, eu sinto uma falta de compreensão não só dos meus alunos, mas, de maneira geral, dos conceitos básicos do Direito para a gente poder tratar de questões penais, de questões de sanção civil porque, no Brasil, a gente está vinculado aos preceitos constitucionais.

Bom, falando, então, propriamente de educação digital, quero destacar o que já foi dito, tanto pelo representante da União Europeia, o Carlos Oliveira, como pelo Thiago Tavares, brilhantemente, no sentido da *media literacy*, ou, em português, a alfabetização para o uso das mídias.

É necessário, Senador, que a gente hoje ensine as crianças a ler, escrever, interpretar, a fazer conta, mas também a mexer no computador, a mexer no celular.

O Senador tem uma frase interessante, ao dizer que é curioso como os tribunais, o Senado, eventualmente, quando vai descartar os computadores faz uma doação para as escolas.

Isso é maravilhoso, mas o ideal seria que as escolas estivessem doando computadores para o Senado e para o tribunal. Como assim uma criança vai estudar com um computador desatualizado? Essa é uma questão de prioridade, e se eu pudesse encerrar minha palestra agora dar essa proposta seria isso. É necessário que as crianças tenham um primeiro acesso às tecnologias.

Então, estou falando aí nesse caso de educação formal, no âmbito da educação digital. Para esse propósito, Senador, eu destaco que o Marco Civil da Internet tem uma proposta expressa, vigente desde 2014, completamente ignorada.

Quero crer que o Senador conhece o art. 26, que diz:

> *Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.*

Pronto, temos lei. Isso que o Marco Civil da Internet diz com todas as letras há já quase quatro anos, na minha percepção de quem acompanha, foi zero implementado.

A gente teve uma limitação de recursos para a educação para 20 anos; não vejo como a gente pode ter algo mais do que uma aulinha de informática em que o aluno vai ficar completamente desinteressado. É impossível um professor em 50 minutos ensinar algo que crianças, adolescentes e jovens não consigam fazer com seu próprio celular de forma mais interessante.

Não vejo capacitação de professores para educar as nossas crianças e adolescentes de forma que eles construam o nosso futuro, que eles se vejam alfabetizados, autônomos, detentores, emancipados para a internet.

Claro, isso é questão de longo prazo. Então, além da educação formal, a gente tem que pensar também em quem já está atuando, na questão da atualização dos profissionais. Estou pensando aqui em juízes. Quantas decisões catastróficas a gente vê de juízes, bem-intencionados, inclusive, mas que apresentam decisões completamente desconexas do que a internet precisa.

Para isso, a gente tem o Marco Civil, que é o fundamento, a base, mas o Marco Civil é de 2014. Quando os juízes aprenderam o Direito? Nos anos 80, nos anos 70. Então, a gente tem que ter atualizações do STF ao juiz que acabou de ser nomeado.

No Ministério Público, a gente tem alguns casos de Promotores, de Procuradores que buscam se atualizar, mas cadê uma atuação institucional do Ministério Público para promover essa atualização com relação aos potenciais da cultura digital?

Advogados... A presença do Fabrício aqui como representante da OAB pode servir para agente veicular essa encomenda, para que os advogados se atualizem talvez até de forma obrigatória. A gente pode estabelecer um prazo de 10 anos, 15 anos, 5 anos. Mas o que não pode acontecer é um cliente contratar um advogado para defendê-lo *on-line* e advogado não ter a menor ideia de como fazer isso ou faz tudo errado.

E aí o que a gente vai ver muito são clientes que perdem o seu direito porque o advogado atual mal, e o cliente não tem condição de avaliar o advogado. Não é sabão em pó em que ele pode dizer: "Na próxima roupa eu compro uma marca diferente." Escolheu o advogado, o advogado atuou errado, ele perdeu a causa e acabou. Não tem controle de mercado.

Provoco também aqui os Parlamentares no sentido de que busquem também essa atualização. Há espaços, essa audiência pública é um ótimo espaço para essa atualização. Infelizmente, a gente não tem um Plenário lotado de Parlamentares devidamente interessados. E também professores, obviamente, eu acompanho meus colegas e vejo que nem todo mundo está a par, nem todo mundo se sente à vontade, mas nem todo mundo tem um mínimo.

Um professor de Direito Civil tem que saber português; o professor de Direito Civil, hoje, não tem que saber diferenciar *e-mail* de *web*, de *deep web*, de mensageiro, de Pier2pier, de Instagram, de Snap? Tem que saber.

Quando que ele vai saber com a remuneraçãozinha que ele recebe, com férias de três semanas no meio do ano? Não dá tempo. A gente tem que ter um projeto.

Talvez o Senado, por meio do Instituto legislativo Brasileiro, que é uma escola de governo, junto com as outras 20 escolas de governo, pudesse empreender algum tipo de atuação, inclusive, junto ao Poder Judiciário, para poder realizar essa atualização de profissionais.

A gente fica falando da população aqui. Todo mundo acompanhou o caso do Parlamentar, da juíza que se manifestaram de maneira completamente errônea no caso da Marielle.

A gente não está falando de pessoas que são analfabetas. São pessoas de todas as classes, como bem foi dito, estão propensas a praticar cibercrimes e a serem vítimas de cibercrimes.

Então, a sociedade, de forma ampla... A gente precisa promover uma circulação social dos saberes. Eles não podem ficar só na escola, só nos cursos de atualização.

Então, a gente tem cartilhas do CGI, cartilhas da Safernet. A OAB produz bons materiais. E a gente tem que promover familiaridade com temas como segurança. A gente sabe que, por exemplo, a fechadura da minha casa... Eu não quero que a delegada tenha acesso a uma chave mestra que abra a minha casa. E aí a gente vai pensar em senha, em criptografia e, de repente, parece uma ideia legal que o Estado possa ter um *backdoor* ao meu computador.

Falta a familiaridade de entender que pelo computador você consegue saber tudo o que a pessoa está fazendo, em especial pelo computador dela, pelo celular dela. A gente tem a ideia de que a casa é um asilo inviolável pela Constituição, e a gente tem artigos do Ministro Gilmar Mendes - e já deve ter 10 anos esse artigo -, retratando que na Alemanha existem decisões da suprema corte, reconhecendo que o celular merece a mesma proteção, porque se eu não entro na sua casa de 10 da noite às 6 da manhã, olhando o celular eu sei tudo o que você fez de 10 da noites às seis da manhã, às vezes, até como foi o seu sono - se usar um aplicativo para acompanhar como vai a saúde.

E aí temos a questão da biometria para proteção de dados pessoais; não tratar com descaso... O TSE estava tratando com descaso os nossos dados naquela relação com o Serasa. E agora o TSE vai ser detentor do banco de dados biométrico de toda a população eleitora do Brasil.

Quem está preocupado com a segurança da guarda desses dados? Quem vai verificar o TSE?

Quanto aos bancos. Tem as questões do bitcoin, mas tem também o comércio eletrônico, paga-se com o celular uma conta hoje facilmente, com uma pulseira.

O jornalismo tem a questão das *fake news*, que vou adentrar, mas tem o velho compartilhamento de mídia, a pirataria, memes. O meme é pirataria. Quando a gente circula a Nazaré Confusa, para quem conhece. Agora a gente vai entrar na Copa do Mundo, há circulação de memes. Eu pego uma imagem da Rede Globo e ponho um texto em cima, isso é violação de direito autoral. No nosso País, isso é crime. Art. 184 do Código Penal: violar direito autoral. A gente podia mudar essa lei.

(Soa a campainha.)

O SR. PAULO RENÁ - Senão, as crianças que estão se alfabetizando estão cometendo crimes. Na Lei de Direito Autoral, não tem exceção para produzir meme, por exemplo.

O discurso de ódio *on-line* é uma encruzilhada, porque a gente tem que promover os direitos humanos, mas a gente não pode violar os direitos humanos sistematicamente para promover os direitos humanos. É um absurdo vigiar todo mundo para impedir que as pessoas agridam umas às outras. O Estado vai violar os nossos direitos sistematicamente ou as empresas vão ser obrigadas a violar o nosso sigilo para identificar quem está cometendo crime, quem não está? Isso em si é um crime.

A questão da neutralidade de rede, sem a qual isso já tem uma familiaridade, mas ainda pouca gente conhece, mas sem neutralidade de rede não tem como a criança aprender. Como ela vai subir um vídeo se só com o YouTube tem liberdade de acesso, mas não tem com o Vimeo, não tem com o Facebook? Eu tenho contrato com a Tim, no WhatsApp eu posso mandar texto e foto, não posso mandar vídeo. E os vídeos que eu produzo? Não vão subir, eu posso consumir, mas não posso produzir. Neutralidade de rede é importante para isto: protege a inovação, o que a gente não sabe o que vai ser, porque ainda não foi inventada, então, a gente tem de manter em aberto. É difícil ver o valor da inovação. É difícil, por isso, entender a neutralidade de rede. Aí a Anatel vem dizer que *Zero Rating*, que a não cobrança não é violação da neutralidade de rede. É, porque, se eu não cobro do ICQ, nunca vou ter WhatsApp. Se eu não cobro do Orkut, nunca vai ter Facebook no Brasil. Se eu não cobro do Facebook, qual a próxima rede social que a gente está matando sem nem conhecer?

Na questão de transporte, a gente pensa em Uber. Todo mundo debate o Uber. Tem o Waze. O Waze sabe a que velocidade eu vim para cá, que horas saí de casa, por onde passei. Eu não quero que os dados do Waze sejam utilizados para fins que não aceitei quando eu contratei o uso do Waze. Tem lá um banco de dados riquíssimo meu, do Senador, da plateia, do Presidente da República, dos seus assessores. É questão de Estado, é questão do indivíduo. Isso é muito sério. A gente tem de se familiarizar com essas discussões, que não são novas.

O Senador perguntou desde quando há cibercrime. O termo é de 1999. Virou Convenção de Cibercrimes na Europa, da qual o Brasil não faz parte, em 2001. Um Senador tentou fazer essa Convenção de Cibercrimes ser interiorizada, depois ele virou Deputado, agora está com ordem de prisão, mas esse Senador tentou trazer uma lei para o Brasil de graça. Sem que o Brasil fosse convidado a participar da convenção, ele pegou o texto, traduziu e quis transformar em lei. Daí surgiu o Marco Civil da Internet, em resposta a essa proposta de trazer o termo cibercrime para o Brasil antes da hora, porque a gente não tinha maturidade.

Mas violação há desde 1960, desde que se tem acesso a um sistema por sabotagem, isso estava classificado como crime contra a informática. Em 1980, a gente tinha cartão de crédito, o medo do cartão de crédito, dos caixas automáticos. Se procurar no YouTube, a gente acha notícias engraçadíssimas da época: você vai ter coragem de usar um cartão em que você pode pegar o seu dinheiro sem ir ao banco? Hoje é a mesma coisa com pagamento por celular, uso de bitcoin. Não é novidade. A discussão não é nova. O termo cibercrime existe há pelo menos 17 anos.

Então, vamos falar de cibercrimes. Essa história do Marco Civil é interessante porque, no Senado, a gente teve um momento crucial de debates para a evolução do Marco Civil da Internet, que foi quando, por meio de blogues, diversos blogueiros conseguiram criar um momento que parou a tramitação do Marco Civil, por um momento, aqui no Senado, e depois foi aprovado. Após uma audiência pública realizada na época - o Pedro Abramovay era o Secretário de Assuntos Legislativos do Ministério da Justiça -, foi aprovado, foi para a Câmara. Como havia modificações, conseguimos parar o projeto na Câmara. Daí, surgiu a demanda: antes de falar que as pessoas têm que ser presas, vamos dizer quais direitos podem ser violados para que elas eventualmente tenham sua liberdade restrita ou sejam alvo de uma sanção.

Antes que o Marco Civil virasse realidade, a gente teve a Lei Carolina Dieckmann, pelo acontecido, mas a delegada não vai me desdizer aqui que a Lei Carolina Dieckmann não serviu. Ela não resolve nem o caso da Carolina Dieckmann, porque, no caso dela, foi acesso ao computador, e a lei não fala em acesso a computador; fala de invasão. Como bem colocou a delegada, invasão quer dizer entrada. Eu não entro em lugar nenhum; eu acesso. No Direito Penal, você tem o princípio da legalidade estrita. Se está invasão e eu acessei, não é invasão, eu não posso ser preso. Imaginem o trabalho que os delegados têm que ter, o Ministério Público, o juiz. É Direito Penal, o juiz não pode conceder interpretações abrangentes, têm que ser restritivas.

Ao mesmo tempo, com relação à classificação do cibercrime, quais são as distinções? A Lei de Cibercrimes fala em algumas categorias. A Convenção de Cibercrimes, lá em 2001, categorizou como crimes contra a confiabilidade, a integralidade, a disponibilidade dos dados, quer dizer, eu posso corromper, falsear ou inviabilizar o seu acesso aos seus próprios dados. Crimes relacionados a conteúdo, acho que as *fake news* entram aqui, mas não só, também o discurso de ódio; crimes relacionados à propriedade intelectual. Repito, no Brasil, violar direito autoral, por mais absurdo que possa parecer, não é uma questão de pagar uma indenização; é crime com detenção de três meses a um ano. Se tiver lucro indireto, essa pena sobe de dois a quatro anos. Não faz o menor sentido isso ainda estar previsto no Código Penal. Ninguém vai preso por violar direito autoral. Mas, num ambiente de perseguição, um delegado mal-intencionado pode pegar, abusar e restringir a liberdade de alguém que estava fazendo algo completamente lícito, como, por exemplo, denunciar esse delegado. Aí eu copio a foto do delegado. O delegado fez a própria foto, é autor da foto, você usou sem autorização, cometeu um crime.

A gente tem diversas situações de assassinatos cometidos por policiais mal preparados por meio dos autos de resistência. A gente tem de lidar com a realidade em todo o seu espectro. Criar crimes que possam abrir para abuso não vai solucionar nada, em especial porque a gente não sabe como vai ser o Brasil depois das eleições. Eu espero que a gente seja mais democrático e não menos.

Falando, então, sobre o tema que ganhou esta centralidade aqui, das *fake news*, sendo bem sintético: a gente não deve criminalizar *fake news*, para dizer que *fake news* é crime...

(Soa a campainha.)

O SR. PAULO RENÁ - ... porque a gente já tem o suficiente no nosso Código Penal, mais do que suficiente. A gente tem tipos penais que, eventualmente, são desconhecidos por parte dos profissionais na aplicação para a internet. Esse debate tem que ser público, não pode acontecer na delegacia, no gabinete do Ministério Público, no gabinete do juiz; tem que

acontecer aqui. A gente tem que revisitar o conceito, como bem coloca o Senador no requerimento, de injúria, calúnia, difamação, o que é, o que não é.

Alertar a sociedade, diz o Senador Cristovam, sobre os limites e o uso responsável da internet, promover a construção de um senso crítico, para que as *fake news* e a desinformação não tenham a força e a influência que hoje possuem nas decisões políticas de um país, tendo o exemplo dos Estados Unidos.

Mas eu quero lembrar que, no Brasil, em 1989, a gente teve uma conhecida notícia falsa a respeito de um dos candidatos, que, provavelmente, comprometeu o sucesso do Lula à época nas eleições, na disputa contra o Collor. Não é uma novidade que notícia falsa influencia no processo eleitoral. Quem morou em Município do interior sabe como é feita a disputa pelo político detentor do canal de TV, do jornal, do alto-falante. *Fake news* não é novidade. No Brasil, a gente está cansado, eu estou cansado de notícia falsa influenciando na política, sim, não é de hoje, não é pela internet, não começou na internet. A internet revisita todos esses temas, mas, se a gente mirar só na internet, se a gente mirar em *fake news* só no período eleitoral, a gente cria um novo art. 184 no Código Penal. Não vai servir para nada de útil, só para abusos.

A gente tem diversos projetos tramitando. Qualquer lei hoje seria prematura, porque a gente ainda não entende, falta diálogo, ainda não há base social. Os projetos que existem têm terminologia imprecisa, impondo dever aos intermediários, como a Convenção de Cibercrimes previa. E o Marco Civil superou esse debate. Eu não posso matar o mensageiro, senão ele não me entrega a mensagem. Se eu disser que quem me entrega uma notícia falsa é responsável, essa pessoa vai analisar tudo que está sendo entregue para mim. Se eu falar para os Correios: "Não me entreguem uma carta que me ofenda", o que os Correios vão fazer? Ler todas as minhas cartas. Eu quero isso? Não quero. Senão os Correios vão ter de me indenizar porque me entregaram uma carta que não sei de quem é. Anonimato é proibido, o.k., mas os Correios vão ter de ler a identidade da pessoa e verificar para saber se podem mandar a carta? Não vão, senão a carta não chega.

No YouTube, no Facebook, no Instagram, você tem horas de vídeo por minuto. A gente pode resolver isso, é só matar a internet. Se eu coloco um editor que vai ler tudo o que acontece antes de permitir a comunicação, isso tem um nome que é proibido na nossa Constituição. Isso se chama censura - e não é nada novo. É o problema central ameaçar a liberdade de expressão.

Isso gera também, mesmo sem um cenário caótico, autocensura: estou com medo, pois será que vou botar na capa de jornal uma manchete que vai ser enquadrada? Há exceções, mas será que a minha é exceção? O editor fala: "Não precisamos comprar essa briga, tira." E aí o repórter, da próxima vez, já não vai ser tão investigativo. Quem é que perde com isso no momento eleitoral? Corremos o risco - espero que, cada vez mais, esse risco seja menor - de termos eleições muito chapas-brancas, porque só vamos ter notícias favoráveis, só elogios, para tudo quanto é candidato, nenhuma crítica, nenhuma denúncia. Esse não é o tipo de eleição que eu quero ter. Como eu disse, eu estou cansado. Espero que o meu sentimento não seja único.

Vou falar de uma política que já não pode mais concorrer: a Marielle. Aí eu tenho um exemplo em que a participação da internet serviu para desmentir tudo o que estava sendo dito sobre ela. Desculpem-me por eu me emocionar; é sincero, porque, quando a Marielle morre, morre uma parte de todo mundo que luta por direitos humanos. Não foi o assassinato de um político que estava concorrendo, foi de uma ideia; tentaram matar uma ideia. E houve diversas pessoas desdizendo; não foi a grande imprensa que desmentiu, porque a grande imprensa não estava nem ligando para o que estava circulando no WhatsApp, no Facebook; foram grupos organizados em torno das ideias da Marielle que vieram desdizer.

Se colocamos um intermédio para avaliar, não vai dar tempo de desdizer; quem mente, mente mais rápido - fiz uma mentira, desmentiu; fiz outra, desmentiu; eu vou fazer 15, 30... Não é intermediário, temos que usar a rede. A rede é feita de nós que não são só descentralizados; eles são difusos, em que não é preciso passar por um ponto central para chegar a um outro. A ideia da internet como fundamento militar foi: eu tenho que comunicar desta mesa até o Thiago; se eu rompo a comunicação no Senador Cristovam, ela não chega lá; então, eu tenho que ter uma rede para saber até se essa comunicação foi rompida nesse ponto. É daí que surge a internet como rede, para poder contornar qualquer bloqueio na comunicação. Aí queremos resolver as *fake news* bloqueando a comunicação? A comunicação vai continuar acontecendo por meios cada vez mais ilícitos, prejudicando a educação, pois como um professor vai ensinar uma criança a cometer crime?

Além da imprecisão dos termos que é destacada pela ONU, pela OEA e por outras organizações mundiais, há uma carta aberta de representantes da sociedade civil da América Latina e do Caribe com as preocupações para *fake news*.

Exemplo de texto... Falam que o texto é ruim. Há texto que fala que é crime divulgar notícia que possa distorcer a verdade... Possa distorcer? Não precisa nem distorcer? Corromper gravemente a verdade no processo eleitoral. Há jeito de corromper que é leve, médio, grave? Só o grave que é punido? Podem dizer: "Ah, esse foi médio, não precisa punir." Qual é a verdade? Houve um caso semana passada de uma decisão que mandou tirar um *site* a título de *fake news*, uma decisão do TSE. O *site* estava divulgando uma notícia da Folha, o editorial da Folha de ontem criticando essa decisão, porque a

notícia é verdadeira - ela está de um jeito sensacionalista, mas ela é verdadeira. Então, os projetos erram na mira, acertam coisa demais.

Fake news são um problema complexo de desinformação, que...

(Soa a campainha.)

O SR. PAULO RENÁ - ... precede à internet, pois a desinformação já existia muito antes. Aí há no jornalismo busca por audiência a qualquer custo. Há disputa por poder também, em que os meios de comunicação tradicionais se envolvem, seja como mecanismos, seja como diretamente interessados.

O processo eleitoral. O Senador já foi prejudicado num processo eleitoral por conta de um *outdoor*... São três dias para recorrer. Um político com uma equipe consegue recorrer em três dias, um indivíduo não consegue. E esse é o processo eleitoral em que vamos debater *fake news*? Agora, as consequências não vão se encerrar nesse processo eleitoral.

Para finalizar, cumprimentando a participação de todos, agradeço poder falar por último, por poder ter todo esse conhecimento acrescentado, e peço mais dois minutinhos para me referir ao que o Dr. Emilio Simoni falou a respeito do cibercrimes - que, em 2006, estavam se estruturando. O pessimismo é lembrar que há notícia da Folha Online do dia 19 de novembro de 2002 dizendo que o Brasil lidera o *ranking* mundial de cibercrimes. Em 2002! Já estava estruturado em 2002, não era uma novidade!

De que cibercrime estamos falando? Precisamos de dados, precisamos estudar, porque o cibercrime de sabotagem é diferente do cibercrime de publicidade veiculada no YouTube para crianças. Uma dica de quem tem dois filhos: veja os vídeos junto com os seus filhos. As crianças aprendem pelo exemplo; se você as terceiriza para televisão, para a babá eletrônica... O problema já acontecia nos anos 80, nos anos 90. O que víamos nas manhãs de domingo nos anos 90 não servia para nenhuma criança. O que está no YouTube hoje também... Nem tudo serve, mas há coisa que serve no YouTube, na Netflix etc.

Enfim, agradeço também o esforço da PSafe de produzir dados. Isso é uma coisa que falta, Senador. O Marco Civil da Internet tem muita encomenda para produção de dados, e há pouca resposta a essa encomenda. Então, há a quantidade de crimes que as pessoas que usam aplicativo no Android denunciaram... Ainda não dá nem para questionar os dados, porque eu não sei qual o universo dessas pessoas no âmbito das pessoas que usam internet no Brasil, com Android, com iPhone, no computador... Temos que ter mais dados, mais dados empíricos para eu saber onde a Delegada não consegue atuar por falta de leis. Tem que haver dados. A Delegada não vai conseguir fazer estatística do trabalho dela; senão, ela não faz o trabalho dela. Tem que haver produção de dados para se tratar de *fake news*, de tráfico, de venda de arma, de tudo, com base na realidade. É um compromisso com a democracia que não geremos *fake news* para combater *fake news*.

É isso, Senador.

Muito obrigado.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Muito obrigado. Creio que foi muito instrutivo, deixando muitas provocações, que é o que a gente mais precisa para continuar buscando.

Eu passo a palavra ao Fabricio da Mota Alves, que é o último orador da Mesa.

O SR. FABRICIO DA MOTA ALVES - Senador Cristovam, Presidente da Mesa, agradeço, mais uma vez, aqui, a oportunidade de poder participar desta audiência pública.

Faço um registro de agradecimento ao Senador Pedro Chaves, que foi autor do requerimento que permitiu a minha presença aqui.

Registro os cumprimentos à Deputada Cristiane Brasil que está aqui presente; e ao Senador Dário Berger, que representa um Estado hoje tido como a nova Acrópole do empreendedorismo digital no Brasil. Santa Catarina, especialmente Florianópolis, é candidatíssima ao Vale do Silício brasileiro, tal a profusão de *startups* e de empresas de tecnologias que têm sido criadas, que têm surgido cada vez mais com grande taxa de êxito nesse Estado. Isso é digno de nota. Cumprimento os colegas da Mesa também, muitos deles meus amigos pessoais.

Senador, ser o último a falar é um fardo e, ao mesmo tempo, talvez seja um privilégio, dependendo de como se enxerga. Não vou cansá-los com muito do que já foi dito aqui, não há essa necessidade, mas há a possibilidade de identificar alguns tópicos que não foram tratados.

Também registro um agradecimento a duas pessoas que são colaboradoras do seu gabinete: a Diana Leiko e o Ricardo Durigan, que são realmente molas propulsoras dessa temática. Isso também é necessário se registrar.

Nesta discussão em torno da educação digital e sua vinculação com a prática criminosa, na verdade, se nós subtrairmos os adjetivos que constam dessa frase que nominam a audiência pública e colocarmos simplesmente "educação como instrumento de combate a crime", já estaríamos suficientemente tratando de um assunto extremamente relevante, porque é exatamente disso que se trata. A educação talvez seja a principal maneira de se combaterem práticas criminosas. Há um estudo de doutorado, uma tese de doutorado, que foi realizada pela USP, em 2003, em que se concluiu que, a cada 1% de investimento de recursos públicos em educação, há uma redução de 0,1% de taxas de criminalidade. Então, há uma relação direta econômica entre educação e taxas de criminalidade. Sabemos que, quanto mais investimos nesse aspecto, melhores serão os resultados para toda a sociedade brasileira.

Quando falamos em educação digital, há algo que a Drª Cristhiane colocou de forma bastante interessante. Ela trouxe ao eixo o aspecto da educação como instrumento para desestimular a prática criminosa, pois, quanto mais educados formos como sociedade, menos propensos estaríamos a práticas infracionais; o outro lado que ela apresentou seria a educação como forma de prevenção, ou seja, quanto mais conhecimento acerca dos instrumentos, dos serviços, do sistema de um modo geral, melhor a forma de prevenir o crime. Eu talvez sugeriria um terceiro eixo para essa fala da Drª Cristhiane, que é educação digital como instrumento colaborador da repressão criminal. Por que isso? Porque, infelizmente, como foi dito aqui por vários colegas da Mesa, as pessoas não têm conhecimento suficiente sobre tecnologia. O Brasil talvez seja uma das nações que mais bem utiliza tecnologia. Todo mundo aqui consegue instalar um aplicativo, todo mundo consome internet de forma efusiva e até mesmo com problemas de ética, comportamento social - está todo mundo numa mesa de bar, todo mundo saca o telefone, ninguém fala com ninguém, ficam todos tuitando e escrevendo no telefone, problemas dessa natureza. Só que, apesar de toda essa facilidade de acesso, nós não temos dimensão de responsabilidade. Não sabemos as consequências e não refletimos de forma crítica sobre as consequências do uso das tecnologias. Isso impede e dificulta muito o trabalho das polícias, da Polícia Judiciária, das forças policiais responsáveis pela investigação. Por quê? Porque boa parte da comprovação do crime, que todo crime tem que ser comprovado... Esse é o nosso sistema legal, nosso sistema constitucional. Primeiro, tem que haver a previsão legal, como o Renã mencionou. É preciso que haja uma lei prevendo aquela conduta como um crime. É o primeiro elemento. E o segundo elemento: é preciso que haja prova. Você precisa comprovar a prática criminosa, comprovar a autoria da prática criminosa. Isso, muitas vezes, é dificultado - se não completamente impossibilitado - porque as vítimas não têm noção de como preservar a prova.

Os Srs. Parlamentares têm sido vítimas cada vez mais constantes de clonagens, por exemplo, de aplicativos. A Câmara dos Deputados volta e meia tem ondas de clonagem. Vários Deputados Federais têm o celular clonado, assessores têm o celular clonado. Pessoas têm acesso a conteúdos que, às vezes, politicamente, são extremamente sensíveis. Mas não somente isso: criminosos usam essas condutas para extorquir, para chantagear, para fraudar, e acabam conseguindo recursos financeiros de pessoas de boa-fé que tenham um relacionamento. Com certeza, se a Deputada Cristiane mandar um WhatsApp para o Senador Cristovam, ele nunca vai questionar se aquela mensagem é de fato dela, jamais. Há uma confiança tão absurda na tecnologia que ninguém questiona. Qualquer mensagem que eu receba, eu tenho certeza absoluta de que eu estou tratando com a pessoa que está identificada naquele aplicativo. Eu não duvido, em nenhum momento. Isso propicia que criminosos consigam, cada vez mais, atuar em um ambiente digital. Então, na medida em que nós não temos essa dimensão do uso da tecnologia, nós dificultamos a própria prova.

Eu vou dar um exemplo muito clássico de uma conduta extremamente condenável: a vingança pornográfica. As vítimas de vingança pornográfica, de um modo geral, sofrem um constrangimento tão absurdo naquela situação que, muitas vezes, quando elas são contactadas por pessoas que estão ali para de alguma forma ameaçar, ou tentar extorqui-las, de alguma maneira, ou até mesmo tentando obter alguma vantagem até mesmo sexual - "olha, se você não fizer sexo comigo, eu vou vazar o conteúdo" -, chegam ao ponto de bloquear o perfil, por exemplo, se for em uma rede social o contato, ou apagar as mensagens. Às vezes o indivíduo criminoso manda o conteúdo como prova de que tem aquele conteúdo e ela apaga aquela mensagem.

Isso tudo dificulta sobremaneira o resultado de uma investigação policial, porque ainda que se tenha condições de contactar empresas, redes sociais, que tenham, em alguns casos, obrigações de armazenar determinados registros... Não são todos os conteúdos. As empresas têm obrigações, pelo Marco Civil, de armazenar registros de algumas movimentações de tecnologia, mas não conteúdo. Isso inviabiliza completamente a investigação e aumenta as estatísticas de impunidade, justamente porque nós, brasileiros, de um modo geral, não sabemos como preservar. Se nós formos vítimas de crimes comuns, crimes que são praticados contra bens jurídicos comuns - patrimônio, contra a honra mesmo, que seja -, nós temos uma dimensão muito clara: se alguém me atacar, me violentar ou me agredir fisicamente, eu vou até o IML, vou até uma delegacia de polícia, e busco fazer a prova daquela agressão com um exame específico sobre a minha condição. Se eu tenho um patrimônio furtado, eu tenho como demonstrar que aquele patrimônio me pertencia e não me pertence mais, e as circunstâncias demonstram que houve um furto. Mas com relação à tecnologia, nós não temos essa noção. Isso nos torna vítimas cada vez mais vulneráveis, Senador. Então, a educação digital tem o aspecto de prevenção.

Ela tem o aspecto também de desestímulo, na medida em que, quanto mais educados, mais civilizados somos, e tem o aspecto de compreensão da dinâmica do sistema como um todo. Se não tivermos essa condição, não temos como cobrar sequer resultados. Existem cada vez mais estatísticas policiais que não estão vinculadas diretamente à capacidade dos agentes da força policial, mas às dificuldades às vezes estruturais. Eu estou falando aqui não somente, como a Drª Cristhiane mencionou, da necessidade de qualificação dos servidores públicos, dos agentes, delegados e dos operadores do Direito, como também das estruturas de investigação, ferramentas tecnológicas capazes de investigar, capazes de fazer uma auditoria adequada, uma perícia adequada em um dispositivo informático, em um celular ou em um computador. Há delegacias, especialmente de cidades do interior, que não têm sequer profissionais que tenham a menor condição de compreender a tecnologia. Não conseguem entender como funciona, quiçá efetivar a investigação policial. Então, esses elementos trazem uma soma de fatores que tornam cada vez mais difícil o resultado do combate à criminalidade no ambiente tecnológico. Isso é muito ruim para o Brasil, na medida em que o nosso País é um país que tem, como eu falei, um dos maiores consumos de tecnologia do mundo, e é um país que representa uma potência econômica com grande e enorme potencial efetivo, com uma grande capacidade de se tornar líder em tecnologias, se assim dimensionar adequadamente os investimentos sobre esse aspecto.

Nós estamos aqui agora, como foi dito por alguns colegas, diante da necessidade de aprovar a Lei Geral de Proteção de Dados. A Câmara aprovou, no dia 29 de maio, e o Senado agora está com a fase de revisão desse projeto. É um instrumento legal extremamente importante. Nós temos que, no aspecto de educação, não somente pensar em conhecimento do cidadão, mas também em instrumentos do Estado. Muito do que se faz hoje... É até um ponto que eu queria comentar sobre a temática da audiência pública. Muitas violências que são cometidas através de tecnologia hoje não são sequer crime. O Renã comentou, e a Drª Cristhiane também, a dificuldade de classificação penal, de tipicidade penal. O que significa isso? Que você só pode ter uma conduta criminosa se houver previsão na lei de que aquilo é crime, com todos os elementos que existem. Como foi dito aqui, a Lei Caroline Dieckmann é uma lei de baixíssima utilidade, porque são tantos elementos para classificar o crime que você raramente consegue o enquadramento legal adequado para processar.

Então, você tem dificuldades em todos os aspectos. Como eu falei, vingança pornográfica não é crime.

A SRª CRISTIANE BRASIL (Bloco/PTB - RJ. *Fora do microfone*.) - *Stalking* não é crime, *cyberbullying* não é crime.

O SR. FABRICIO DA MOTA ALVES - *Stalking* não é crime, *cyberbullying* não é crime, *fake news* também, em grade dimensão, não é uma atividade criminosa. Essas são dificuldades, porque o Estado não corresponde a essa estruturação, que é não só de políticas públicas, mas também de instrumentos legais. E não somente prever o crime, mas dar condições processuais para solução do crime. Você pode ter o direito material muito bem previsto, muito bem dimensionado, mas se você não tiver um direito processual muito bem dimensionado, você não tem a satisfação do direito material, você não consegue satisfazer. Você não resolve. O cidadão ganha, mas não leva - é basicamente isso. Ele consegue ir até a delegacia, registrar a ocorrência. Às vezes o delegado faz o seu papel, manda para a Justiça, e nesse procedimento você tem uma inviabilização da solução de investigação e da persecução penal. Por que isso? Porque as nossas leis estão defasadas. As soluções são pontuais e ineficazes. Temos que, efetivamente, sentar. Volta e meia temos aqui discussões de novo Código Penal. O Senado agora está em um procedimento de deliberação de uma proposta de novo Código Penal; a Câmara está com o Código de Processo Penal; o Código Comercial também tem instrumentos de legalidade sob o aspecto da tecnologia. Mas nós precisamos também dimensionar um escopo maior, não somente ações setoriais, ações esparsas. Temos de ter uma dimensão maior.

O Código de Processo Civil foi aprovado pelo Congresso Nacional, já está em vigor, mas ainda temos dificuldades de implementação com relação ao aspecto digital. Ainda temos essa dificuldade. Estamos cada vez mais envolvidos com tecnologia e cada vez menos protegidos dela. Essa é que é a verdade. Não temos essa percepção porque não temos uma realidade tão brutal de violência digital. Porém, aqueles que enfrentam essa realidade sabem que a impunidade é a regra. Eles, infelizmente, experimentam a impunidade porque sabem que o Estado não consegue investigar. Às vezes, não tem sequer instrumentos legais.

Particularmente, eu tenho um escritório de advocacia, milito nessa área, especificamente, e é frustrante, Senador, você ver uma vítima de uma violência cometida através da internet e você ver uma sentença judicial de arquivamento daquele procedimento. Por que arquivamento? Porque não há crime. Não há crime porque não há lei. A pessoa sofreu a violência. Ela foi real, ela foi efetiva, às vezes tem os elementos de prova, mas não há previsão correspondente na lei. Então, você tem o arquivamento. Isso gera uma frustração, e uma confiança do Judiciário e nos poderes públicos cada vez menor. O cidadão não consegue... E isso pode se tornar ainda mais grave se o resultado dessa audiência pública for efetivo. Eu me atrevo até a dizer isso, Senador, porque o cidadão com mais conhecimento sobre educação digital tem condições de maior cobrança e controle social do Estado.

(Soa a campainha.)

O SR. FABRICIO DA MOTA ALVES - E, se o cidadão começar a investir em educação digital e o Estado não acompanhar com a instrumentalização legal de políticas públicas, o cidadão vai se frustrar. Ele vai ter conhecimento de uma série de direitos que não vão ser efetivados, porque o Estado não vai dar conta.

É muito próximo do que a gente experimenta com relação à violência doméstica. Os direitos estão todos aí, previstos. O Código Penal tem muitos instrumentos criminalizadores da violência doméstica, mas a vítima nunca conseguiu efetivamente uma resposta do Estado. Foi necessária a edição de uma nova lei, uma lei que trouxesse um valor social muito forte, que é a Lei Maria da Penha, para que o Estado pudesse dar uma resposta mínima para esses direitos que já existiam, mas que não eram efetivados.

É uma falência que, na verdade, se viraliza - até utilizando uma expressão bem típica de tecnologia -, porque ela começa com a vitimização e passa por um processo de revitimização, que não se encerra nunca, porque não há resultado efetivo. A vítima constantemente sofre a violência e é obrigada a viver e reviver aquilo constantemente, em todas as etapas, muitas delas despreparadas, na rede de atendimento público, para solucionar ou até mesmo para ouvir o seu relato sobre a violência que ela sofreu. E chega ao ponto de ir até o juiz e ele não poder dar uma resposta, porque a lei não o autoriza a dar essa resposta.

Então, possivelmente, sendo muito bem-sucedida essa audiência pública, como eu espero que seja, assim como seus planos e ideais de vida no sentido de colocar a educação como a primazia de todos os elementos que vão solucionar os problemas sociais, ou, em grande parte, diminuir os problemas sociais, teremos a necessidade de correspondência do Estado, porque um cidadão consciente, um cidadão educado e conhecedor dos seus direitos tem condições de cobrar. E, se o Estado não corresponde a esse conhecimento, a essa percepção de cidadania, o Estado começa a ser um propulsor da descrença e da instabilidade democrática.

Então, de uma forma geral, o que eu tinha a dizer - não vou extrapolar o tempo, sou o último a falar e sei que estão todos cansados -, o recado que gostaria de passar é basicamente este: educação digital, sim, mas com correspondência de políticas públicas e de instrumentalização. E aí a responsabilidade do Congresso Nacional e desta Casa é cada vez maior.

Parabenizo-o pela iniciativa e agradeço-lhe a oportunidade, Senador.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Eu agradeço a você e a todos os demais.

Pergunto se a Deputada quer fazer alguma consideração ou alguma pergunta, deixando, já de imediato, meus agradecimentos pela sua presença, prestigiando esta audiência.

A SRª CRISTIANE BRASIL (Bloco/PTB - RJ) - Boa tarde a todos os presentes.

Eu quero saudar todos na sua pessoa, Senador Presidente desta Comissão, e agradecer a oportunidade de tratar de um tema de tamanha importância, não só pelo fato em si da minha pessoa, de eu entender que sou bastante vítima desse tipo de crime, mas também pela importância da discussão desse tema neste ano eleitoral, desse processo eleitoral que se aproxima.

Gostaria de parabenizar a explanação dos presentes, sem mais, nem menos, porque todos foram bastante brilhantes e gostaria de fazer algumas perguntas. Eu não sei se as dirijo para uns ou outros, mas gostaria de que alguns se indicassem para responder essas perguntas, pois penso que são bastante importantes. Vou até explicar o porquê.

Eu vi, em algumas explanações, que alguns dos senhores colocam o Estado como uma das possibilidades de ser o grande provedor da educação digital, mas eu penso que, como hoje os provedores de aplicação se tornaram cada vez mais ferramentas com cunho claramente financeiro - o Facebook, o próprio Instagram agora, mais do que nunca, que reduziu o acesso aos próprios seguidores -, não seria o momento destes grandes nomes, como o Facebook, o Google, o Instagram, o Twitter, serem obrigados, até por lei - e eu digo que vou fazer um projeto de lei nesse sentido -, a disponibilizarem vídeos, *cards*, fotos, campanhas com uma parte do lucro que obtêm por essa comercialização, com esse caráter financeiro que têm, justamente incentivando essa educação digital? Eu acho fundamental. E gostaria de que alguns dos senhores pudessem responder a essa provocação.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Muito obrigado, Deputada.

A SRª CRISTIANE BRASIL (Bloco/PTB - RJ) - Olha, acho que... Posso fazer as três perguntas e aí vocês respondem?

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Pode, é melhor. E todos respondem.

A SRª CRISTIANE BRASIL (Bloco/PTB - RJ) - A pergunta número dois é sobre o marco civil. O marco civil, de certa forma, não ajuda os provedores de aplicação na inércia das remoções de certos direitos ao colocarem como condicionantes decisões judiciais, como, por exemplo, no direito de imagem? Porque, antes, bastava que você comunicasse ao Google, por exemplo, que você está tendo seu direito de imagem ferido que o Google tirava aquele conteúdo. Agora, você precisa entrar na Justiça para você ter, numa decisão judicial, garantido o seu direito de imagem; aí, sim, por uma obrigação judicial, o Google vai lá e tira, por um direito seu de ter sua imagem restabelecida.

Terceira pergunta - e eu já até sei a resposta do Paulo; portanto eu queria ouvir os outros, porque ele já falou na resposta dele: a única solução, para mim, viável para combater as *fake news* na internet seria um controle prévio de publicações. Se isso é possível em outros países - eu sei que é caro, custa dinheiro e mexer no bolso é complexo -, como na China, nos países árabes, por que não pode ser feito no Brasil, já que nós aqui não estamos sabendo lidar com a liberdade de expressão, já que ela fere constantemente a dignidade da pessoa humana? Essa é a minha terceira pergunta.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Obrigado, Deputada.

Eu vou passar a palavra a cada um dos três, que podem responder e já de despedir também da audiência.

A SRª CRISTIANE BRASIL (Bloco/PTB - RJ) - Ah, por último, mas não menos importante, quero falar para o Fabrício: Fabrício, eu estou redigindo aqui exatamente o Projeto de Lei nº 5.555, que é da *porn revenge*, a vingança pornô. Está aqui já prontinho para encaminhar para votação na Comissão de Constituição e Justiça.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Eu creio que três minutos são suficientes para responder e se despedir. E vou fazer nessa ordem.

O SR. PAULO RENÁ - Senador, eu posso pedir uma quebra da ordem, porque eu estou com meu filho recém-nascido vindo me buscar para a gente ir para uma consulta?

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Não tem problema.

Quer ser o primeiro, então?

O SR. PAULO RENÁ - Por favor.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Com o maior prazer.

O SR. PAULO RENÁ - E vou ter mesmo de me limitar aos três minutos; não posso passar disso.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Vamos passar para o Paulo.

O SR. PAULO RENÁ - Com relação - não vou me furtar a responder - a por que a gente não pode vigiar as comunicações como a China faz: porque a gente é uma democracia de verdade, ponto.

O marco civil coloca que o direito de imagem não fica a cargo de as empresas privadas protegerem porque eu não quero que o Facebook seja o fiel guardião dos meus direitos, assim como eu não quero a Sadia ou a Lenovo ou a Apple... Eu quero que o Estado seja o fiel guardião dos meus direitos, para isso há o Poder Judiciário. Se eu estou frustrado na minha expectativa, eu recorro ao Poder Judiciário. O Poder Judiciário é lento: liminar, antecipação de tutela, tutela de urgência...

Na proposta original do Marco Civil da Internet - é bom a gente recuperar um pouco da história para a gente saber como chegou até aqui -, a nossa proposta no Ministério da Justiça, eu participei da elaboração no Ministério da Justiça entre 2009 e 2010, era: eu publiquei; o Senador Cristovam não gostou; ele dizia para o Facebook: "Tire"; aí o Facebook tirava. Essa era a proposta. E falava: "Rená, o Cristovam está pedindo para tirar e eu tirei; resolvam-se entre vocês dois." Isso serve quando são pessoas de mesmo calibre. Quando o prefeito está brigando com o Kajuru, em Goiânia, ele não vai conseguir. Se o Presidente questionar um conteúdo de um pequeno veículo de comunicação, esse pequeno veículo de comunicação não vai conseguir fazer aquela informação ficar na rede. A gente tem assimetrias de poder. Então, o que vai acontecer é a eleição chapa branca: a gente vai ter todos os conteúdos removidos... Atira primeiro para perguntar depois. É o que vai acontecer. Seria bom atirar primeiro para perguntar depois? Como negro, eu tenho de dizer que a gente tem um monte de negros mortos por conta de suspeitas; uma polícia que trabalha com um perfil e atira primeiro para perguntar depois. A gente tem diversos casos recentes no Brasil de inocentes mortos. Um menino pergunta para um policial: "Por que você atirou em mim?" Não era melhor o policial ter perguntado antes?

Eu acho que a gente tem... Há umas bases, não é? Tortura: a gente sabe que a população admite tortura; um tapa na cara de quem roubou o celular a população admite. Mas a Constituição diz que não; os nossos compromissos internacionais

dizem que não; a nossa legislação diz que não. E a gente tem de reafirmar o que a gente quer. Eu quero um país que pratica tortura para sanar crime? Porque é uma via possível. A gente tem o 24 Horas, um seriado mundialmente famoso: o cara comete crime e salva o mundo. A gente pode querer esse mundo, mas ele não está expresso na nossa Constituição, na nossa legislação. Eu prefiro ser positivista nesse ponto e respeitar os direitos que estão valendo.

É isso.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Obrigado, Paulo, e fique à vontade de sair quando quiser para estar com seu filho.

O SR. PAULO RENÁ - Obrigado, Senador. A esposa já está reclamando, com razão.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Thiago.

O SR. THIAGO TAVARES NUNES DE OLIVEIRA - Muito obrigado, Senador Cristovam Buarque.

Antes de entrar nas perguntas específicas da Deputada, desde já eu agradeço e me coloco à sua disposição para a gente, com mais tempo, poder aprofundar um pouco este debate.

Eu não poderia deixar de mencionar, de fazer referências a duas intervenções que houve ao longo do debate que me parecem que têm resultados muito efetivos. Uma foi do próprio Paulo Renà quando chamou atenção para o art. 26 do Marco Civil da Internet e manifestou a preocupação de que esse artigo não estava sendo devidamente observado.

E eu não posso me afastar da minha condição também de Conselheiro do Comitê Gestor da Internet no Brasil. Nessa condição, eu tenho orgulho de dizer que o Comitê Gestor da Internet, a SaferNet, o Unicef e o Ministério Público Federal se uniram e juntaram esforços para realizar um ciclo de oficinas que percorreu as 27 capitais do País exatamente para contribuir com a implementação do art. 26 do Marco Civil. Nesse ciclo de oficinas, em três anos, foram realizadas 31 oficinas, que capacitaram diretamente 4.529 educadores, de 364 Municípios brasileiros, nas 27 unidades federativas e beneficiaram 1.061.964 alunos em mais de 700 atividades de multiplicação feitas nas escolas. É claro que são números ainda insignificantes quando comparados à dimensão continental do Brasil e também à população brasileira de 200 milhões de habitantes, e também ao número de mais de 100 mil escolas públicas e particulares que nós temos no País; mas é um começo. É uma contribuição...

(Soa a campainha.)

O SR. THIAGO TAVARES NUNES DE OLIVEIRA - ... que vem de uma articulação entre um organismo multissetorial, como é o caso do Comitê Gestor, a sociedade civil, como é o caso da SaferNet, um organismo internacional, como é a Unicef, e também um órgão público, que é o Ministério Público Federal.

Quero apenas destacar isso e também destacar um trecho da fala do Conselheiro Carlos Oliveira, quando ele mencionou o Safer Internet Day, que é uma campanha que começou por iniciativa da Comissão Europeia, na Europa, há 15 anos e cujas atividades aqui no Brasil nós temos o orgulho de coordenar por uma década. Foi realizada agora a décima edição, em fevereiro deste ano, e, nesses dez anos, ocorreram 725 eventos relacionados diretamente ao Dia Mundial da Internet Segura, o Safer Internet Day, em 218 Municípios brasileiros dos 27 Estados da Federação. Então, apenas em 2018, foram 85 eventos em 49 cidades de 19 Estados. São iniciativas que independem do Poder Público e que somam esforços, inclusive das empresas, para que aconteçam no País.

A pergunta que eu deixo também como contribuição para o debate é: será que nós não temos leis ou não temos políticas públicas?

Muitas vezes, estamos buscando apontar uma lacuna legislativa, mas, na verdade, nós já temos leis. Por exemplo: *fake news*, a delegada mencionou aqui, até leu o art. 323 do Código Eleitoral. A lei já existe, já está tipificada, inclusive, no Código Eleitoral.

Mesmo o *stalking* tem uma particularidade, eu concordo que merecia um olhar mais aprofundado, mas a Lei Maria da Penha, em determinadas situações, já faz referência expressamente à perseguição sistemática de mulheres, sobretudo, à violência doméstica e assim por diante. E o *cyberbullying*? O conteúdo do *cyberbullying* é o quê? É ameaça, é calúnia, é injúria, é difamação, e isso tudo está previsto em lei, no Código Penal de 1940. Agora, há uma peculiaridade aí: quem é o autor do *cyberbullying*? É um pré-adolescente, é um adolescente. E quem é a vítima? Também, tem a mesma idade. Então, não pode ser crime, porque o ECA não permite; o ECA não permite que menores de 18 anos sejam imputados criminalmente. A não ser que tenhamos que revogar o ECA, com o que eu absolutamente não concordo, e espero que esse dia não chegue, porque a redução da maioridade penal definitivamente não é, do ponto de vista da SaferNet, a solução para os problemas de violência no Brasil.

Então, a pergunta que deixo para nossa reflexão é: nós não temos leis ou não temos políticas públicas? Eu acho que lei já temos demais. O que falta é colocá-las em prática, é cumpri-las, é estruturar as polícias para que possam fazer uma investigação célere, para que tenham condição efetiva de investigar os crimes, que não vivam sobrecarregadas de trabalho, com poucos delegados, com poucos agentes, com falta de equipamento, com falta de treinamento etc.

E, para encerrar, apenas também como contribuição, eu destaco que nós temos de ter muito cuidado quando começamos a mexer em pilares fundamentais que estruturam a própria democracia, como, por exemplo, a liberdade de expressão.

A internet chegou aonde chegou e é o que ela é, porque não há controle prévio de conteúdo. Nem na China! A China monitora o que a população faz, como a internet é utilizada, mas ela não...

(Soa a campainha.)

O SR. THIAGO TAVARES NUNES DE OLIVEIRA - ... aprova ou desaprova um *post* antes de ele ser postado numa rede social. Não existe, o departamento chinês não diz o que pode ou o que não pode ser publicado. A internet não é como um jornal ou uma revista em que há um editor lendo as matérias e aprovando: "Isso publica, isso não publica; essa pauta cai, e essa segue." Não é assim. Na internet, você tem liberdade de postar o que você quiser e responder pelos seus atos em caso de cometimento de ilícito, mas essa responsabilização é sempre *a posteriori*, e não *a priori*. O controle de conteúdo, *a priori*, faz com que nós estejamos voltando para um Estado que não é democrático, é um Estado de exceção, onde haverá um departamento de ordem política e social que irá monitorar o que é dito por cada um...

(Soa a campainha.)

O SR. THIAGO TAVARES NUNES DE OLIVEIRA - ... dos cidadãos na rede e poderá dizer que isso aqui pode ser dito e isso aqui não pode ser dito.

Nós temos uma democracia recente, cambaleante, mas sabemos o que é viver uma ditadura. Eu não sei, porque nasci em 1979, estava em plena infância, portanto, com tenra idade, mas aprendi com os meus pais e aprendi, sobretudo, nos livros de história o que significa viver numa ditadura.

Eu permaneço à disposição para a gente poder aprofundar esse debate. Acho que são perguntas extremamente complexas que têm várias implicações, mas eu gostaria de poder ter oportunidade de aprofundar essa discussão com muito mais tempo.

Obrigado.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Muito obrigado, Thiago.

Passo a palavra ao Dr. Emilio.

O SR. EMILIO SIMONI - Eu acredito que a gente vai justamente em caminho oposto com relação ao bloqueio; a gente tem de investir na divulgação, na conscientização para que as pessoas incitem uma consciência, porque, com a magnitude que a internet vive hoje, não é possível mais controlar. E justamente a proposta da internet é essa falta de controle. E a gente acredita realmente que as pessoas, através da educação, da conscientização, têm a capacidade de discernir o que é verdadeiro, o que é verídico, o que é falso e prejudicial, e aí, sim, ela tomar essa decisão.

Com relação específica aos bloqueios, eles têm um impacto muito pequeno, apenas inicial. As pessoas são adaptativas, então elas vão rapidamente se adaptar àquele ambiente e àquele cenário, vão passar por aquele bloqueio e continuar fazendo aquela divulgação. E falando isso de forma muito focada na parte técnica da questão, que é o meu forte aqui hoje.

Obrigado.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Obrigado.

Fabricio.

O SR. FABRICIO DA MOTA ALVES - Obrigado, Senador.

Com relação a um questionamento que a Deputada colocou do Marco Civil da Internet.

Eu tenho uma percepção bastante aproximada com o que a senhora apresenta na medida em que eu entendo que houve uma resposta, e foi a melhor ou a menos pior possível, que foi judicializar. Só que isso tem consequências que talvez sejam consequências não desejadas para a sociedade brasileira. Uma delas, como a senhora bem pontuou, é a dificultação que existe na solução de problemas, porque nem todas as vítimas de violências praticadas na internet têm acesso ao Judiciário facilmente. Claro que você sempre vai ter a opção de ir ao juizado especial cível; você sempre vai ter a opção de contratar um advogado, mas nós entramos numa discussão sobre acesso efetivo ao Judiciário. O direito é garantido

na Constituição, porém a efetivação desse direito nem sempre é fácil. Contratar um advogado não é barato, sobretudo num caso tão específico como este, que envolve questões tecnológicas de direito digital. Às vezes, é necessário contratar um bom profissional, capacitado para isso. Até o Renato comentou aqui que há muitos advogados que não têm essa qualificação ainda, e é uma luta nossa na OAB para permitir essa qualificação. Até mesmo no PJE, que é o Processo Judicial Eletrônico, temos dificuldades de advogados manipulando um sistema que deveria ser básico, como um garfo e uma faca, para qualquer um. E esse é um problema estruturante. Mas foi a resposta que a sociedade encontrou. Se foi a mais adequada ou não, Deputada, a senhora está colocando num sentido, talvez num viés um pouco crítico, porque as consequências são ruins para muitas pessoas. E eu até acrescento algumas mais consequências a isso - e também discordando um pouco do que meu amigo Thiago colocou: eu acho que há necessidade, sim, de atualização legislativa em vários pontos.

Eu vou apenas mencionar um ponto específico, que é o processual. Se uma pessoa sofre uma violência praticada na internet, ela pode até ir a uma delegacia. Mas, em muitas situações, a competência para investigar ou até mesmo para processar aquele fato nem é sequer da delegacia onde está situada...

(Soa a campainha.)

O SR. FABRICIO DA MOTA ALVES - ... essa pessoa, onde ela reside. É possível que, pelas regras processuais, a competência seja uma outra localidade, o que torna também elementos de dificuldade de acesso ao Judiciário. Você chega até um delegado, ele pode até receber aquela ocorrência, mas ele constata que... "Não, a competência não é daqui, você vai ter que entrar lá no Município, no Estado tal, lá no Norte, no Amazonas, em Manaus, para processar esse crime, para investigar esse crime, porque eu não tenho competência. A lei não me autoriza."

O Judiciário não encontra solução para isso, o STJ patina fortemente com relação a isso, o tempo todo muda a sua jurisprudência. A mais recente agora estabelece a competência para alguns crimes como sendo aquela do local onde estão situados os dados no servidor do provedor de aplicação. Mas isso é tão já defasado, porque nós estamos pensando em *sites* em que há um armazenamento efetivo. Mas, e no WhatsApp, por exemplo, alguém sabe onde estão os servidores que efetivamente armazenam os dados que trafegam por ele, se é que seja esse o caso específico?

Então, são dificuldades que talvez mereçam uma reflexão no momento oportuno. Por enquanto, a resposta que se encontrou foi a de dimensionar o marco civil para a judicialização necessária dos problemas.

A SRª CRISTIANE BRASIL (Bloco/PTB - RJ) - Dr. Thiago, o senhor me permite só uma pergunta? O senhor é advogado ou não?

O SR. THIAGO TAVARES NUNES DE OLIVEIRA - Eu sou professor de Direito.

A SRª CRISTIANE BRASIL (Bloco/PTB - RJ) - Ah, porque o senhor repete uma *fake news:* que a gente não tem de fazer atualização legislativa na Câmara.

Pelo que entendi, na opinião do senhor, a Câmara legisla demais, mas, muitas vezes, a gente tem de fazer uma atualização legislativa porque aqui muitas leis são malfeitas, muitas leis precisam de atualização, e, às vezes, essa atualização leva muito tempo para acontecer. E aí a gente justamente trabalha com uma legislação que não atende a realidade da população brasileira. E é por isso que muitas vezes a gente fica aqui com essa alta produção de projetos de lei, de projetos de lei... E eu peço até ao senhor que não permita que se propague isto, como "Ah, tem projeto de mais! Tem projeto de mais!". Por aqui passa todo tipo de legislação de todo tipo de tema que o senhor nem imagina. Eu, não aceitando ser membro de comissão nenhuma quase, estou em 19. Sem querer. Então, o senhor não imagina quantas acontecem ao mesmo tempo! É mentira?

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Não, é verdade.

A SRª CRISTIANE BRASIL (Bloco/PTB - RJ) - Sem querer, estou em 19. A gente aqui é super-herói de estar em várias comissões que acontecem ao mesmo tempo. Por estar aqui, estou faltando a pelo menos sete. Então, é muito complicado o nosso dia a dia. Inclusive convido os senhores a participar dele para entender como é que se faz a produção legislativa, que não é mole.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Obrigado, Deputada.

Passo a palavra ao Dr. Carlos Oliveira.

O SR. CARLOS OLIVEIRA - Muito obrigado!

A minha postura neste diálogo, neste debate é sobretudo de partilhar experiências entre o que é a perspectiva da União Europeia e a experiência dos 28 Estados-membros, e também apreender o que são os problemas com que o Brasil está a

confrontar e as soluções que estão a ser desenvolvidas. Por isso, permitam-me enfocar um pouco o modelo de reservas sobre aquilo que é a adequação do quadro legislativo no Brasil.

Todavia, aproveitava para partilhar algumas ideias sobre precisamente a experiência europeia. Vou tomar, a título de exemplo, a legislação que entrou recentemente em vigor sobre proteção de dados. Isso resulta, digamos, numa experiência que tem um pouco mais de 20 anos e que demonstrou as virtudes, mas também as limitações da judicialização de muitos aspectos, até porque o edifício judicial tem, digamos, trâmites próprios que são específicos e que têm toda a sua razão de ser porque lançaram um grau de ponderação para ter em consideração todos os interesses que estão em jogo. Em alguns aspectos, também há algumas limitações quando estamos a falar de utilizadores individuais que são confrontados com situações como as que foram mencionadas. Uma pessoa faz uma corporação como o Google, Facebook, e isso não envolve nenhum apontar de dedos em relação a essas empresas, é apenas um exemplo, que esteja apresentando problemas como o direito ao esquecimento, como, por exemplo, o direito à imagem. No caso, até que foi levado ao desenvolvimento e tinha alguma relação. Os meios e recursos que lançaram...

(Soa a campainha.)

O SR. CARLOS OLIVEIRA - ... a mobilizar para entrar numa disputa judicial são, de fato, fenomenais para se fazer essas organizações.

Por isso, por exemplo, no âmbito da legislação sobre a proteção de dados, foi instituída a criação de uma autoridade de proteção de dados, precisamente com o propósito de agir como entidade mediadora e obter uma resposta mais ágil, mais eficaz para problemas que, quando são confrontados por utilizadores individuais que não têm os recursos e a capacidade, muitas vezes, de envolver tudo aquilo que é necessário para chegar à via judicial.

A nossa perspectiva, mesmo com base num longo histórico de mediação, é que isso funciona e permite, digamos, uma razoável eficácia. É necessário salvaguardar aspectos fundamentais como a independência das entidades reguladores, neste caso, da autoridade de proteção de dados, porque sabemos que a nossa história nos ensina coisas que convém não esquecer. O poder político é muito volúvel e convém preservar precisamente o risco de instrumentalização dessas entidades com o poder político, que, às vezes, nos é desfavorável e, outras vezes, nos é muito desfavorável. Isso é muito importante.

Sobre a questão das *fake news*, precisamente a nossa história é muito pesada sobre essas matérias e há, digamos, uma linha muito tênue, às vezes, entre a autorização prévia... A título de exemplo, durante muitos anos, essa entidade que fazia a censura em Portugal chamava-se exame prévio. Portanto, uma vez mais, são áreas muito... Do nosso ponto de vista, é muito mais importante capacitar a sociedade civil, os atores, jornalistas, grupos de cidadãos para de fato ter uma ação indireta sobre essas matérias e evitar isso. Eu sei que essa não é uma resposta universal, mas tem muito que sei do Ministério da Verdade.

Só para terminar, uma frase sobre a questão do desenvolvimento das empresas. No âmbito das iniciativas que a União Europeia tem vindo levar a cabo nessa área, há de fato sempre um convite que tem sido respondido de forma favorável a que as empresas, sobretudo as grandes multinacionais, tenham um papel e sejam corresponsáveis no lançamento destas iniciativas: a coligação para competências digitais para o emprego; o código de conduta, por exemplo, sobre *fake news*, que vai ser publicitado durante o próximo mês de julho, é algo, digamos, que prevê precisamente a mobilização dessas entidades no sentido de limitar a propagação indiscriminada de notícias que são ostensivamente falsas, ofensivas, difamatórias, e associado a isso também um esforço de identificação das fontes, porque o anonimato tem coisas, digamos, como há pouco mencionava, que são muito desagradáveis e que não correspondem a uma conduta socialmente aceitável em uma sociedade em que somos todos cidadãos com iguais direitos.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Obrigado, Dr. Carlos.

Passo a palavra à Delegada Christiane.

A SRª CRISTHIANE ANDRADE FRANÇA - Deputada, eu vejo que você foi alvo de algumas *fake news* e foi vítima de diversos crimes dessa natureza. Crimes, porque, em um período eleitoral, até as *fake news* são crime do 323, mas fora isso elas podem ser uma difamação, uma injúria. Eu acredito que, quando se fala em controle de qualquer tipo de produção de conhecimento no Brasil, que viveu um período ditatorial tão longo, as pessoas ficam muito amedrontadas com isso. Elas ficam com muito medo. Realmente, é complicado você fazer esse controle e criar um limite para até onde vai ser controlado isso. Então, vejo que essa não seria mesmo...

(Intervenção fora do microfone.)

A SRª CRISTHIANE ANDRADE FRANÇA - Ao mesmo tempo em que é difícil fazer esse controle, nós devemos então investir da educação digital em si, e mostrar às pessoas que elas têm de se conscientizar com o conteúdo que elas veem na internet.

Quando você questionou a respeito dessa dificuldade de retirar um conteúdo da internet nos provedores de aplicação - Facebook, Instagram, seja qualquer um deles -, eu acredito que essa opção de judicializar deve ter sido porque nós temos dois direitos fundamentais ali: o direito de imagem e o direito à liberdade de expressão. Então, você tem de passar para um juiz analisar e sopesar o que ele vai aplicar naquela situação. Realmente, é complicado. Muitas vezes, eu lido com diversas situações no dia a dia, de a pessoa chegar à delegacia e pedir que nós tiremos aquele conteúdo do ar. A gente não tem essa possibilidade de tirar aquele conteúdo que foi postado do ar. Aí a gente aconselha que ela procure um advogado. O que a gente pode fazer é registrar ocorrência e descobrir quem é o autor daquilo, porque muitas vezes as pessoas se utilizam do anonimato para isso. A gente aconselha que procure um advogado ou a Defensoria Pública, ou vá até um Juizado Especial, mas infelizmente a gente não consegue retirar isso, porque nós temos dois bens jurídicos protegidos ali, e a gente acaba passando para a mão de um juiz analisar isso.

Eu quero, mais uma vez, agradecer por estar aqui presente hoje e agradecer o convite do Senador Cristovam.

O SR. PRESIDENTE (Cristovam Buarque. Bloco Parlamentar Democracia e Cidadania/PPS - DF) - Eu quero agradecer a cada um de vocês, muito especialmente à Deputada pela honra que nos dá de estar aqui, e dizer que um evento como esse só passa uma certeza: a de que estamos cheios de dúvidas.

Nós não temos o mapa de como enfrentar os próximos anos, talvez, décadas, de como manter uma democracia que não censure e que não deixe que as notícias saiam sem compromisso com a verdade. Não sabemos como fazer isso. Não sabemos de onde saem as notícias, não sabemos nem como identificar com clareza quais são os autores. Eu creio que caminhamos, talvez, para algo mais além das *fake news*: *fakes realities*. Até as realidades vão ser falsificadas.

Assistindo ao encontro do Presidente dos Estados Unidos com o Presidente da Coreia do Norte, eu me perguntei se aquilo não era uma falsa realidade, se aquilo, de fato, estava acontecendo ou não, ou se aconteceu fisicamente, mas nada do que eles dizem que vão conseguir vão conseguir; se não foi para que assistíssemos.

O mundo, Dr. Carlos, está virando um grande teatro e é difícil quem não queira ser artista, quem quer ser, de fato, político, quem quer ser um agente das transformações no mundo real, mas, de qualquer maneira, demos uma boa contribuição hoje e eu agradeço muito pelo que vocês nos passaram. Vamos transcrever isso, vamos transformar essas falas, inclusive a da Deputada, numa brochura e vai ficar passando na televisão, como vocês sabem, algumas vezes, ao longo dos próximos dias.

Eu, antes de encerrar, convoco para o dia 19 de junho, terça-feira, em caráter excepcional, às 11h30min, reunião, extraordinária, desta Comissão, destinada à deliberação de proposições e à apreciação das emendas deste colegiado ao PLN 2, de 2018.

Nada mais havendo a tratar, com meus agradecimentos a todos, declaro encerrada esta reunião.

(Iniciada às 10 horas e 48 minutos, a reunião é encerrada às 13 horas e 52 minutos.)