DEPARTAMENTO DE TAQUIGRAFIA, REVISÃO E REDAÇÃO

NÚCLEO DE REDAÇÃO FINAL EM COMISSÕES

TEXTO COM REDAÇÃO FINAL

Versão para registro histórico

Não passível de alteração

CPI - CRIMES CIBERNÉTICOS			
EVENTO: Reunião Ordinária/Audiência Pública	REUNIÃO Nº: 1799/15	DATA: 22/09/2015	
LOCAL: Plenário 14 das Comissões	INÍCIO: 15h02min	TÉRMINO: 17h10min	PÁGINAS: 49

DEPOENTE/CONVIDADO - QUALIFICAÇÃO
PATRÍCIA PECK PINHEIRO - Advogada especialista em Direito Digital. CRISTIANA OLIVEIRA GONZALEZ - Representante do Instituto Brasileiro de Defesa do Consumidor — IDEC.

SUMÁRIO
Apreciação de itens constantes da pauta. Exposições sobre crimes digitais.

OBSERVAÇÕES
Houve exibição de imagens.

O SR. PRESIDENTE (Deputado Leo de Brito) - Boa tarde.

Declaro aberta a 14ª Reunião Deliberativa Ordinária de audiência pública da CPI dos Crimes Cibernéticos.

Encontra-se à disposição dos senhores membros cópia da ata da 13ª Reunião, realizada no dia 15 de setembro de 2015.

Pergunto se há necessidade de leitura da ata.

O SR. DEPUTADO RODRIGO MARTINS - Sr. Presidente, solicito a dispensa da leitura da ata.

O SR. PRESIDENTE (Deputado Leo de Brito) - Fica dispensada a leitura da ata a pedido do Deputado Rodrigo Martins.

Em discussão a ata. *(Pausa.)*

Não havendo quem queira discuti-la, em votação.

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

Aprovada.

Comunico o recebimento das seguintes correspondências:

Documentos em que o Facebook Serviços Online do Brasil, o Twitter Brasil Rede de Informação e o Google Brasil encaminham respostas às indagações dos senhores membros, na reunião ordinária do dia 27 de agosto de 2015. Esses documentos serão encaminhados aos gabinetes dos membros da CPI;

A Secretaria da CPI também recebeu ofício do Diretor-Geral da Polícia Federal, Delegado Leandro Daiello Coimbra, que informa que a Polícia Federal possui informações consolidadas de fraudes bancárias apenas em relação à Caixa Econômica Federal;

Ofício do Sr. Deputado Jean Wyllys informando missão oficial na cidade de Washington, Estados Unidos, entre os dias 20 e 25 de setembro;

Ofício do Sr. Deputado Odorico Monteiro informando missão oficial na cidade de Washington, Estados Unidos, entre os dias 15 e 17 de setembro.

Ordem do Dia.

Apreciação dos requerimentos, conforme o roteiro.

O SR. DEPUTADO RODRIGO MARTINS - Sr. Presidente, só uma sugestão para economicidade do nosso tempo. Se for de comum acordo, proponho fazermos

a votação dos requerimentos em bloco para adiantar a audiência pública. As duas representantes já estão presentes.

O SR. PRESIDENTE (Deputado Leo de Brito) - O.k. Vamos fazer a votação em bloco.

Com a palavra a Deputada Alice Portugal.

A SRA. DEPUTADA ALICE PORTUGAL - Sr. Presidente, concordo que a votação seja em bloco, contudo, tenho uma sugestão em relação ao item 3 da pauta: Requerimento nº 73, de 2015.

Primeiro, quero fazer uma correção relativa ao cargo do convidado, Sr. Edinho Silva. Na verdade, ele é Chefe da Secretaria de Comunicação Social, mas consta no requerimento que ele é Ministro da Comunicação. Que realmente seja estipulada a natureza de convidado para a sua presença.

Quero também sugerir que seja acrescido na lista dos convidados um representante do Instituto Alana, ONG que trata da promoção da infância. O.k.?

O SR. PRESIDENTE (Deputado Leo de Brito) - Certo. Todos estão de acordo com as modificações propostas pela Deputada Alice Portugal? *(Pausa.)*

Então, passemos à votação em bloco dos três requerimentos.

Vou apenas ler aqui o conteúdo dos três requerimentos com as modificações propostas.

O SR. DEPUTADO RODRIGO MARTINS - Sr. Presidente, queria solicitar à Deputada Alice Portugal que esclareça que ONG é essa para que fique registrado.

O SR. PRESIDENTE (Deputado Leo de Brito) - Pois não.

Com a palavra a Deputada Alice Portugal.

A SRA. DEPUTADA ALICE PORTUGAL - Trata-se de uma ONG que cuida da promoção da infância, da valorização da atividade infantil, como brincadeiras, e também dos cuidados relacionados com a divulgação do perfil infantil nas redes sociais.

Essa sugestão foi dada por pessoas que tratam da questão da infância, que manifestam preocupação com o objeto do crime de pedofilia que se dá na Internet. Essa ONG tem bastante experiência nesse assunto.

O SR. DEPUTADO RODRIGO MARTINS - Deputada, essa modificação seria feita no Requerimento nº 73?

A SRA. DEPUTADA ALICE PORTUGAL - Requerimento nº 73. É a minha sugestão.

O SR. DEPUTADO RODRIGO MARTINS - No caso, solicita que sejam tomadas as providências necessárias para convidar os expositores elencados, a fim de prestarem esclarecimentos sobre publicidade e comércio virtual na Internet.

A SRA. DEPUTADA ALICE PORTUGAL - É isso. Ela trata de maneira intensa dessa questão da infância na Internet.

O SR. DEPUTADO RODRIGO MARTINS - No sentido de publicidade? Aqui tem mais a ver com publicidade. Eu tenho o temor de que essa questão não se configure dentro do tema do requerimento.

A SRA. DEPUTADA ALICE PORTUGAL - Ela trata com grande interesse o problema da publicidade infantil, do uso de crianças em publicidade e da publicidade infantil como um todo.

O SR. PRESIDENTE (Deputado Leo de Brito) - O.k., Deputado?

O SR. DEPUTADO RODRIGO MARTINS - Tranquilo.

A SRA. DEPUTADA ALICE PORTUGAL - Nós vamos trabalhar aqui agências de publicidade, agência brasileira de anunciantes, o Chefe da Secretaria de Comunicação Social, a autorregulamentação publicitária, e uma ONG que trata de promoção da infância e publicidade infantil. Eu acredito que isso é interessante. Essa é uma discussão séria.

O SR. DEPUTADO RODRIGO MARTINS - O Deputado Sandro Alex, autor do requerimento, está chegando. Acho que S.Exa. pode até discutir sobre o tema.

O SR. PRESIDENTE (Deputado Leo de Brito) - Sim, Deputado.

A SRA. DEPUTADA ALICE PORTUGAL - Então, não é o caso de fazer aprovação em bloco. Sugiro fazermos de um em um, porque dá tempo até de conversarmos.

O SR. DEPUTADO RODRIGO MARTINS - Retira-se o bloco.

A SRA. DEPUTADA ALICE PORTUGAL - Vai de um em um.

O SR. PRESIDENTE (Deputado Leo de Brito) - Deputado Sandro Alex, nós fizemos um acordo de votar em bloco os três requerimentos, e a Deputada Alice está apenas sugerindo a inclusão da representante do Instituto Alana, ONG que

trata das questões de criança e adolescentes relacionadas à publicidade infantil, na audiência pública proposta por V.Exa.

Eu gostaria de saber se V.Exa. está de acordo, porque aí nós poderíamos votar...

O SR. DEPUTADO SANDRO ALEX - Sr. Presidente, a inclusão é do nome do Alana, como publicidade. Vejam que estamos falando aqui sobre crimes cibernéticos. Publicidade, o Governo... Eu trabalho com o Alana dentro da Comissão de Ciência e Tecnologia, Comunicação e Informática. Aliás, fui Relator do projeto de publicidade infantil em conjunto com o Alana, do qual foi aprovado um substitutivo, um voto em separado de minha autoria, que hoje tramita na CCJ. Conheço bem o assunto, mas não cabe, nessa discussão sobre crimes na Internet, esse assunto do Alana. São coisas muito distintas as que nós vamos tratar aqui. Podemos até fazer outra audiência para falar, se for o caso, dentro da pedofilia ou algo assim. Enfim, este tema não tem relação com o Alana, e eu respeito profundamente.

Aliás, fui autor de convites feitos ao Alana para a discussão de publicidade infantil tanto na CCJ quanto na Comissão de Ciência e Tecnologia, Comunicação e Informática, e acho que não cabe trazer o Alana à CPI, pelo menos não há nenhum envolvimento direto, não há relação direta.

O SR. PRESIDENTE (Deputado Leo de Brito) - Deputada Alice.

A SRA. DEPUTADA ALICE PORTUGAL - Foi solicitada a mim a inclusão do nome da ONG, do Instituto Alana, exatamente para fazer essa transversalidade com a propaganda infantil e a pedofilia, ou seja, fazer um *link* com o aspecto dos crimes na Internet.

Evidentemente, o autor do requerimento tem a primazia sobre essas indicações. Se S.Exa. acha que fica desconexo com o objetivo original, não há problema. Nós podemos até formatar, juntos, uma solicitação de vinda. Eu acho que seria interessante. Eu, que não tenho essa vivência em relação a essa questão de publicidade infantil, quero saber o que o Alana diz sobre o cruzamento entre publicidade e pedofilia. A ideia foi essa, a ideia da assessoria foi essa, mas nós podemos fazer uma coisa exclusiva. Eu não sei se temos tempo, Deputado Sandro.

O SR. DEPUTADO SANDRO ALEX - Eu acho que nós poderíamos deixar, dentro das outras Sub-Relatorias, para uma audiência pública relacionada ao tema

específico que a nobre Parlamentar coloca. Neste tema que vamos apresentar aqui são...

A SRA. DEPUTADA ALICE PORTUGAL - Publicitários, não é?

O SR. DEPUTADO SANDRO ALEX - ...os publicitários, as agências, o Governo e o envolvimento direto com essa nova tecnologia, ou seja, a Internet e a publicidade no Brasil.

Então, não há relacionamento direto, mas considero relevante. Isso pode ser feito, em outra audiência pública, com o tema específico.

O SR. PRESIDENTE (Deputado Leo de Brito) - Há acordo, Deputada Alice?

A SRA. DEPUTADA ALICE PORTUGAL - Eu acho que o ideal seria, realmente, nós já adiantarmos a oitiva de interlocutores que têm inserção na temática, e o Alana trabalha de maneira intensa.

Eu fiz uma varredura nas redes sobre o trabalho dele. É um trabalho intenso, interessante, criativo. E é um trabalho focado em publicidade.

O SR. DEPUTADO SANDRO ALEX - Eu até vou apresentar, no dia dessa audiência pública, informações relevantes. Pergunto se não seria possível incluirmos no mesmo requerimento do Deputado Leo, que vai trazer aqui a fundadora do Projeto Infância Livre.

A SRA. DEPUTADA ALICE PORTUGAL - Se for colocar o Infância Livre, inclua o Alana.

O SR. DEPUTADO SANDRO ALEX - Então, esse requerimento do Deputado Leo de Brito, o Requerimento nº 2, já vai convidar a Sra. Joanna Maranhão. É um tema mais... Eu não sei se o Deputado permitiria, mas enfim.

A SRA. DEPUTADA ALICE PORTUGAL - Ah, sim, o Requerimento nº 2. Pronto!

O SR. PRESIDENTE (Deputado Leo de Brito) - Da minha parte não há problema.

A SRA. DEPUTADA ALICE PORTUGAL - Eu acho interessante. Talvez conecte melhor o foco. Iria então para o Requerimento nº 2, porque o interesse é trazer o Alana a esta CPI.

O SR. DEPUTADO SANDRO ALEX - Poderíamos fazer esse acordo, então.

A SRA. DEPUTADA ALICE PORTUGAL - Para mim, tudo bem.

O SR. DEPUTADO SANDRO ALEX - Isso se V.Exa., que é o autor do requerimento que convida o Projeto Infância Livre, concordar.

A SRA. DEPUTADA ALICE PORTUGAL - Para mim, tudo bem.

O SR. PRESIDENTE (Deputado Leo de Brito) - Se há acordo, da minha parte também não há nenhum problema.

A SRA. DEPUTADA ALICE PORTUGAL - Pronto, pronto! Aí ouvimos o Alana e vemos essa experiência. Acho importante. Para mim, tudo bem. E a correção do Ministro Edinho como convidado.

O SR. PRESIDENTE (Deputado Leo de Brito) - Sim, será feita.

A SRA. DEPUTADA ALICE PORTUGAL - E do Chefe da Secretaria de Comunicação Social.

O SR. PRESIDENTE (Deputado Leo de Brito) - Será feita a correção.

Então, nós vamos votar em bloco com as modificações já propostas pela Deputada Alice no tocante a essa modificação, inclusive à ida do item 3, Requerimento nº 73, para o item 2 da pauta, Requerimento nº 69.

Então, vou ler as ementas para fazermos essa votação em bloco.

Item nº 1. Requerimento nº 65, de 2015, do Sr. Delegado Éder Mauro, que "*solicita realização de audiência pública para debate sobre a ausência ou ineficiência de cobertura de telefonia em Municípios do Estado do Pará e criptografia de WhatsApp com os convidados Bayard Gontijo, Presidente da Oi; Rodrigo Abreu, Presidente da TIM; Carlos Zenteno, Presidente da Claro; Amos Genish, Presidente da Vivo, e João Batista de Rezende, Presidente da ANATEL"*.

O SR. DEPUTADO SANDRO ALEX - Pela ordem, Sr. Presidente.

V.Exa. leu o Requerimento nº 1. Nós estamos em votação em bloco, não é isso?

O SR. PRESIDENTE (Deputado Leo de Brito) - Sim. Estou só lendo as pautas para votarmos em bloco.

O SR. DEPUTADO SANDRO ALEX - A minha preocupação é porque eu sou contrário a esse requerimento, que tem também um objetivo importante, mas em outra Comissão.

Nós estamos aqui solicitando uma audiência pública na CPI de Crimes Cibernéticos para falar de ineficiência de cobertura de telefonia, pontualmente, num Estado, inclusive, importante, chamando Presidentes.

Já falamos da criptografia no WhatsApp com representantes das empresas, foi o SINDITELEBRASIL que nos trouxe as informações, juntamente, com as autoridades que tratavam do tema. Mas falar de cobertura de telefonia e ineficiência? Inclusive, subscrevo, apoio essa matéria na Comissão de Ciência e Tecnologia, Comunicação e Informática, que trata desse tema. A nossa CPI trazer uma audiência pública de cobertura de sinal?

O SR. PRESIDENTE (Deputado Leo de Brito) - Bem, diante da divergência, eu vou encaminhar. Como são três requerimentos, podemos votá-los individualmente. Inicia-se pela discussão deste. V.Exa. já pode fazer a defesa, já pode iniciar a defesa, e aí quem quiser faz a contradita.

Passo a palavra ao Deputado Éder Mauro. Depois passaremos à votação.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Sr. Presidente, colegas Deputados, na verdade, esse é apenas um dos tópicos que com certeza acabou sendo acrescido no momento da confecção, porque foi debatido numa reunião anterior, mas o que o requerimento solicita — inclusive, quero aqui pedir a retificação em parte do requerimento em relação às pessoas citadas — é que não seja na pessoa dos Presidentes, porque sabemos que é muito difícil eles virem. Que sejam representantes dessas operadoras, em primeiro lugar.

Em segundo, o requerimento diz respeito, sim, ao assunto que é tratado na CPI, crimes cibernéticos, que vai desde o estelionato e chega ao pior deles, que é a questão da pedofilia, principalmente, no tópico em que se diz sobre o fato-crime e o início da apuração.

Há operadoras que têm, quando a autoridade policial requer por ofício que se forneça dados cadastrais das pessoas que utilizam determinado *chip,* a cultura, muita vezes, por não informação ou pelo setor jurídico não colocar dessa forma, de não informar achando que tem que ser por ordem judicial, quando não é. A legislação permite, autoriza e determina que forneçam, sim, esses dados para a autoridade policial. Isso vai fazer com que muitos crimes não só sejam solucionados, como também sejam, inclusive, evitados.

Então, nós queremos a presença dessas operadoras aqui, inclusive do representante da ANATEL, para que possamos, através de documentação e de resolução, fazer com que as operadoras cumpram, para questões dos crimes cibernéticos, o que as autoridades policiais solicitam, o que a legislação permite que não é hoje cumprido.

As ordens judiciais são para determinadas outras coisas, não a questão de dados cadastrais, bloqueio de *e-mail...* Então, são por essas questões que nós estamos querendo que as representantes venham aqui para tratar junto com a ANATEL e conosco, Deputados.

A questão da abrangência, eu mencionei no final do meu pronunciamento na reunião anterior, do Estado do Pará. Eu tenho certeza de que não é só o Estado do Pará, mas são vários Municípios do interior dos Estados. Eu questionei que pode não ter uma ligação direta, mas eu tenho certeza de que indiretamente contribui muito de forma negativa para a segurança pública e vai não só na questão dos outros crimes, mas também na questão dos crimes cibernéticos, na falta de sinal de Internet, na falta de sinal de telefonia em muitas cidades do interior, que não é o principal. O principal são esses que eu coloquei e para os quais eu peço aos colegas Deputados a aprovação do requerimento. Acho muito importante para as questões dos crimes cibernéticos.

O SR. DEPUTADO RODRIGO MARTINS - Sr. Presidente, eu queria me inscrever.

O SR. PRESIDENTE (Deputado Leo de Brito) - Deputado Rodrigo Martins com a palavra. *(Pausa.)*

O SR. DEPUTADO DELEGADO ÉDER MAURO - Inclusive, colega, esse requerimento citado — V.Exa. está com o anterior — já foi retificado nesse ponto, já há uma retificação.

O SR. DEPUTADO RODRIGO MARTINS - Eu queria só solicitar...

O SR. PRESIDENTE (Deputado Leo de Brito) - Só um esclarecimento. Houve uma modificação da ementa: *"Solicita a realização de audiência pública para tratar questões de crimes cibernéticos no que diz respeito à operacionalização entre fato criminoso e investigação, entre outros"*.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Exato. Foi uma retificação.

O SR. DEPUTADO RODRIGO MARTINS - Eu, como Sub-Relator da área de segurança, queria pedir a aquiescência do nobre Deputado Delegado Éder Mauro para que possamos subscrever esse requerimento, tendo em vista a grande importância da participação das empresas de comunicação a fim de que possa solucionar alguns tipos de crimes que acontecem pelo uso da Internet, cibernéticos.

O SR. DEPUTADO SANDRO ALEX - Muito bem, Sr. Presidente. Ainda consta aqui no nosso sistema o requerimento antigo. Como V.Exa. já leu o novo requerimento...

O SR. PRESIDENTE (Deputado Leo de Brito) - Passarei a V.Exa.

O SR. DEPUTADO SANDRO ALEX - E também o Delegado Éder Mauro solicita que pode vir um representante da empresa. É isso?

O SR. DEPUTADO DELEGADO ÉDER MAURO - Representantes, que não os Presidentes, mas representantes das empresas.

O SR. DEPUTADO SANDRO ALEX - Acredito que é importante. Então fica essa ementa: “representante das empresas”.

O SR. PRESIDENTE (Deputado Leo de Brito) - Podemos votar em bloco, então, com as modificações propostas pela Deputada Alice Portugal?

Então, em discussão os requerimentos. *(Pausa.)*

Em votação.

Aqueles que concordam com a aprovação dos requerimentos mantenham-se como se acham. *(Pausa.)*

Aprovados os três requerimentos.

Passemos, então, à audiência pública com a participação das autoridades de segurança locais.

Convido para compor a Mesa a Sra. Patrícia Peck Pinheiro, advogada especialista em Direito Digital, e a Sra. Cristiana Oliveira Gonzalez, pesquisadora do Instituto Brasileiro de Defesa do Consumidor — IDEC.

Cada uma das participantes disporá do tempo de 20 minutos. Após as apresentações, será passada a palavra ao Relator, aos Sub-Relatores e aos autores dos requerimentos por 5 minutos. As convidadas respondem às indagações. Em seguida, respeitada a lista de inscrições, os senhores membros poderão interpelar as convidados por até 5 minutos.

Feitos esses esclarecimentos, vamos iniciar a audiência.

Passo a palavra à advogada Patrícia Peck Pinheiro. V.Sa. dispõe de 20 minutos.

A SRA. PATRÍCIA PECK PINHEIRO - Boa tarde a todos.

Obrigada Deputado Leo de Brito e demais Deputados pelo convite para estar aqui. Eu disponibilizei um material em Power Point para uma apresentação, que está sendo colocada na tela. Como temos pouco tempo, acredito que o convite venha no sentido de eu contribuir com a minha especialização em Direito Digital e a experiência que eu já reúno de 1998 a 2015. São 17 anos atuando com esse tipo de atividade. Já são 16 livros publicados.

Eu vou deixar o material, que ficará à disposição para quem quiser um pouco mais de literatura a respeito.

(Segue-se exibição de imagens.)

Inicio colocando que hoje temos uma necessidade de combate ao crime cibernético, chamado eletrônico, chamado digital. Dessas três nomenclaturas, do ponto de vista técnico, a mais atual é a de crime digital, mas a cibernética ficou mais popular em outros países. Então, independentemente da terminologia utilizada, podemos dizer que quase todo o crime, hoje, tem alguma faceta em meio digital, seja o início dele, seja sua forma de ocorrência, *modus operandi*, o meio em que acontece, seja o meio digital ser um facilitador para acesso a uma vítima, até de forma a torná-la mais, digamos, indefesa frente ao criminoso, assim como pode ser um fim em si mesmo, quando vamos atrás ou comparamos com o crime de invasão, ataques relacionados a bombas de dados, tirar do ar um sistema, fazer até mesmo apagão digital através de uma rede IP. Aí já são novas categorias tipicamente digitais. Então, vivemos esse paradigma, essa quebra de paradigma.

Compartilho com os senhores e as senhoras um sentimento de despreparo, em geral uma falta de capacitação seja de quem é o operador do direito nesse assunto, seja da própria população, como a linha de frente da defesa daquele que pode se proteger para evitar que haja uma ocorrência.

Do ponto de vista da cultura, no Brasil, apesar de vivermos uma insegurança na via pública das cidades e dos centros urbanos, as pessoas ainda têm uma

postura de extrema inocência perante a rua digital, chamada Internet, que é uma rua que alcança 2 bilhões de pessoas no mundo.

Todo o crime atual tem alguma dessas facetas em meio digital. Isso significa uma amplitude muito grande. Dificilmente qualquer ocorrência que chegue a uma delegacia não terá, se se fizer uma investigação mais completa, em algum momento, um digital. Hoje temos a *deep web* como uma internet praticamente assumida pelo crime organizado, apesar de não ter nascido com essa natureza. Temos ainda poucos meios ou ferramentas de acesso e combate a ela pela autoridade policial brasileira, apesar de haver mais monitoração da *deep web* pela Interpol e pelo FBI. Temos alguns grupos dedicados da Polícia Federal de algum Batalhão Militar fazendo essa vistoria, mas com pouco ferramental técnico.

Esse era o segundo ponto a que queria chegar. Temos hoje uma necessidade maior de investir em ferramentas técnicas no preparo da autoridade. Eu dei treinamento para uma equipe chamada GLO — Garantia da Lei e da Ordem, uma equipe militar, que, na época, atuou na Copa das Confederações e na Copa do Mundo. Temos as Olimpíadas no ano que vem. Quando pensamos em estratégico tático operacional em termos de combate ao crime, hoje há ainda um desafio de integrar essa atividade: quem tem o dever de agir e quem reporta para quem.

Eu vou ouvir o debate sobre o Alana. Conheço a instituição, que é muito bem quista, faz um trabalho ótimo. Seja ela, seja o instituto que eu criei, iStart, seja a SaferNet. Instituições que estão olhando a sociedade civil e tentando proteger o cidadão não têm com quem dialogar como sendo esse interlocutor dentro do ambiente público para esse tipo de trabalho, ou seja, um repasse de denúncia, um trabalho de inteligência de reunir dados, de aprender mais a verificar provas e perícias digitais.

Então, essa formação, do ponto de vista universitário, poderia ser algo chancelado como obrigatório. Eu acredito que toda faculdade com uma relação direta para formar um operador do direito teria que ter aula obrigatória de prova e perícia digital. Eu acho que uma faculdade, hoje, de Direito que não tem nenhuma aula no laboratório informático para ensinar àquele que está estudando como aplicar a lei, como se coleta uma evidência, como se extrai uma informação de um WhatsApp...

Este ano tivemos um aumento muito grande de inquéritos policiais cuja instrução é o WhatsApp. Se o cidadão comum tiver sua carteira furtada, ele sabe o que fazer. Ele vai fazer um boletim de ocorrência de furto na delegacia. Agora, se ele tem um celular furtado com dados que ele tinha ali dentro, ele já não sabe como agir. Se ele precisar juntar uma prova que está na Internet, ele não sabe como agir — se basta um *print* de tela ou se precisa fornecer o equipamento, como em muitos casos, para que se colete evidências de autoria.

Casos envolvendo jovens e adolescentes que são assediados por pedófilos ou são envolvidos em algum tipo de ataque de engenharia social para assalto ou sequestro, em geral, por vergonha, apagam aquilo que estava localmente no seu celular. Assim os próprios pais não imaginam que tinham que ter retirado o dispositivo da posse daquele jovem para fins de verificação e perícia na delegacia.

Já vimos integrantes do Ministério Público, que já tive a chance de apoiar também em treinamentos, perguntarem, terem dúvidas do que deve ser feito para a coleta de prova. Então, esse um ponto fundamental é a formação em nível universitário e campanha de conscientização da população.

Há condutas não tipificadas. Preocupa-me muito o fato de que paramos aquilo que havia de discussão de crimes cibernéticos, informáticos, digitais ou eletrônicos no Brasil, contentando-nos com meros quatro artigos praticamente em termos de conduta. Apesar de toda uma evolução para atualizarmos o Código Penal, o crime dessa categoria exige penalidade mais alta, até para justificar que haja autorização de interceptação de comunicação.

Nós temos todo um *modus operandi* investigativo. Não é tratado com um nível de periculosidade e de gravidade que tem hoje o crime cibernético no Brasil. Isso é alterado por lei, em termos de aumentar pena e tentar entender o que fazer, que é o último ponto, com o criminoso digital.

Não podemos pegar aquele que pratica latrocínio, juntá-lo com alguém que sabe fazer *fishing*, que é um arquivo malicioso, deixá-los numa mesma cela por um ano e liberar dali o bandido versão 3.0.

Então, do ponto de vista da sustentabilidade, também é uma visão legislativa o que vamos fazer em termos de execuções penais de encarceramento digital daquele que pratica o crime digital, que pode ter também como punição contribuir

para o combate ao crime digital, como acontece em outros países com o uso do *ethical hacking.* Mesmo aquele que já foi pego, depois tem que ajudar a pegar os outros.

Os crimes digitais mais comuns. Do ponto de vista prático, para alcançarmos uma efetividade quando evoluirmos o nosso conceitual, envolve pensarmos que há hoje tipos penais que precisam ser melhorados para enquadrar esses crimes.

Nós temos tido muitos casos *in dubio pro reo.* Esse é o princípio no Direito. Temos ainda muita dúvida de autoria porque temos dificuldade do flagrante *on-line*, que é o flagrante de pegar praticamente a pessoa com a mão na máquina ou alcançar materialidade daquele crime.

No crime de entorpecentes, apesar de ter muitos casos em que a prova do tráfico está em mensagem do WhatsApp, ainda se tem uma dificuldade maior de punição se não chegar ao local, onde estiver o conteúdo da droga. Então, nós temos situações hoje...

Concordo em ouvir empresas de telecomunicações, provedores, mais à frente. É uma forma de enxergar quem tem hoje as testemunhas-máquinas que nos dizem quem fez o quê.

Enquanto não mapearmos esse fluxo de colaboração com a autoridade, que pode significar aumentar, por exigência legislativa mesmo, o que guardar, para quem apresentar e como...

Hoje em dia, é muito fácil, pelo que ficou previsto no Marco Civil da Internet, alegar que, por uma questão de limitação técnica, não há como apresentar aquela evidência.

Isso ficou sendo algo colocado dentro da lei, do Marco Civil da Internet, que ainda acaba prejudicando bastante o entendimento do que significa uma limitação técnica para apresentação de uma evidência digital.

Há o furto de identidade, ou *identity thief*, que é hoje talvez o crime mais combatido no mundo. É justamente quando alguém consegue fingir ser outra pessoa para atacar alguém e dar um golpe como, por exemplo, praticar uma compra falsa no nome de uma pessoa, montar um perfil falso para provocar difamação de outra pessoa. Então, isso nós vamos ver que está diretamente relacionado à discussão do

modelo de identidade digital obrigatório. Já tivemos aí alguns andamentos no Brasil, mas enquanto não ficar bem resolvido a *identity thief*...

No Estado da Califórnia, nos Estados Unidos, há pena altíssima, reclusão de 5 anos, multa altíssima, tudo para se combater "o fingir ser outra pessoa".

No Brasil nós favorecemos muito algumas práticas por uma questão de consenso social que, para nós, não nos choca tanto: a pequena mentirinha sobre a identidade. Quem é aquela pessoa? O brasileiro eventualmente se faz passar por alguém ou pede para alguém se fazer passar por ele por uma questão de conveniência. Hoje muitos pais permitem que filhos mintam a idade para o Facebook. Então, eles escrevem uma data de nascimento falsa para poder ter acesso a um serviço que exige idade mínima de 13 anos.

A meu ver, acostumamos as pessoas desde pequenininhas a praticarem o art. 307 do Código Penal. Eu acho que mentir uma identidade para enganar os outros na Internet ou praticar um crime deveria ter uma pena, com certeza, muito maior do que a que tem hoje.

Há a fraude eletrônica, há o estelionato digital, que — hoje temos o golpe da loja *on-line* fantasma —, quando vai chegando a época de *black Friday,* aumenta bastante. Isso é algo que afeta diretamente o cidadão — diretamente! Na maior parte desses crimes ou não identificamos autoria, ou não conseguimos enquadrar completamente num tipo penal. Crime de furto, art. 155 do Código Penal, trata que é furto tornar indisponível coisa alheia móvel. Tornar indisponível significa "se eu tenho, você não tem". Isso é da época ainda física.

Nós construímos um conceito do furto de bens intangíveis, como é o furto de energia e o furto de sinal. Mas quando falamos de furto de dados, que é o Ctrl+C, Ctrl+V, que é alguém entrar e levar uma informação, não conseguimos aprimorá-lo. Melhoramos com a legislação de crimes eletrônicos, apelidada de Carolina Dieckmann, o crime de invasão, mas não o furto: alguém levar uma coisa que não era dela — o Ctrl+C, Ctrl+V. Tivemos dificuldade ainda do quê? De redigir. A redação técnica para leis sobre esse assunto é desafiadora não só no Brasil, mas também em outros países, porque senão facilmente enquadramos uma conduta lícita numa ilícita. E realmente envolve todo um estudo aprimorado de como está sendo feito. Temos muitos avanços sobre esse tema, principalmente na Europa

(Alemanha e Reino Unido) e assim por diante. No Reino Unido porque houve as Olimpíadas da última vez.

Há o golpe do boleto falso e o golpe do aplicativo falso. Ainda me admira muito o quanto não há um compromisso de orientar o cidadão para se proteger nesse ambiente. Por que aumentou o golpe do aplicativo falso? Não sei se vocês têm o hábito de baixar qualquer aplicativo só porque é de graça. Vivemos esse problema. Não existe almoço grátis. As pessoas acham que porque é de graça está tudo bem. Antigamente os antigos diriam que se é de graça, desconfiem. Então, acabamos mudando um pouco a cautela, que seria uma cautela que herdamos na família de que você tem que ter cuidado, que às vezes aquilo ali pode ter algum problema.

Há ainda os crimes de pedofilia e pornografia infantil, de invasão, de furto de dados, crimes contra a honra em geral (difamação), crimes de racismo e de ameaça que acabam sendo bem recorrentes também. Esses são os mais recorrentes.

Quadrilhas usam jogos *on-line* para atacar vítimas. Hoje qualquer jovem que se conecta na Internet está na rua. Os pais têm autorizado as crianças a partir de 6 anos de idade, em média, a usar jogos que estão nesse *ranking*, como League of Legends, World of Warcraft, Dota 2, Minecraft, Dragon Age. A maioria deles permite um *chat* de diálogo entre as pessoas.

Se antes alguém ligasse na casa de alguém diria: *"Quem está falando?"* Hoje o bandido salva a vida daquele jovem no jogo digital. Vocês acham que o jovem não vai contar tudo para ele depois? Vai achá-lo o seu herói: "Você me salvou no jogo!"

Então, está muito fácil entrar na residência, na escola. Não mais existem muros e paredes nas portas. A sociedade digital está sem essa proteção. Essa proteção física não segura o crime digital.

A pornografia infantil cresce. A *deep web* tem tido ambientes como esses OnionPedo com vídeos de pornografia infantil. Muitos aplicativos falsos baixados acionam no *tablet* daquela criança a câmera. Filmam a criança de baixo para cima, em ângulo sensual e mandam para o OnionPedo. Então, quando formos olhar é logico que existe uma força-tarefa que não vai funcionar se não for por imposição legal, por lei. Ou eu obrigo um fabricante ou não, como fizemos com a indústria automobilística, porque segurança vem de fábrica. Se cinto de segurança não viesse

obrigatório de fábrica, será que nós escolheríamos colocá-lo? É aí o porquê de todo o resto, antivírus e todas as outras questões.

Aqui é o do boleto falso. Também acontece por um vírus instalado no equipamento. Muitas universidades estão sofrendo com esse tipo de golpe, que acaba afetando a relação dela com aquele aluno que paga um pagamento *on-line* em qualquer máquina, que troca o código de barras. E aí, claro, deveríamos ter campanha de segurança pública digital em televisão e rádio obrigatória, o que foi previsto no Marco Civil da Internet, mas não está acontecendo.

Tem que ser algo forçado para todo e qualquer que hoje ganha dinheiro com economia digital, seja um provedor de conexão, seja uma empresa de telecom, seja um fabricante de celular, seja um fabricante de *tablets.* Se todos orientassem sobre isso obrigatoriamente, como fazemos com outras indústrias... A indústria da tecnologia é a única que faz *recall* sem obrigação legal. Ela diz que é uma atualização.

Aqui mostra: *App Store sofre seu primeiro ataque; onda de malwares já foi removida.* Há 344 aplicativos falsos dentro da App Store. Digam os senhores e as senhoras: quando algum brasileiro entra numa App Store, ele acha que lá dentro está baixando um aplicativo que é o criminoso, que é o bandido na máquina dele? Qual a probabilidade de esse cidadão se defender e qual a colaboração para saber de onde veio aquele aplicativo? Hoje o problema é que aquele que desenvolve esse artefato malicioso não tem punição. Nós chegamos, no máximo, àquele que faz a transferência da conta do dinheiro de uma pessoa para outra pessoa — e olhe lá se não estiver envolvido um laranja. Então, tendo mais tempo, daria para explicar esse *modus operandi*. Eu ensino isso hoje nas aulas para a faculdade, para a polícia: como o *fishing*, que hoje virou aplicativo, não é mais o clique aqui por *e-mail,* é o golpe do aplicativo, mas está em algum lugar sendo baixado.

Então, aqui também: Facebook, com lojinha do androide aqui, é a mesma coisa. Cowboy Adventure, Jump Chess, ou seja, são joguinhos. Hoje qualquer cidadão brasileiro e também qualquer cidadão de outro país estão sujeitos a isso. De repente, eu tenho a cracolândia digital, eu estou na rua escura digital, com alguém chancelando com uma marca e vem até aqui. E o que você baixar é problema seu, o risco é seu, por sua conta e risco. O meu termo de uso me garante que a segurança

não depende de mim. Coloque um bom antivírus, um bom *antispyware*. A cultura do brasileiro para colocar antivírus no celular... Quem de vocês tem antivírus no celular? Todos? *(Pausa.)* Por favor. Coloque no dos filhos também, no celular de qualquer parente ao redor. O pior sabe qual é? O aplicativo gratuito que finge que é um antivírus. Você baixa, e ele é o vírus. É impressionante isso!

Google remove apps falsos da Caixa Econômica e do Banco do Brasil. Remove, fez uma gentileza. E a responsabilidade? Onde está a responsabilidade?

Apps falsos do Minecraft são colocados na Google Play.

O meu filho tem 8 anos de idade, gente! Qual é a probabilidade? Ele tem um *tablet,* o aplicativo é gratuito, ele não precisa do meu cartão de crédito. Ele baixa isso daqui, e aquilo passa a se tornar já algo que pode depois até vir a pegar o meu cartão de crédito na hora em que eu usar o *tablet* dele para ajudá-lo a comprar alguma coisinha para o jogo. Querendo ou não, por omissão, negligência, inação, o que seja, existe um ambiente propício para que uma quadrilha ataque pessoas em uma arapuca digital, com uma característica de um local seguro e idôneo. É assim que a gente entra nesses lugares na Internet.

Aqui também é a mesma coisa. Um vírus disfarçado de emulador do Nintendo, roubando dados do androide e assim por diante. Isso aumentou muito. Uma dupla suspeita de fraude relacionada a isso, em bancos, foi achada aqui no Brasil, e o brasileiro, inclusive, exporta técnicas para ataques. Nós somos muito criativos. Somos também bem especializados em explodir caixa eletrônico. Também exportamos isso para o Chile e Portugal. Duas pessoas são vítimas de golpe a cada 5 minutos do Brasil. A grande questão não é só o preparo da polícia, a falta de treinamento, a falta de ferramenta, a capacidade de gerar uma punição mais elevada, a capacidade de guarda de provas e leis mais fortes relacionadas a combate de crime, porque não dá para parar no que fizemos nos últimos 10 anos.

Aí estão *sites* já atacados. Há vários casos no material. Eu trouxe bastante caso.

Agora vou para a conclusão.

Nós já temos no Reino Unido...

Aqui, colocando que a testemunha da era digital é a máquina. Quem tem uma máquina pode ser chamado a depor, porque foi a máquina que viu o que aconteceu.

Não sei se a máquina colaborou, participou, se existe uma responsabilidade pelo dono da máquina, mas, em princípio, ele é chamado como testemunha, e, se não apoiar de forma rápida, não temos nada. Hoje a prova é digital. Esse conjunto de zeros ou uns é a nossa grande prova digital.

Como proteger o cidadão? Hoje o pai dá um celular para o filho no Dia das Crianças e diz três coisas: *"Querido filho..."*

Celular de verdade não tem idade mínima, não tem nenhuma indicação de segurança escrito na embalagem pelo lado de fora, por dentro, não importa. O celular da Barbie vendido na loja de brinquedos tem idade mínima de 3 anos e pelo lado de fora diz dicas de segurança, inclusive para você não comer o celular e morrer engasgado.

O que os pais dizem quando dão um celular para o filho de presente? "*Não vai gastar muito crédito, não vai quebrar a telinha e não vai perder o aparelho!"* Disse o que para proteger o filho? E quem disse? Quem tem o dever de dizer? Esse é um ponto para nós pensarmos do ponto de vista de legislação, para, pelo menos, proteger as crianças.

Esta é a rua onde crescemos. Nós ainda pensamos muito em crime aqui.

Esta é a rua de praticamente mais de 20% dos brasileiros, com menos de 24 anos, que crescem nessa rua, que falam que estão sozinhos em casa no Twitter e atrai o cara para sequestrá-lo ou o assaltante para assaltar a família. Esse é o *modus operandi* do digital afetando o presencial e vice-versa.

A Inglaterra tem um *plugin* no *browser* que você aperta e vai uma denúncia de um *site* suspeito para a polícia investigar. Você já tem grupos de WhatsApp de bairros para tentar fazer reunião de provas para juntar para as pessoas. Como a *web* é pública, se alguém estiver de olho... Hoje não estamos fazendo policiamento digital da Internet. Não existe a viaturazinha passando nessa rua.

Por último, só para fecharmos, um jovem, que tem acesso à tecnologia cada vez mais barata, que vai ganhar um celular no Dia das Crianças, independente da idade — tem gente dando celular para o filho com 4, 6, 10 anos com capacidade de tirar foto, filmar, de reunião de dados; dados valem dinheiro, dinheiro são dados —, conecta-se ao mundo, a uma rua digital de bilhões de pessoas, usando qualquer

wi-fi, sem orientação, sem vigilância, sem supervisão. É risco. Então, vivemos hoje uma conta grande de risco digital.

Temos várias campanhas educativas como, por exemplo, *Eu faço o que você quiser, só me devolve meus dados*. Isso hoje é uma ameaça muito comum pela qual as pessoas passam. Será que tinha que ter idade mínima? Como fazer *enforcement* dessas idades mínimas que já estão no termo de uso? Como trabalhar a segurança pública digital? Há aspectos técnicos, há aspectos jurídicos.

Eu deixei um *check-list* de como combater o crime digital: fazer campanhas de conscientização de segurança pública digital — dá para pegar o que foi previsto no passado no Marco Civil da Internet; elaborar novas leis — precisamos de novas leis para combater mais efetivamente, inclusive o que é terrorismo digital, porque ainda está incompleto esse assunto; atualizar a questão sobre o encarceramento digital e implementar o procedimento de polícia para revista digital.

O que é a revista digital? É que grande parte das provas hoje vão estar em um dispositivo de celular; é a possibilidade, como o Reino Unido fez nas Olimpíadas de Londres, que está aqui.

Esta é uma matéria muito interessante para quem tiver interesse em olhar. Estão aqui todas as referências de que você pega o celular, passa, conecta aqui, passa um *software* com palavras-chave e com imagens. Você não tira nada do celular, só vê se ali dentro tem uma evidência de algo que pode ser suspeito para um crime. Se sim, leva a pessoa para procedimento de averiguação; se não, a pessoa segue. Isso aqui só se pode fazer no Brasil se conseguirmos avançar em termos de lei, de legislação mesmo.

Estes são os países que já possuem revista digital. Estão combatendo o crime eletrônico, estão ficando mais fortes.

Aqui está toda uma legislação que ajuda a nos apoiar naquilo que quisermos continuar construindo, mas temos que cumprir esse papel de defesa digital. Temos motivação jurídica desde a legítima defesa, do art. 25 do Código Penal, a vários outros que eu coloquei aqui para vocês.

O que seria importante esta CPI conseguir alcançar ao final é um combate mais ostensivo do crime cibernético, trazendo para nós um cidadão brasileiro blindado, mais protegido, a legislação, liderança em leis. O Executivo poderia apoiar

na implementação de campanhas educativas, inclusive com *enforcement* do MJ; a própria ANATEL junto com as operadoras exigir campanhas de segurança pública digital; o Judiciário combatendo a impunidade; a autoridade policial agindo de forma integrada e podendo coletar provas; a sociedade civil aprendendo a se proteger, não deixando mais a porta aberta. Tem que colocar senha de bloqueio e tem que fechar a porta. Por que a família brasileira, hoje, quando vai dormir, não fecha a porta da Internet? Não sei. Mas hoje existem 23 Estados brasileiros com legislação que proíbe celular na sala de aula. A culpa não é da tecnologia, mas, com toda a certeza, a tecnologia tem que ajudar a resolver o problema que ela criou, tem que ajudar a proteger a pessoa no uso da própria tecnologia.

O homem não pode se tornar um verdadeiro homem sem a educação. Eu acredito muito que, com legislação, poderemos trazer uma obrigação maior de educar para combate ao crime. Vamos diminuir o número de pessoas que caem no golpe fácil, e, quanto ao restante, ajudamos a evitar aquilo que possa acontecer de maior.

Pensem sobre isto: o que eu faço com um criminoso digital? Nós não podemos pensar a lei penal apenas na previsão do tipo penal, mas temos que pensar no depois, no que eu vou fazer com esse criminoso digital. Gostaria que vocês ficassem com essa reflexão. Primeiro, temos que pegá-lo, temos que diminuir a quantidade de cidadãos que caem num golpe, temos que aumentar a própria proteção, no geral, que temos na Internet, com ajuda de quem são os principais agentes operadores da Internet brasileira e das tecnologias. Mas temos que pensar o que vamos fazer com ele. Acho que sobre isso seria importante refletir.

Os outros países têm colocado o criminoso digital em prisão domiciliar ou em presídio de segurança máxima. Ou é um caso, ou é outro caso, mas tem que se fazer o encarceramento digital, senão ele continua lá preso, operando, assaltando e furtando todo o mundo pela via digital. Uma grade física não segura o novo bandido da Internet.

Era isso que eu queria dizer para vocês.

Obrigada.

O SR. PRESIDENTE (Deputado Leo de Brito) - Agradecemos à Dra. Patrícia Peck.

O SR. DEPUTADO ARNALDO FARIA DE SÁ - Sr. Presidente, eu só queria saber se a Dra. Patrícia vai disponibilizar...

A SRA. PATRÍCIA PECK PINHEIRO - Ah, sim.

O SR. DEPUTADO ARNALDO FARIA DE SÁ - ...toda essa exposição, que é importante para nós.

A SRA. PATRÍCIA PECK PINHEIRO - Sim, temos bastante material.

O SR. PRESIDENTE (Deputado Leo de Brito) - A exposição ficará disponível, inclusive na página da CPI.

A SRA. DEPUTADA MARGARIDA SALOMÃO - Presidente, além dessa questão, eu tinha solicitado — e foi aprovado por esta Comissão — a presença, aqui, nesta audiência, do Prof. Pedro Mizukami; mas ele não foi contactado pela Comissão, nós verificamos isso. Então, eu queria...

O SR. PRESIDENTE (Deputado Leo de Brito) - Fica registrado o pedido de V.Exa.

A SRA. DEPUTADA MARGARIDA SALOMÃO - ...apresentar esse fato e dizer que, quem sabe, ele pode ser convidado para uma outra audiência.

Agora, de todo modo, também quero pedir a sua atenção, como Vice-Presidente, para que isso não se repita.

O SR. DEPUTADO ARNALDO FARIA DE SÁ - Sr. Presidente, eu queria fazer uma indagação à Dra. Patrícia sobre se faltou algo que ela pudesse trazer de informação, de orientação e de esclarecimento para a CPI.

O SR. PRESIDENTE (Deputado Leo de Brito) - Dra. Patrícia...

A SRA. PATRÍCIA PECK PINHEIRO - Ah, sim. *(Risos.)* Com os minutinhos que eu tive para a apresentação, eu tentei ser o mais sucinta possível; mas sim.

O SR. DEPUTADO ARNALDO FARIA DE SÁ - Eu acho que nós poderíamos, Presidente, convidá-la novamente ou permitir que ela complementasse no tempo. Eu abriria mão do meu tempo, por exemplo, para que ela pudesse falar.

O SR. PRESIDENTE (Deputado Leo de Brito) - Não, se ela...

O SR. DEPUTADO DANIEL COELHO - Nós vamos fazer as perguntas, e ela vai ter tempo para...

O SR. PRESIDENTE (Deputado Leo de Brito) - Nós vamos ter tempo. Ela não está indo embora agora. Ela vai continuar conosco. Inclusive, se V.Exa. tiver

algumas perguntas pertinentes, algumas dúvidas que ficaram em relação à apresentação, terá oportunidade também de apresentá-las. As inscrições estão sendo feitas agora.

O SR. DEPUTADO ARNALDO FARIA DE SÁ - Sr. Presidente, eu acho que ela poderia falar mais, sem necessidade de ser perguntada. Depois perguntaríamos. Dê mais algum tempo adicional para ela, porque eu percebi que ela correu, e havia coisa importante que ela poderia ter clareado. Era isso que eu queria propor.

O SR. DEPUTADO SILAS FREIRE - Sr. Presidente, eu sugiro... A expositora fez uma exposição baseada nos minutos que estavam dados a ela. Serão feitas algumas perguntas aqui. Eu sugiro a ela que, se tiver alguma informação fora das perguntas que serão formuladas aqui, complemente com o material, para que V.Exa. disponibilize a todos os integrantes da CPI.

A SRA. PATRÍCIA PECK PINHEIRO - Está ótimo.

O SR. PRESIDENTE (Deputado Leo de Brito) - Nós tínhamos combinado assim. Inclusive agradeço a ela não só pela colaboração com a CPI, mas também por disponibilizar para todos os Parlamentares e também para convidados esta cartilha, *Ética e Segurança Digital,* uma cartilha orientativa da Campanha *Família mais Segura na Internet*, que certamente também é um dos trabalhos que a CPI está fazendo, doutora, exatamente trabalhando a questão da prevenção do crime, porque, do ponto de vista de uma política de segurança pública, nós sabemos que o aspecto preventivo é muito forte.

A SRA. PATRÍCIA PECK PINHEIRO - Isso é fundamental.

O SR. PRESIDENTE (Deputado Leo de Brito) - Então, nós lhe agradecemos. A doutora vai ficar à disposição também para as perguntas e vai ter os seus minutos finais, podendo, inclusive, acrescentar algo nas suas considerações finais. Está bom?

A SRA. PATRÍCIA PECK PINHEIRO - Está ótimo.

O SR. PRESIDENTE (Deputado Leo de Brito) - Então, agora, passo a palavra, pelo tempo de até 20 minutos, para a Dra. Cristiana Oliveira Gonzalez, do Instituto Brasileiro de Defesa do Consumidor — IDEC.

A SRA. CRISTIANA OLIVEIRA GONZALEZ - Boa tarde a todos! Gostaria de agradecer o convite da Comissão. Eu sou pesquisadora da área de

Telecomunicações e Internet do Instituto Brasileiro de Defesa do Consumidor — IDEC, onde trabalhamos tanto com a regulação sobre o serviço de telecomunicações quanto com questões relacionadas à Internet, sejam elas a liberdade de expressão, a privacidade ou o próprio acesso à Internet. Mas hoje eu vou limitar a minha apresentação à questão do cibercrime e à proteção dos consumidores, já que é o tema desta CPI.

Eu não vou fazer uma grande explanação sobre o contexto que nós vivemos atualmente, mas acho que é bastante claro para quem está aqui que nós vivemos um contexto de grande abundância e disponibilidade de dados, principalmente de dados pessoais.

Então, toda vez que nós entramos na Internet, toda vez que usamos o celular, seja *on-line*, seja *off-line*, com uma câmera gravando a nossa imagem, o banco colhendo as nossas digitais, pagando o cartão de crédito, nossas compras, tanto *on-line* quanto *off-line*, nós estamos gerando dados. Para onde esses dados vão? Essa é uma grande questão.

Esses dados, então, são armazenados, analisados, estudados, vendidos para governos e empresas — e aqui eu não estou falando só do Brasil; eu estou falando de um contexto global —, com finalidades diversas, seja para vigilância, seja para controle das nossas atividades, no caso de uma câmera, inclusive das nossas digitais, seja simplesmente para *marketing*.

A chamada publicidade comportamental, a publicidade dirigida na Internet, ocorre quando acessamos um *site* e começa a aparecer uma série de anúncios ligados à nossa atividade *on-line*, palavras-chave que procuramos nos buscadores, termos usados em redes sociais ou mesmo para a própria obtenção de lucro, que são os grandes intermediários chamados *data brokers*, que utilizam os nossos dados registrados na Internet para revender a terceiros.

Também podemos falar de conceitos ligados à inovação e até de políticas públicas, quando nós usamos dados para analisar determinado tipo de comportamento em uma população ou no caso de doenças e até mesmo na própria inovação e geração, por exemplo, de remédios, no caso da Medicina. Enfim, existem diversos usos legais e ilegais para esses dados. O que acontece é que hoje nós vivemos no limbo, principalmente no Brasil, mas eu vou falar mais sobre isso depois.

Nesse contexto de abundância de dados — existe um termo para isso chamado *big data* —, a Internet adquiriu um duplo caráter. Então, por um lado, ela dá grande poder e autonomia para o usuário de criar o seu próprio conteúdo, de ter mais mobilidade. Por outro lado, ela pode ser usada para determinados tipos de abuso e práticas ilegais. Isso acaba quebrando a própria confiança dos indivíduos em algumas instituições.

A Dra. Patrícia já falou bastante dos tipos de crimes e acho que vocês já têm discutido razoavelmente bem essa questão. Inclusive, no Congresso, já há leis aprovadas sobre esses temas, mas nós temos vários problemas. Então, nesse contexto de abundância de dados, nós temos vazamento de fotos, crimes de pornografia infantil, racismo inclusive, fraude, furto e perda de dados, *spam* e inclusive o *malware*.

Então, por que não discutir, não incrementar o uso das leis, já que o Brasil — como tem sido anunciado e essas reportagens são recentes — enfrenta um grande problema em relação aos crimes cometidos na Internet, que inclusive afetam empresas e consumidores? Eu diria que o cibercrime é como qualquer outro tipo de crime, só que ele é cometido com táticas diferentes. O autor dessa frase chama-se Bruce Schneir. Ele é um americano, atualmente pesquisador de Harvard, e é um especialista em segurança e criptografia.

Então, quando nós pensamos nesse contexto de abundância de dados, onde crimes podem ocorrer, nós, por outro lado, temos que pensar que na verdade é apenas um crime sendo cometido por outro meio e com uma técnica, uma tática diferente. Os dados estatísticos, então, nós temos que questionar, e eu já vou mostrar o porquê. As questões das leis atuais, eu discordo um pouco da Dra. Patrícia de que nós temos que incrementar a legislação, principalmente sobre a Internet.

Acho que, no Brasil, nós temos problema, sim, que têm que ser resolvidos, mas também nós temos que olhar para as leis que estão disponíveis hoje e podem ser muito bem usadas na persecução criminal e os próprios cuidados que o indivíduo deve ter. No caso, ninguém sai de casa sem fechar a porta. Por que nós deixamos nossa senha disponível? Por que nós não temos algum cuidado quando acessamos um *site*? Ninguém estaciona o carro, deixa a janela aberta e a chave na

ignição. Então por que, quando nós lidamos com tecnologia, o nosso comportamento é diferente? Ele é mais descuidado e isso pode dar margem para que os crimes aconteçam.

Então, vamos às estatísticas: algumas pesquisas mais recentes que outras, ou não, têm questionado a questão dos números sobre cibercrimes e também do custo para a sociedade. É por aí que elas questionam: a qual conclusão essas pesquisas chegam? Do ponto de vista econômico, poucos criminosos conseguem alcançar ganhos efetivos e é uma atividade de baixa lucratividade para a maioria. Enfim, quando nós falamos de *spam,* de roubos de senha, entre outros crimes, o acesso ao recurso comum, que seriam esses dados na Internet, o acesso a recursos comuns, ele é um mau negócio, porque quanto mais criminosos existirem e tiverem acesso a esse dado, esse negócio, vamos dizer assim, do crime vai ter um retorno muito pequeno. Então, na verdade, quando nós, em geral, falamos de cibercrime, o discurso é do medo: *"Vejam como as nossas crianças estão vulneráveis*!";*"Vejam quantos crimes acontecem na Internet!"; "Vejam os prejuízos que ela causa!".*

Mas eu acho que uma recomendação aqui para esta Comissão seria de analisar mais profundamente, com dados técnicos, quais são os impactos do cibercrime e quais são os números reais desses crimes. Então, na verdade, esse dinheiro fácil, vamos dizer assim, do crime acaba se esgotando facilmente. Então, não existem grandes milionários cibercriminosos. Existe um par, vamos dizer, de cibercriminosos e o resto, enfim, não consegue lucrar em cima dessas atividades, vamos dizer assim, ilícitas cometidas na rede.

O outro problema dessas estatísticas é que, enfim, elas têm equívocos diretamente proporcionais à forma como esses dados são gerados. É habitual que entrevistem uma ou duas pessoas, uma ou duas empresas, e perguntem quais são os prejuízos que elas têm com o cibercrime, e esses valores são superestimados e nunca reduzidos a zero. Então, são exemplos cartões de crédito roubados, enfim, quando um número de cartão de crédito é roubado, por quanto se pode revender esse cartão de crédito? Em geral, são centavos de dólares ou poucos reais, que são bem difíceis de serem monetarizados.

Bom, eu tinha falado sobre a lei. Nós já dispomos de uma legislação específica. Não sei, imagino que vocês devam se lembrar. Eu me lembro bem que o

IDEC fez uma campanha aberta para tentar barrar o Projeto de Lei Azeredo. Por quê? Porque ele ia permitir uma série de violações e porque ele tinha termos muito abrangentes. Ele ia, por exemplo, criminalizar a obtenção e a transferência de dados e informações sem autorização, o que é muito complicado do ponto de vista tecnológico. Quando nós acessamos um *e-mail*, estamos transferindo ou fornecendo dados sem autorização, necessariamente. Então, essa atividade, a simples leitura de um *e-mail*, passaria a ser criminalizada; e seria difundir um código, uma licença em um sistema informatizado. Esse termo "sistema informatizado" é demasiado amplo também. Enfim, outras questões previstas no próprio PL Azeredo são bastante complicadas.

Para tentar solucionar o problema, porque isso não significa que nós não enfrentemos questões importantes na questão do cibercrime*,* houve todo um movimento de aprovar leis alternativas, o que ficou apelidado de Lei Carolina Dieckmann, pelo vazamento de fotos íntimas de uma atriz famosa, e acabou contemplando alguns pontos que eram previstos pelo projeto de lei do Deputado Azeredo. É o caso da invasão a dispositivo informático, por exemplo; ação penal, no caso da questão de roubo de cartão de crédito; acesso ao sistema sem autorização. Vários pontos ficaram suficientemente contemplados e descritos de uma maneira muito mais específica na chamada Lei Carolina Dieckmann, que é a Lei nº 12.737, de 2012.

Outras questões, como a pedofilia na Internet, acabaram sendo também contempladas na reforma do Estatuto da Criança e do Adolescente, e, por último, para provar que mais importante do que criminalizar ações na Internet é garantir direitos, direitos civis, direitos fundamentais, direitos humanos na Internet, por isso veio a aprovação do Marco Civil da Internet.

Eu também queria falar que, além das leis, existem outras formas de se combater atividades ilícitas e de se proteger na Internet ou de se proteger diante do avanço da tecnologia. O CERT, que é a sigla para Centro de Estudos, Resposta e Tratamento de Incidentes, hoje, no âmbito do NIC.br, que, vamos dizer assim, abriga esses grupos de tratamento de incidentes, desenvolve várias cartilhas com orientações para os usuários, para as empresas, para quem desenvolve um *site* sobre formas como se proteger melhor *on-line.* É claro que ninguém, sozinho, vai

chegar a esta cartilha, enfim, o consumidor comum. Mas aí eu acho que eu concordo com a Dra. Patrícia: uma campanha de educação, usando esse tipo de instrução, seria importante nessa questão.

Então, em termos gerais, são milhares e milhares de cartilhas sobre vários temas. Eu não vou me especificar nessa questão, mas o primeiro passo seria que o consumidor ou usuário estivesse ciente de que tudo o que faz *on-line* é real. Os seus dados, que estão sendo fornecidos num determinado *site* de comércio eletrônico, são reais; o número do seu cartão de crédito é real. Dessa forma, uma vez conscientizados de que cada passo que nós damos na Internet é real, não é virtual, nós podemos, enfim, estar mais vulneráveis a riscos reais. Então, esse projeto de conscientização tem que ser feito com os consumidores em geral.

Além de ser consciente de que esses riscos são reais, outro passo importante a ser dado é que, como eu falei no começo, todos os cuidados que nós temos fora, ou seja, ninguém sai de casa sem trancar a porta, nós temos que ter no ambiente *on-line*, ou seja, visitar os *sites* e fazer compras em *sites* de lojas confiáveis, ficar atento quando for usar o banco *on-line* ou fazer compras, não passar sua senha ou suas informações para pessoas estranhas, enfim, é o que nós chamamos de não deixar a porta da casa aberta.

Nas questões do *site*, é preciso sempre se certificar de que o *site* é confiável, pesquisar referências, não fazer compras por *wi-fi* pública, por exemplo, nem por computadores de terceiros. No caso específico do acesso a *sites*, devemos utilizar *sites* que tenham *https*, que é um protocolo que usa certificados digitais e assegura a identidade do *site*, tanto de destino quanto do próprio *site* sendo visitado. Há uma série de precauções possíveis, fáceis, que não vêm sendo tomadas e dispensam uma nova legislação.

Então, para se proteger e reduzir os riscos, é importante adotar uma postura preventiva, no caso do consumidor, e que tenha sempre atenção à segurança como um hábito incorporado, não deixar a porta nem a janela de casa aberta nem o vidro do seu carro também aberto. Existem diversos mecanismos de segurança sobre como lidar com contas e senhas, inclusive de como proteger a forma do seu fluxo de dados na Internet, por exemplo, criptografando *e-mails*.

Nesse contexto em que existe um fluxo muito grande de dados também, além do cuidado com o indivíduo, como nós falamos, um cuidado com as pontas, ou seja, existe um indivíduo aqui, uma empresa, um servidor do outro lado, nós temos que ter muito cuidado com a questão da responsabilidade dos intermediários. E quem são os intermediários? São as operadoras de rede, os provedores de conexão, os desenvolvedores de uso de conteúdo no *site*, de aplicativos no celular. Existe um rol imenso de intermediários, de prestadores de serviço, comerciais ou não, e plataformas de rede social que muitas vezes são responsabilizados pelas ações cometidas na Internet.

O Marco Civil, no art. 18 e 19, fala sobre a questão da remoção de conteúdos *on-line*, por exemplo, que deve ser feita apenas com ordem judicial. Mesmo que exista uma previsão de antecipação de tutela, essa remoção só deve ocorrer com ordem judicial. Além disso, deve-se garantir a inviolabilidade e o sigilo das comunicações, do fluxo das comunicações, que só podem ser quebrados com ordem judicial.

Por que é importante haver esse processo de ordem judicial? Quem são esses intermediários? Qual seria o custo de responsabilizar de maneira excessiva um intermediário? Poderia afetar questões de inovação, por exemplo, em que empresas acabariam não desenvolvendo tecnologias por receio de serem excessivamente responsabilizadas na Internet; poderia afetar a liberdade de expressão e a própria privacidade. Uma das modalidades de responsabilidade, por exemplo, é o que nós chamamos de *notice and takedown*, que seria a notificação da empresa ou da plataforma responsável por um determinado aplicativo, em que ele tem a responsabilidade de remover aquele conteúdo, sem avisar a quem produziu efetivamente aquele conteúdo ou sem provar necessariamente que aquele conteúdo é ofensivo. Isso poderia muitas vezes, violar, por exemplo, a liberdade de expressão.

Um caso comum de que tem se falado muito é o próprio Ministério da Cultura, que postou uma foto, no Dia do Índio, de uma índia com os seios nus, e essa foto acabou sendo removida da rede social. Então, uma foto de celebração da cultura brasileira, da história brasileira, acaba sendo removida, acaba não sendo de conhecimento público, porque é um intermediário, uma empresa privada. Isso é o que nós chamamos de censura privada e acaba retirando o conteúdo sem avisar a

quem postou e sem necessariamente analisar o mérito daquele conteúdo que está ali exposto.

O fundamento dessa necessidade de ordem judicial é a própria inimputabilidade da rede. É um dos princípios do decálogo do conteúdo gestor da Internet. Eu sempre responsabilizo as pontas, ou seja, quem produz conteúdo, quem recebe aquele conteúdo, mas eu deixo a rede intacta. Um dos casos mais famosos e que tem se discutido muito é a própria questão dos direitos autorais, ou seja, conteúdos que infringem direitos autorais.

Na verdade, essa questão no meio digital é muito discutível. Nós discutimos bastante esse tema no Marco Civil da Internet. Às vezes, não é que uma lei não se aplica, mas, na verdade, ela precisa ser reformada e ser adaptada a esse meio. Na nossa própria lei brasileira, estabelecer cessões e limitações para usos não comerciais, e existem, inclusive, relatórios internacionais, um relatório especial das Nações Unidas, que afirma que o acesso à cultura e ao conhecimento é reconhecido como direito humano. Então, como nós pensamos essa questão no meio digital, em que época é mais fácil reproduzir um determinado material? Isso não significa necessariamente não reconhecer os direitos do autor, mas sim equilibrar direitos.

Um caso famoso, por uma questão de considerar o acesso a conteúdos crime, ou seja um cibercrime, foi o próprio caso do governo americano contra Aaron Swartz, um garoto, um estudante, que baixou mais de 4,8 milhões de artigos científicos do MIT e acabou sendo processado por isso, tendo se suicidado. Ou seja, quando o legislador pensa na lei, ele tem de pensar nas consequências dessa lei e como ela vai ser implementada, porque esses abusos podem acontecer tanto do lado do criminoso, mas também de uma lei que é excessiva e estabelece penas excessivas.

Eu queria falar rapidamente do falso *trade-off* entre privacidade e segurança. Geralmente, como eu falei, quando se fala em cibercrime, nós tendemos a disseminar o discurso do medo, o excesso de crimes cometidos na Internet. Mas, na verdade, é comum que algumas leis que tentam combater o cibercrime acabam violando a própria privacidade, que é um direito fundamental e um direito humano. Enfim, acabam colocando esses dois temas em lados opostos, mas, na verdade,

eles são complementares, porque alguém que não tenha a sua privacidade assegurada se sente mais vulnerável, logo se sente mais inseguro.

Existem diferentes formas de se garantir a segurança. O Tor é um exemplo em que se discute muito a questão do cibercrime *versus* a privacidade. Ou seja, enquanto alguns defendem o uso do Tor, o *software* livre, aberto para navegar anonimamente na Internet, para proteger a privacidade ele é importante. Hoje é amplamente comum governos tentarem acessar ou bloquear o Tor para censurar, para violar a liberdade de expressão. Por outro lado, existem aqueles que afirmam que uma série de crimes e de atos ilegais acabam sendo cometidos. Mas, na verdade, acho que a questão que está posta é a seguinte: ou uma determinada infraestrutura irá proteger todo mundo — e aí nós temos que assumir que quem comete crimes é a minoria, não é a maioria —, ou a população fica inteiramente desprotegida e vulnerável. Eu acho que esta questão ainda temos que pensar.

Como eu acabei de falar, em que mundo queremos viver? Em um mundo onde o acesso a dados pessoais é totalmente limitado, onde as pessoas se sentem vulneráveis e quem tem acesso a esses dados tem mais controle, ou em um sistema que é desenhado para se ter o mínimo possível de monitoramento e vigilância, em que se obtém apenas a informação necessária para determinado fim?

Exemplo disso é o atual PL 215, que está sendo discutido hoje na CCJ, e o exemplo de uma má legislação, em que se viola a privacidade, com acesso a dados pessoais sem ordem judicial, em que aumentam a pena de um crime, tornando crime contra a honra um crime hediondo e violando diversos direitos na Internet.

Com isso, eu quero dizer que sem proteção dos dados pessoais não existe segurança, e a Internet acaba sendo um ambiente inseguro para todos.

Recentemente, o Ministério da Justiça promoveu uma consulta pública sobre um anteprojeto de lei de dados pessoais. Ele tem diversos pontos positivos: estabelece princípios da necessidade, proporcionalidade e a questão do consentimento. Ou seja, na medida em que eu entrego os meus dados para determinado *site*, para determinada empresa num aplicativo, eu tenho que ser informada sobre os usos que vão ser feitos daqueles dados e tenho que ter a possibilidade de consentir ou não. E, claro, existem diversas formas de se fazer isso. Existe uma ideia que podemos discutir mais adiante: a granularidade desse

consentimento. Ou seja, para cada uso específico posso autorizar ou não o uso desses dados.

A proteção da privacidade é importante na questão da segurança *on-line*, a exemplo dos mecanismos como criptografia e a própria garantia da anonimização dos dados. Recentemente o Relator Especial das Nações Unidas para Liberdade de Expressão publicou um relatório. Nele recomenda que os Estados devem garantir mecanismos de proteção específicos da privacidade *on-line* de uso de tecnologia de criptografia e que permitam a anonimização dos dados na rede.

Com isso, eu queria afirmar que o anonimato pode, sim, representar a garantia de um direito não só da privacidade, mas da própria liberdade de expressão. Na medida em que eu tenho garantia de que a minha comunicação não vai ser interceptada nem lida, eu consigo me expressar de uma maneira mais livre, claro que com limites.

No último caso, os próprios direitos dos consumidores é um exemplo de como os nossos dados e a ausência da proteção da privacidade dos dados pessoais podem afetar o consumidor e fazer com que ele viva em um ambiente mais inseguro, vulnerável a qualquer crime. Esta é a forma como as empresas intermediárias de dados usam os dados do consumidor sem o seu próprio conhecimento ou, como falei, sem consentimento. E o uso desses dados às vezes pode ser usado para discriminar o consumidor.

Recentemente, foi publicada uma reportagem falando que as farmácias, ao fazerem aquele cartão de usuário, que todo mundo faz porque vai ter desconto, criam uma base de dados, vendem para um intermediário essa base de dados e, por sua vez, esse intermediário vende para os planos de saúde. Então, os planos de saúde acabam tendo acesso aos seus dados de consumo e podem ofertar planos, digamos assim, customizados que podem ser mais caros do que uma pessoa pode pagar, mas, por terem acesso aos seus hábitos de consumo, acabam obrigando as pessoas a pagar um valor mais alto do que o de mercado.

Enfim, para encerrar, quais seriam as recomendações? Seriam sempre transparência nas políticas e principalmente no combate ao cibercrime. Quando o Estado tem acesso aos dados dos cidadãos, qual seria a finalidade, qual seria a

necessidade daquele dado específico — por isso, a ordem judicial também é importante —, a proporcionalidade daquela ação, do acesso a esses dados.

Outra questão também importante, como eu falei, é a capacitação, no caso de se ampliar o conhecimento dos indivíduos sobre formas de se proteger *on-line*, sempre privilegiando a segurança, mas uma segurança que ande lado a lado com a a privacidade, uma segurança da infraestrutura, da rede que está sendo usada.

Em relação à vigilância, deve-se garantir, sim, a privacidade, a liberdade de expressão, com a possibilidade de se usarem tecnologias de criptografia, de anonimização dos dados.

E, por último, a anonimização é importante para se garantirem não só os direitos mencionados, mas também a não discriminação dos consumidores *on-line*.

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

Concedo a palavra aos Deputados inscritos. *(Pausa.)*

Vamos passar aos debates.

Concedo a palavra ao nosso Sub-Relator, Deputado Daniel Coelho.

O SR. DEPUTADO DANIEL COELHO - Sra. Presidente, eu desci aqui porque, pelo adiantado da hora, eu vou ter que me ausentar, mas queria fazer algumas observações.

Primeiro, faço uma pergunta bem objetiva, que acho que tanto Cristiana quanto Patrícia sabem responder: se um *site* coloca no seu endereço um *ponto com ponto br*, obrigatoriamente ele precisa ter um CNPJ brasileiro e um endereço físico no Brasil, ou uma empresa baseada fora pode utilizar esse endereço?

Vocês têm essa resposta? Alguma das duas sabe?

A SRA. CRISTIANA OLIVEIRA GONZALEZ - O *ponto com ponto br* é feito pelo Registro.br, que é de responsabilidade do intergestor da Internet. E, para obtenção do *ponto com ponto br*, assim como do *org ponto br*, é preciso ter CNPJ brasileiro.

O SR. DEPUTADO DANIEL COELHO - Exato. Queria direcionar uma das questões um pouco mais a você, Cristiana, em relação à defesa do consumidor, mas nada impede que Patrícia também faça comentários no momento em que tiver a palavra.

Nós vemos que muitos *sites* têm sua empresa baseada no exterior e utilizam o português como linguagem. Ao acessá-lo, você não tem nenhuma identificação de que está fazendo uma compra no exterior. Então, o consumidor faz uma compra num país da Europa, da África ou de qualquer lugar do mundo sem necessariamente saber disso. O máximo que ele pode fazer é ir buscar lá... Se tiver o *ponto com ponto br*, ele vai ter uma identidade que está no Brasil, mas, se for o *ponto com*, por exemplo, pode estar fora do País, mas com a impressão de que ele está comprando aqui.

No momento em que for lesado, a quem o consumidor vai recorrer? Se a empresa não tiver CNPJ no Brasil, ele vai ter que entrar com processo no exterior contra a empresa que, por exemplo, fez uma cobrança indevida no seu cartão de crédito?

Então, esse padrão da Internet internacional, que é natural da rede, causa ao consumidor muitas preocupações, muitas fraudes ou prejuízos. Se possível, gostaria que vocês fizessem comentários sobre isso.

Eu senti na declaração de Cristiana e de Patrícia uma opinião talvez um pouco divergente — eu queria que isso ficasse um pouco mais claro — em relação à atual legislação nossa. Eu gostaria que vocês comentassem um pouco mais especificamente sobre o Marco Civil da Internet. Onde ele avança? Em que ele pode avançar mais? É realmente uma legislação suficiente para combater os abusos da Internet ou precisamos de novas leis. No caso, Patrícia chegou a colocar em sua apresentação a necessidade de nova legislação. Gostaria de saber se ela tem algo específico para ser trazido agora ao debate ou se posteriormente poderá ser entregue à Presidência da CPI. Gostaria, realmente, de um comentário mais específico sobre a nossa legislação em vigor, o Marco Civil da Internet.

E gostaria apenas de fazer um comentário — não é nenhuma crítica ao que foi colocado por Cristiana — sobre essa situação da chave no carro. Há muitos países em que se deixam as chaves no carro, em que se deixam as portas abertas de casa, e ninguém rouba. É claro que nós devemos nos prevenir, mas o que faz o criminoso também é a oportunidade e a impunidade.

Por que em alguns locais que estão numa situação civilizatória mais avançada do que a nossa as pessoas podem deixar a chave no carro ou a porta

aberta? É porque há certeza absoluta de que, se um crime for cometido, ele será punido. Isso não é um problema brasileiro, é evidente que é um problema hoje global, mas, na Internet, o sentimento de impunidade faz com que nós tenhamos de se preocupar um pouco mais do que em outras situações. Então, é muito importante realmente que haja a prevenção, mas eu acho que nós temos que avançar também na punição.

Nós temos um conflito sempre quanto à liberdade de expressão. Mas, por outro lado, da mesma forma que a nossa Constituição garante a liberdade de expressão, ela também proíbe o anonimato. A Internet e as redes sociais, de uma forma geral, não garantem a identidade de quem ali atua. É muito fácil abrir uma conta em qualquer uma das redes sociais e não há garantia, através de CPF, de identidade ou de nenhum tipo de registro, de que aquela pessoa que está falando, de fato, existe.

Então, eu acho que esse também é um tema que merece um debate, até onde nós devemos avançar numa legislação que proíbe e coíbe esse anonimato, para que, inclusive, a liberdade de expressão seja garantida, mas ela seja garantida com as pessoas assumindo suas opiniões e tudo aquilo que escrevem no meio virtual.

No mais, eu queria agradecer e parabenizar as duas, que foram excelentes debatedoras. Peço até desculpas, porque, realmente, vou ter que me ausentar, mas estou com a equipe de assessoria aqui e tudo está sendo gravado também, para depois analisarmos as respostas.

Obrigado.

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

Nós vamos fazer um bloco de perguntas e depois vocês respondem a todas.

Com a palavra o Deputado Silas Freire.

O SR. DEPUTADO SILAS FREIRE - Presidenta, Deputada Mariana, senhoras convidadas, Patrícia Pinheiro, Cristiana Gonzalez, cada vez que nós escutamos debatedores nesta CPI, nós nos assustamos com a insegurança da grande rede. Eu confesso que não era um profundo conhecedor, estou agora me

aprofundando, mas a cada palestra de pessoas que vivem no trabalho, na grande rede, nós nos assustamos.

Nós temos algumas colocações a fazer até mesmo para a Dra. Patrícia. Nós temos problemas, na realidade, com o uso do *deep web*, que foi citado pela senhora, como também do *dark web*, que são semelhantes, na Internet, sem possibilidade de controle desses dois acessos.

O que as senhoras podem nos dizer sobre as garantias da segurança, por exemplo, dos processos digitais? Os processos judiciais hoje estão todos digitalizados, estão digitais, são digitais. As partes podem ficar tranquilas que não terão ação dos *hackers* nesses processos? É uma pergunta. Como produzir provas do crime cibernético? De onde partiram os perfis falsos? Como nós vamos encontrar esses perfis falsos? É uma outra resposta que eu estou buscando. Todas as agressões sofridas através da Internet podem ter resposta na Justiça? Essa é uma outra interrogação. Quais penas podem ser aplicadas, diante das leis que estão expostas, para agressões expostas na grande rede? Nas suas opiniões, o Governo brasileiro se precipitou ali na aprovação do Marco Civil devido à denúncia de invasão dos dados secretos pelo Governo norte-americano? Nós não poderíamos ter debatido mais o Marco Civil e termos, inclusive, aperfeiçoado mais o Marco Civil? Vocês acham que ele deveria ou não ter sido mais debatido antes dessa aprovação, até pelas evoluções que estão contínuas?

E eu tenho uma última pergunta, que as senhoras poderiam me responder. Nós falamos muito de campanhas educativas. E na hora de se falar de campanhas educativas, nós buscamos um órgão e não temos. Quando se fala em criar agência, órgão neste País, todo mundo chia, porque ele já está muito inchado. Mas seria o caso de nós criarmos uma agência, se não reguladora, mas que pudesse acompanhar a grande rede no território brasileiro, para desenvolver campanhas, para orientar, para defender?

Essas são as minhas perguntas.

Pela fala da Dra. Patrícia, parece-me que nós precisamos legislar mais. Pela fala da Dra. Cristiana, parece-me que nós precisamos aperfeiçoar as leis já legisladas.

Para onde nós vamos? Vamos legislar mais ou aperfeiçoar as leis que temos? Para onde correr? Ou a situação é tal que se correr o bicho pega e se ficar o bicho come?

Muito obrigado.

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

Concedo a palavra ao Sub-Relator Deputado Rodrigo Martins.

O SR. DEPUTADO RODRIGO MARTINS - Eu quero saudar a Presidente Mariana Carvalho e pedir desculpas por ter tido de me ausentar para participar de uma reunião do partido. Mas eu ouvi atentamente a palestra da Dra. Patrícia.

Assim como o Deputado Silas Freire, que falou há pouco, eu fiquei com uma vontade danada de fazer perguntas a respeito de sugestões de alteração da legislação vigente. O que, do ponto de vista prático, V.Sa., que vencia esse tema no seu dia a dia, pode nos sugerir para apertar a legislação vigente e dar uma solução mais prática na hora da investigação?

O Facebook esteve aqui conosco — é a empresa que comprou o WhatsApp — e disse, simplesmente, que hoje é impossível controlar ou dizer que um WhatsApp partiu de determinado ponto de acesso e que é daquela pessoa indeterminada.

Em alguns países, como os Estados Unidos, se não me falha a memória, invadir um sistema ou um computador, seja ou não para buscar alguma informação, para furtar alguma informação ou programa, já é considerado crime. A invasão, por si só, já é crime. Isso também poderia ser colocado?

Também me chamou a atenção a menção à revista digital. Eu acho que é uma das alternativas que nós temos para provar que determinado aparelho telefônico ou computador teve alguma ligação com determinado crime.

Eram essas as minhas perguntas.

Eu peço desculpas à Dra. Cristiana, porque eu tive que me ausentar deste plenário. Vou assistir a sua palestra depois no vídeo e fazer uma avaliação. Como Sub-Relator da área de segurança, sempre me preocupo muito com os resultados práticos desta CPI para que ela possa facilitar a investigação e a punição dos culpados em todos os crimes cibernéticos.

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

Concedo a palavra ao Deputado Rogério Peninha.

O SR. DEPUTADO ROGÉRIO PENINHA MENDONÇA - Eu, na verdade, vou fazer algumas perguntas para a Dra. Patrícia, mas o Deputado Rodrigo Martins já foi mais ou menos dentro dessa linha. Então, vou repetir.

Tenho três perguntas rápidas para a Dra. Patrícia: é possível, com a legislação atual, punir os criminosos que utilizam a Internet? Quais as medidas de aplicação imediata que nós poderíamos tomar para diminuir o número desses crimes? Com a sua vivência no dia a dia como advogada especialista em Direito Digital, quais são as principais reclamações das vítimas quanto à resolução desses crimes e em relação à punição das pessoas que os cometem?

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

Concedo a palavra ao Deputado Rafael Motta, Sub-Relator desta Comissão.

O SR. DEPUTADO RAFAEL MOTTA - Boa tarde a todos.

Rapidamente, eu acho que me dirijo mais à Dra. Patrícia. Não pude acompanhar a sua fala, mas, como Sub-Relator desta Comissão na área do combate à pedofilia, sei que, em 2009, o Senado, com a CPI que tratou da pedofilia naquela Casa, assinou diversos termos de ajuste de conduta com algumas empresas dessa área, por exemplo, a Claro, a NET, a Vivo, a TIM e a Oi. Inclusive, segundo esses termos, a quebra de sigilo telefônico pode ser feita em até 24 horas, se houver risco de violência contra criança ou adolescente, ou em 2 horas, quando houver um risco iminente à vida da vítima.

Eu queria saber se V.Sa. tem acompanhado esses TACs e se há alguma possibilidade de esta Comissão gerar alguma diligência ou algum documento com o qual possamos atualizar os TACs para preservar a vida das nossas crianças e adolescentes.

Era basicamente isso. Peço que V.Sa. fale sobre os TACs para podermos — quem sabe? — atualizá-los nesta Comissão.

Obrigado, Deputada.

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

Aproveito para também pedir desculpas à Dra. Patrícia e à Dra. Cristiana pela ausência. Nós ficamos dependendo dos voos e do clima. Hoje houve atraso do meu voo.

Vou passar a palavra à Dra. Patrícia para as suas respostas e, depois, para a Dra. Cristiana.

A SRA. PATRÍCIA PECK PINHEIRO - Como havíamos acordado, vou aproveitar para, ao responder às perguntas, complementar a explanação. Acho que ficou essa grande questão sobre a legislação. Eu trabalho na área há 17 anos e acompanho a evolução da legislação nos demais países em termos de Direito Comparado nesse mesmo período.

O que se pode dizer é que, ainda no tocante ao aumento da capacidade da prova de autoria, que é determinante na área criminal, nós não alcançamos, não logramos muito êxito na resolução, a não ser quando na atividade criminal há um desfecho até de forma tradicional: aquele crime em que uma parte acontece na Internet e não se tem muita dúvida sobre a autoria.

O Marco Civil da Internet tangencia o assunto. Ele tem um propósito muito pertinente, mas retirou parte da capacidade de reação imediata da autoridade policial e do Ministério Público — não no pedido de preservação de uma prova, mas no acesso a ela enquanto se está procedendo à investigação para um flagrante.

Então, nesse momento, que é importantíssimo para o combate a uma lista — que é a primeira lista dos crimes que mostrei no eslaide —, esse lapso temporal de ir para uma ordem judicial é aplicável, sim, se for uma discussão de censura, mas não é a muitas das práticas em que se precisa daqueles *logs* de conexão ou de aplicação para tentar ir atrás de quem estava abordando uma vítima ou de quem estava ofertando algo ilícito. Então, se há a oferta de algo ilícito, se já está envolvido em uma investigação, como é um conteúdo de pedofilia, essa ação imediata para viabilizar a atuação da autoridade policial e do Ministério Público é essencial.

O que acontece — e isso também tangencia esse assunto — é que há vários elementos que envolvem uma intersecção complexa. Em legislação ou se facilita ou se dificulta a ação imediata da polícia. É bem simples. Refiro-me à investigação. Se

depois a própria parte suspeita prova a sua inocência, se depois há outras oportunidades, ao longo do devido processo legal, aquilo sendo instaurado como ação criminal e tudo, é outro momento.

Estamos falando de alguém postar no Facebook que uma bomba foi colocada em um estádio de futebol e eu poder saber quem é essa pessoa, se ela criou um perfil falso no nome de outrem. Mas eu tenho que agir no momento da declaração, que por si só vai causar medo, terror, e as pessoas vão sair correndo. Isso, em outros países, é ato de terrorismo, não é liberdade de expressão.

Então, é claro que existe a necessidade de um treinamento, a legislação consegue trabalhar limitadores para que não se vá ao abuso de autoridade. Mas eu posso fazer uma revista no carro de alguém, é um procedimento de polícia a revista em veículo. Eu posso fazer a revista numa pessoa suspeita na rua, olhar a bolsa, a mochila. Fazemos revista em aeroporto.

Uma grande parcela das evidências de uma prática de crime cibernético não vai estar num papelzinho no bolso, não vai estar na mala do carro, não vai estar na mochila. Vai estar no celular, vai estar no *tablet*. E é por isso que não estamos inventando a roda, estamos usando as melhores práticas de outros países que tiveram de aumentar o *enforcement* de segurança pública digital.

O Brasil, com toda certeza, tem que atrair pessoas — investidores, turistas — fazendo com que se sintam seguras em nosso País. Isso ajuda no crescimento da nossa economia. A insegurança nunca é positiva nesse sentido. E hoje nós geramos a insegurança da pessoa física. Como? Por exemplo, quando se faz um boletim de ocorrência... Eu acompanhei um caso no Rio de Janeiro.

Melhoramos, sim, com o Estatuto da Criança e do Adolescente, com o crime de pedofilia — arts. 241, 241-A e 241-B. Mas não separamos, na redação, a prática do crime em meio digital, para torná-lo mais grave. Por isso, quando registramos os boletins de ocorrência não temos estatística mais exata do aumento da prática do crime em que se utiliza como *modus operandi* o meio digital.

Quando ocorre furto, registra-se como furto. Registra-se furto mediante fraude quando alguém utilizou um aplicativo falso para pegar dados de uma pessoa, entrar na conta bancária, tirar 4 mil reais, que é a média de valor da operação de transferência possível de ocorrer. Não há tempo hábil para a polícia, quando

avisada, solicitar dados para a caixa postal de *e-mail*, que é do Google, para saber de onde vem a conexão de acesso àquele IP, para me dizer quem foi e eu ir atrás dessa pessoa no rastro do dinheiro, antes de ela o sacar no caixa eletrônico.

Estou só querendo dizer que, com esse procedimento e, por algumas barreiras trazidas, sim, pelo Marco Civil da Internet, afetamos um pouco esse poder de ação imediata investigativa no momento de tentar elucidar uma autoria. Então, se não é uma autoria certa, pode ser apenas um suspeito. Mas hoje acabamos tendo bastante dificuldade nisso.

Vamos pensar, por exemplo, na figura do furto. Como falamos de identidade em meio de Internet, ficaria um pouco diferente da falsa identidade do art. 307 simples. Como eu vou saber se uma pessoa fingiu numa boate ser alguém com 18 anos e tem 16 anos ou se foi alguém que criou um perfil falso para dizer que uma bomba foi colocada em um estádio?

Quer dizer, hoje nós não conseguimos, na hora em que isso esbarra em toda a nossa estatística de polícia, diferenciar esses casos que estão acontecendo com Internet. Nós temos um aumento na explosão de caixas eletrônicos, cuja informação é compartilhada na *deep web* usando o Tor — o Tor é um *engine* cuja primeira tela de acesso se chama *wiki onion*, que é a “Wikipédia” do crime. Na primeira tela já se diz como acessar conteúdo pornográfico, como pegar dados de cartão de crédito de uma pessoa, como comprar entorpecentes. Essa é a primeira tela da *wiki* que aparece depois que se acessa o Tor.

Por mais que possamos dizer que quando alguém inventa um *software* possa ter tido um pensamento inovador, o criminoso também é inovador. É um empreendedor do crime, também é um empresário. E nem por isso deveria deixar de ser preso. Aquele que corrompe também está cometendo um crime. Não é porque ele está trabalhando no lado empresarial que não deve ser preso.

Então, dizer que criar um *software,* por si só, não deveria motivar uma prisão depende de para que foi criada aquela ferramenta. Hoje nós ainda temos bastante dificuldade de pegar aquele que desenvolve ferramentas como essa, depois aproveitadas por criminosos bem menos capacitados do ponto de vista inventivo, mas que depois as aplicam na execução de crimes.

Quanto aos termos de ajuste de conduta, eu posso dizer que seria necessário atualizá-los, sim. Hoje nós teríamos que conseguir enxergar esses novos tipos de ocorrência e quem seriam os detentores das testemunhas-máquinas, com o dever de colaboração ágil, que não são as TELCO. Já estamos num nível de aplicação web. É como uma lojinha de aplicativos do Google ou da Apple, entende? Cabe e eles essa informação, porque o Marco Civil da Internet também proibiu o provedor de conexão de informar aquilo que foi colocado no *log* de aplicação. E que o *log* de aplicação passe o de conexão. São duas informações em separado. Então, hoje, como a autoria começa do fato, e do fato é que desconstruímos para achar quem o praticou, eu preciso alcançar quem é provedor de aplicação nessa celeridade, para eu pegar os bandidos com a mão na máquina, fazer o flagrante, conseguir demonstrar para uma vítima que, sim, conseguimos ir atrás e prender o criminoso. Muitos, no meio do caminho, são apenas — digamos — colaboradores da Justiça para aumentar a segurança digital, o que permite que todo mundo, sentindo que seu filho pode ficar seguro na Internet, o deixaria ficar sozinho brincado.

Hoje eu não sinto nenhuma segurança em deixar meu filho de 8 anos sozinho num computador, num *tablet*, num celular conectado na Internet sem ter todo um olhar, uma vigilância ou até o uso de *software* de controle parental para tentar barrar esse tipo de coisa. Eles estão ali por sua sorte e risco.

Aumentamos a inclusão digital da grande população brasileira. Com o Marco Civil da Internet, o direito a conectar-se à Internet tornou-se um direito essencial de cidadania brasileira. Então, a tendência é incluirmos mais. Quanto maior a inclusão, maior o número de pessoas despreparadas, com menos conhecimento, com menos campanhas educativas, tende a aumentar a incidência desses crimes.

Existe um princípio técnico chamado ordem de volatilidade que determina a perda rápida de uma prova eletrônica. E isso é importantíssimo, porque não pode ser utilizado apenas para conseguir o *periculum in mora* de uma ordem judicial. Isso tem que viabilizar a revista digital. Isso tem que viabilizar a ação imediata. Temos até a previsão da legítima defesa. Hoje podemos dizer que estão mais de mãos atadas a polícia, o Ministério Público no combate ao crime do que o indivíduo se ele alegar o dispositivo do Código Penal que trata da legítima defesa. E aí estamos hoje estimulando esse cidadão, como o IDEC defende o interesse dos consumidores,

esse consumidor de Internet, de meios digitais, a fazer justiça com o próprio *mouse*, a se defender sozinho, como disse a Cristiana: *"Feche a sua porta, defenda-se sozinho".* Nós não podemos contrapor direitos humanos com segurança, mas segurança e combate a crime é interesse coletivo. E, dentro da lei, a forma de execução deve permitir que a autoridade aja mesmo quando há restrição de liberdade individual. Senão não haveria o crime de dano, eu poderia destruir uma coisa de outro. Se fôssemos só considerar a liberdade individual, não haveria nenhum dos outros crimes previstos no Código Penal. Fico com raiva de você, mato você, xingo você. Não haveria os crimes contra a honra. Na verdade, é o contrário: nós cerceamos toda a liberdade individual com todos os demais artigos que dizem até onde a liberdade individual pode ir, e até no Código Civil, se não aplica o abuso de direito.

Então, eu ia comentar esses pontos. Nossa legislação está iniciada, acompanha tendências internacionais, mas é incompleta, em alguns momentos, por ter sido feita não com o olhar de integração das leis. Em dados momentos, algo previsto em uma está impedindo a outra de alcançar o seu resultado.

Então, na parte específica desta Comissão, desta CPI de crimes cibernéticos, se nós começarmos a falar sobre o Marco Civil, o que ficou previsto no Marco Civil, hoje, trouxe uma camisa de força e amarrou mais a ação imediata de combate a crime. Não aquilo que eu possa levar numa ordem judicial. Alguém me ofendeu, vou querer investigar quem foi. Hoje o *modus operandi* está mais até no juízo cível, porque eu vou pedir uma ação declaratória de obrigação de fazer, para que aquele provedor me diga o número do IP, dos *logs* que acessaram aquela página e publicaram aquele texto. Eu já sei quem é e posso, diretamente, fazer um BO.

Sem ferramenta, sem preparo da autoridade policial fica mais difícil. Mas se para tudo nós precisarmos da ordem judicial, perderemos o flagrante, perderemos a ação imediata. E isso, em combate a crime ostensivo, menos de 5% de toda uma população é de criminosos qualificados, profissionais, que não são os criminosos eventuais, que por oportunidade cometem crimes: *"Vou levar alguma coisa, vou ganhar algum"*. Não, estou falando daquele que realmente pensa em montar uma quadrilha, em gerar uma prática de crime.

Mas essa pessoa, hoje, está nadando de braçada na Internet brasileira, não tem o menor sentimento de que vai ser alcançada. Há, sim, um grande sentimento de impunidade. Acabamos favorecendo o anonimato pelo próprio Marco Civil da Internet.

Então, assim, eu volto: sim, nós deveríamos pensar a legislação atualizando aquilo que faltou. Nós não catalogamos o estelionato digital. Hoje a coisa, mediante esses ataques — como são os aplicativos falsos, que eu mostrei aqui para vocês —, cresceu muito. Em média, ele tira pelo menos 4 mil reais de uma pessoa, se não tirar um conteúdo de voz, de dados e de imagem.

A vítima brasileira não vai para a delegacia. Não temos delegacias suficientemente especializadas para atender a essas pessoas. Falta, então, essa competência, essa capacitação, não só de delegacia, mas de vara especializada. Então, isso se perde na hora em que vira ação criminal ou outro tipo de ação, civil ou mesmo na vara da infância. Não temos especialização ali, tínhamos poucas delegacias especializadas, a previsão era de uma por Estado, mas isso não alcança o Brasil. Então, a força de tratamento de especializada é pequena.

E a primeira pergunta de todas — ele já se ausentou, eu acho que era o Deputado Daniel Coelho —, só para não deixar de atendê-lo, algumas questões que ele fez sobre comércio eletrônico, nós tivemos o decreto do comércio eletrônico, até complementando ali, estava no meu eslaide, uma parte da legislação que também alcança. Então, ali já teria resposta para o que ele questionou sobre ter que ter dados declarados de endereço e contato naquele que oferta e vende produto ou serviço para o brasileiro. Nosso problema, ali, está em quê? Em fazer a lei ser cumprida. E aí, sim, é multa, é vigilância, é cassação de *site*, tirar do ar, como aconteceu recentemente com os dados do *site* Tudo sobre Todos, entre outros, que nós colocamos ali também.

Então, temos a legislação e a prevenção. Prevenção é campanha educativa. Sim, seria importante reunir isso com aquele que já possa trabalhar a campanha educativa. Quanto a isso, tivemos um bom mérito no Marco Civil da Internet, na época, conversando com o Deputado, falamos muito, e ali, do art. 20 ao 24 do Marco Civil da Internet há toda uma previsão de campanhas públicas educativas para que a população saiba se proteger. Mas tem que ter o canal de denúncia. Não

pode ser só uma denúncia de *spam*, como acontece hoje, ou uma denúncia lá para o Cert.Br ou alguém. Teria que ser uma denúncia já voltada para o *hotline* de polícia mesmo. Temos o desafio internacional, então, em muitos casos, acaba sendo competência da Polícia Federal. Solucionar aquela questão de integração, de ação, quando é Polícia Civil, Militar, Federal, isso é algo que às vezes gera inação, por não se saber quem teria que agir; nem o cidadão sabe para quem ele vai se reportar.

E, logicamente, quanto aos processos digitais, colocados aqui pelo Deputado Silas Freire — não é, Deputado? —, claramente não existe nenhum ambiente seguro, mesmo num tribunal físico alguém pode entrar lá e sumir com um processo ou algo acontecer. Então, acho que tem que ter muitas medidas para trabalhar segurança. A autenticação forte é uma e o uso da criptografia, citado pela Cristiana, é outro, e também depende muito de cultura, de educação. Nós não temos o hábito de uso de algumas dessas ferramentas no País. Mas evitar um ataque, que se invada um servidor de um tribunal e tire dados, ou apague, ou altere coisas é possível, sim. É muito provável. Pode ocorrer muito. Porque o que impediria seria o policiamento ostensivo, fazer mais revista digital, ter ação imediata de polícia, poder pegar em flagrante, pegar com aquilo ainda acontecendo e, aí sim, punir quem praticou o crime.

Se não fazemos esse ciclo, realmente não conseguimos nem deixar o bandido preocupado. Hoje, a maioria dos que tomam ou utilizam o crime digital como *modus operandi*... Temos estatísticas baixas sobre isso por conta do problema da tipificação. Como não colocamos em artigos mais específicos ou em letras, alíneas, incisos mais específicos, quando a ocorrência é digital não conseguimos separar na triagem das estatísticas de polícia para conseguir, inclusive, dedicar, alocar verba para equipamento, para ter uma equipe especializada, para fazer uma vara especializada, tudo isso. E no crime, não adianta, *in dubio pro reo. S*e não temos prova de autoria e não conseguimos um flagrante, em muitas dessas ocorrências não há crime.

Então, a sensação de crime, a sensação de insegurança é do cidadão, porque, juridicamente, quando vamos para o devido processo legal, na grande maioria dos casos não conseguimos a punição, por conta disso. Talvez, se houvesse mais *enforcement* para uma identidade digital obrigatória, para a

apresentação dessas provas de forma imediata por ambientes de aplicação *web*... Isso gera custo, não é? Então poderíamos até dizer que temos mais bandidos, mais criminosos digitais presos. Hoje ainda acaba preso aquele que sai correndo pela rua. Esse nós estamos vendo, nesse caso já sabemos como fazer. Quanto ao resto, acho que o propósito da Comissão é justamente o de aprendermos juntos e implementarmos um plano de ação nesse sentido. E, sim, pelo menos um terço ainda depende de uma melhoria na legislação para pelo menos restabelecermos a autoridade policial.

Nos Estados Unidos a preservação e apresentação de evidências em crimes flagrantes, no caso de crimes considerados mais graves — por isso temos que aumentar a gravidade de alguns crimes no Código Penal — ocorrem por ordem de autoridade policial, não por ordem judicial. Aqui tudo virou ordem judicial, o Judiciário também está cheio de trabalho, e com isso se perde o momento do flagrante. Uma hora, duas horas já é tempo suficiente na ordem de volatilidade para eu não conseguir mais pegar o autor.

Então, claramente, precisamos fazer uma nova análise, revisitar esse assunto, agora com o foco em crime, independentemente do que está no Marco Civil da Internet.

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

Eu tenho certeza de que, além deste momento, hoje, desta audiência, podemos contar com sua contribuição para nos ajudar com sugestões. Não sei se já foi pedido pela Comissão, também, mas se possível, mandar toda a apresentação para disponibilizar a todos os membros desta Comissão.

A SRA. PATRÍCIA PECK PINHEIRO - Certo.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Concedo a palavra à Dra. Cristiana Oliveira Gonzalez.

A SRA. CRISTIANA OLIVEIRA GONZALEZ - Bom, eu vou responder rapidamente, porque eu tenho que ir embora daqui a pouco.

Sobre a questão feita sobre os *sites* internacionais, o Marco Civil da Internet já prevê que quando um serviço é prestado no território nacional, ou é acessado por um cidadão brasileiro, ou o servidor, a empresa está localizada no Brasil, ela deve

responder, deve prover acesso aos dados. Eu acho que o Marco Civil da Internet já dá conta desse problema.

Inclusive quando é necessário ter acesso a dados que estão no exterior, há não só o Marco Civil, mas também acordos entre as autoridades de diferentes países, um acordo chamado MLAT, um processo que pode ser feito da maneira judicial e oficial, enfim. Ou seja, existem soluções para essas questões.

Onde o Marco Civil avança? Bom, como eu disse, eu acho que deixei bem claro, e aí, talvez, nesse ponto, eu discorde da Dra. Patrícia que precisamos tratar de crimes. Na verdade, o Marco Civil é importante porque garante direitos. E quais são esses direitos? Direito à privacidade, direito à liberdade de expressão. Ele garante a regra da neutralidade de rede, e ele garante a Internet como um serviço essencial.

Então, nesse sentido, o Marco Civil avança. Claro que ele tem defeitos, mas eu acho que os defeitos que eu vejo no Marco Civil são diferentes de quem busca aumentar a criminalização dos internautas na Internet, ou seja, o IDEC faz parte de um movimento de um conjunto de organizações chamado Marco Civil Já, e a gente é da opinião comum de que, por exemplo, a guarda do registro dos *logs* deveria ser menor, dentro do princípio da presunção de inocência. Não posso guardar os dados de um cidadão durante mais de 6 meses, 1 ano. É muito tempo. Sendo que esse cidadão, muitas vezes, é inocente. Então, como eu disse, criminoso é minoria, não é maioria.

Sobre a questão da situação civilizatória, o Brasil é um país em desenvolvimento, nós temos diversos problemas de ordem econômica, social, e a questão do crime não é desconectada dessa questão.

Então, temos que nos colocar nesse contexto. Não dá para comparar com outros países onde existe outro nível de desenvolvimento e achar que aqui temos que aplicar soluções mais rigorosas, que isso vai resolver o problema do crime. É claro que essa é uma discussão mais longa e acho que ela tem que ser mais aprofundada.

Se precisamos debater mais o Marco Civil? Eu acho que não. Ele está sendo regulamentado na questão da neutralidade de rede e na questão da privacidade da guarda de *logs.* O Marco Civil da Internet foi fruto de um amplo debate social, uma

das leis mais democráticas aprovadas nesta Casa nos últimos tempos, ou seja, foram feitas inúmeras consultas públicas, receberam inúmeras contribuições, é um processo longo de discussão e de negociação política.

Enfim, pedir mais discussão, então, seria em que termos? Vamos abrir uma nova consulta pública sobre cada projeto de lei que vai alterar o Marco Civil? Seria o ideal, porque respeitaria, pelo menos, o processo em que essa lei foi elaborada.

Mas é claro que precisamos aperfeiçoar as leis. Eu concordo que existem algumas questões ainda a serem definidas. Eu só queria corrigir aqui: eu não afirmei que é responsabilidade única do indivíduo, do consumidor se proteger, é uma das vias possíveis usar os instrumentos disponíveis para a sua proteção, mas também carecemos de uma lei de proteção de dados pessoais. Uma lei de proteção de dados pessoais que inclua consentimento, que inclua a devida proteção da privacidade, que inclua possibilidade de uso de tecnologia de anonimização.

Enfim, eu acho que este é um dos maiores defeitos da nossa legislação: não ter uma lei adequada de proteção de dados pessoais.

Se formos pensar em alguns crimes, por exemplo, o da fraude, o que é uma fraude? É um mau uso dos dados. Na medida em que os meus dados estão protegidos, eu corro menos risco e me sinto menos vulnerável e menos inseguro na Internet.

Eu quero comentar rapidamente a questão da separação dos *logs* de aplicação, dos *logs* de conexão.

Por que ela é importante? Em primeiro lugar, o Marco Civil não trata de perseguição criminal, trata da defesa de direitos. Por que é importante? Porque ele garante a neutralidade de rede.

Hoje a convergência das mídias tem feito com que muitas operadoras, além de operar a rede, ofereçam serviço de conexão e, recentemente, conteúdo.

Na medida em que uma única empresa tem acesso a todos esses dados, é grande o poder que ela tem em mãos. Esse dispositivo do Marco Civil que separa a guarda desses dois dados é justamente para proteger o consumidor do monopólio de uma empresa sobre os seus dados.

Sobre a questão da ordem judicial e a questão de que é preciso acelerar os processos, existe algo que é muito importante pensarmos, principalmente nesse tema dos crimes de honra, que tanto temos discutido aqui no Congresso.

Exatamente, vamos gerar um processo de acusações sem provas, que pode colocar em risco não só a liberdade de expressão, como eu disse, mas o próprio cidadão.

Vamos supor que alguém resolva criticar um dos Srs. Deputados na Internet. Essa pessoa será perseguida, independentemente de o PL 215 ter sido aprovado. Não sei como foi a discussão agora na CCJ, mas ela pode passar até 6 anos na cadeia. E isso sem prova e sem ordem judicial.

Como vamos jogar nas mãos de um ente privado um julgamento sobre um fato que pode ser verídico ou não? Por isso a ordem judicial é importante, porque ela garante o processo adequado em todos os casos.

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

Quero mais uma vez agradecer por vocês terem aceitado o convite para comparecer a esta Comissão para ajudar nos trabalhos desta CPI.

Antes de encerrar os trabalhos, gostaria de informar a todos que esta CPI, no dia 5 de outubro, vai se deslocar para a cidade de Natal, Rio Grande do Norte, para realizar uma audiência pública com a participação das autoridades de segurança locais, para saber como está o enfrentamento do uso da Internet na exploração sexual de crianças e adolescentes naquela cidade.

A audiência é uma iniciativa do Deputado Rafael Motta, responsável na CPI pela Sub-Relatoria dos Direitos das Crianças e dos Adolescentes.

Também gostaria de comunicar que a Comunidade da CPI na Internet está disponível. É preciso acessar a página *camara.leg.br* e entrar no e-Democracia.

Os Deputados que tiverem interesse em participar desta CPI em Natal, por favor, queiram comunicar à nossa Secretaria, que vai organizar a ida de todos.

Nada mais havendo a tratar, vou encerrar a presente reunião, antes convocando reunião ordinária da Comissão para a próxima quinta-feira, dia 24 de setembro, quando ouviremos a FEBRABAN, a DATAPREV, a Secretaria de Informação e Logística do Ministério do Planejamento e a Receita Federal, conforme

pauta que será publicada na página da Comissão e encaminhada aos *e-mails* institucionais dos gabinetes e Lideranças.

Obrigada a todos pela presença.

Está encerrada a reunião.