DEPARTAMENTO DE TAQUIGRAFIA, REVISÃO E REDAÇÃO

NÚCLEO DE REDAÇÃO FINAL EM COMISSÕES

TEXTO COM REDAÇÃO FINAL

Versão para registro histórico

Não passível de alteração

CPI - CRIMES CIBERNÉTICOS			
EVENTO: Audiência Pública.	**REUNIÃO Nº: 1453/15**	**DATA: 20/08/2015**	
LOCAL: Plenário 8 das Comissões	**INÍCIO: 10h19min**	**TÉRMINO: 14h28min**	**PÁGINAS: 86**

DEPOENTE/CONVIDADO - QUALIFICAÇÃO

STÊNIO SANTOS - Delegado de Polícia Federal, Chefe do Grupo de Repressão a Crimes Cibernéticos.
ELMER COELHO VICENTE - Delegado de Polícia Federal, Chefe do Grupo de Repressão a Crimes Cibernéticos.
CARLOS EDUARDO MIGUEL SOBRAL - Assessor da Coordenação-Geral de Projetos de Tecnologia da Informação da Secretaria Extraordinária de Segurança em Grandes Eventos do Ministério da Justiça.

SUMÁRIO

OBSERVAÇÕES

Houve intervenções fora do microfone. Inaudíveis.
Houve intervenções fora do microfone ininteligíveis.
Há orador não identificado em breve intervenção.
Há palavra ininteligível.
A reunião foi suspensa e reaberta.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Bom dia.

Havendo número regimental, declaro aberta a 5ª Reunião Ordinária da Comissão Parlamentar de Inquérito que investiga a prática de crimes cibernéticos.

A Ordem do Dia de hoje prevê a realização de audiência pública e, em seguida, a deliberação de requerimentos.

Dando início à audiência pública, gostaria, em primeiro lugar, de agradecer ao Diretor-Geral do Departamento de Polícia Federal, Leandro Daiello Coimbra, pela colaboração que prestou para a realização desta audiência. Agradeço também aos convidados, que prontamente atenderam à solicitação da CPI.

Desde já, chamo os convidados para comporem a Mesa.

Convido o Sr. Stênio Santos, Delegado da Polícia Federal, Chefe do Grupo de Repressão a Crimes Cibernéticos da Superintendência do Distrito Federal; o Sr. Elmer Coelho Vicente, Delegado de Polícia Federal, Chefe do Serviço de Repressão a Crimes Cibernéticos; e o Sr. Carlos Eduardo Miguel Sobral, Assessor da Coordenação-Geral de Projetos de Tecnologia da Informação da Secretaria Extraordinária de Segurança em Grandes Eventos, do Ministério da Justiça.

Informo que esta audiência cumpre decisão deste colegiado, em atendimento aos Requerimentos nºs 6, 20, 23 e 27, de 2015, respectivamente de minha autoria, de autoria do Deputado Alexandre Leite e das Deputadas Ana Perugini e Alice Portugal.

Solicito a compreensão de todos em relação ao tempo destinado à exposição dos convidados e aos debates. Cada convidado disporá de 15 minutos para proferir a sua fala, não podendo haver apartes.

O SR. DEPUTADO LEO DE BRITO - Sra. Presidente, V.Exa. se esqueceu de me citar como autor do requerimento.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - E também em atendimento ao requerimento do Deputado Leo de Brito.

O SR. DEPUTADO LEO DE BRITO - Do Stênio e do Elmer.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Os Deputados interessados em interpelar os convidados deverão se inscrever previamente e poderão usar da palavra por 3 minutos ao final das exposições, podendo haver réplica e tréplica.

Feitos esses esclarecimentos, vamos dar início à audiência.

Concedo a palavra ao Sr. Stênio Santos, Chefe do Grupo de Repressão a Crimes Cibernéticos da Polícia Federal. V.Sa. dispõe de 15 minutos.

O SR. STÊNIO SANTOS - Bom dia, senhores.

Agradeço, inicialmente, o convite. A Polícia Federal está sempre à disposição para colaborar com esta Casa, com quem tem uma parceria muito forte, desde ações legislativas, proposições.

O que a gente quer, efetivamente, é poder concretizar os dispositivos constitucionais, em especial nossa função de realizar segurança pública da melhor maneira possível. Em razão dessa atribuição, somos muitas vezes demandados a atuar numa esfera de atribuições bastante ampla. No caso dos crimes cibernéticos, essa é apenas uma gama das atribuições que a Polícia Federal possui.

A Operação IB2K, motivo pelo qual nos foi feito o convite para comparecer aqui, origina-se de um projeto de cooperação com a Caixa Econômica Federal, que se iniciou em 2009, chamado Projeto Tentáculos. Então, a partir do Projeto Tentáculos, foi feita uma aglomeração, uma centralização das denúncias de crimes cibernéticos, numa base única, à qual a Polícia Federal tem acesso e, portanto, consegue fazer análises qualificadas.

A partir de análise qualificada, definiu-se um período de pesquisa, de novembro de 2012 a julho de 2013, para se averiguar uma organização criminosa que estava fazendo diversas fraudes, utilizando o Internet *Banking* da Caixa Econômica Federal. Então, a partir dessa análise, identificou-se uma fraude que superava 2 milhões de reais, em 583 processos de contestação. A análise se inicia a partir de dois terminais, que foram identificados como sendo desses suspeitos.

Em relação ao Projeto Tentáculos, só para poder contextualizar, ele muda um paradigma. A gente trabalhava com uma investigação tradicional, que não considerava o aspecto da Internet, em que cada processo de constestação da Caixa Econômica Federal gerava a necessidade de instauração de um inquérito policial.

Então, essas comunicações, em razão da característica da Internet, ficavam dispersas pelo País. Em tese, qualquer pessoa, tendo conhecimento de uma fraude na Internet, pode comunicar a qualquer órgão, porque, a princípio, não se sabe onde ocorreu o local do crime cibernético. Então, isso gerava informações limitadas. Cada

unidade da Polícia Federal tinha uma informação parcial da fraude. Isso impedia que a Polícia Federal tivesse conhecimento de quem era a organização criminosa. Então, eram feitas as instaurações, a partir do local da conta da vítima, e não onde estava o criminoso, o suspeito. Geravam-se as quebras de sigilos bancários, telemáticos, mas, no final, poucas investigações chegavam, efetivamente, à quadrilha. Às vezes, chegava-se a um laranja, mas não se chegava à organização criminosa.

Com essa cooperação técnica e com a centralização das notícias, as agências da Caixa Econômica Federal passaram a encaminhar diretamente à nossa unidade central, que passa a ter uma noção geral de todas as fraudes ocorridas no Brasil e, atualmente, até no exterior.

É feito então esse cruzamento prévio de informações e aí, ao invés de focar numa fraude pequena, a Polícia Federal tem a possibilidade de atuar na criminalidade organizada. Então, a gente vê qual é a fraude realmente grave e aí se utiliza os recursos, que não são ilimitados, para atuar onde é efetivamente necessário. Isso daí faz concretizar, na minha visão, o princípio da eficiência, que está no art. 37 da Constituição Federal. Além disso, permite que nós façamos estudos prospectivos de criminalidade.

Então, identificar que, em determinado local, possui a incidência de um crime maior nos faz atuar para fazer cessar ou reduzir aquela criminaldade, ao invés de investigá-la de forma dispersa. No caso específico da Operação IB2K, o ponto de partida foram dois terminais de Internet pertencentes a Barbosa e Pereira, que fizeram acesso indevido ao sistema de Internet *Banking* da Caixa Econômica Federal.

Aqui no painel é possível averiguar a utilização do sistema da Polícia Federal. Fizemos algumas censuras, mas ali foi identificada, inicialmente, a transferência para 243 contas, os pagamentos de 21 títulos bancários e a recarga de 7 telefones, só que a análise permite que sejam ampliadas. Então, cada fraude que está vinculada com outra vai gerando um aumento dessa pesquisa.

Além disso, as informações que vão chegando à base podem ser confirmadas na rua. Então, a gente não fica simplesmente fazendo pesquisa no computador. As

informações que chegam são confirmadas na rua. Então, a partir dessas pesquisas, dessa análise preliminar, foram sendo ampliadas essas informações.

Estou falando rapidamente porque o tempo de 15 minutos não é suficiente para apresentar tudo. Aqui a gente vai vendo a análise feita na base de fraudes.

A partir dessa análise...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Dr. Stênio, o que o senhor tiver de importante... É importante até porque o requerimento para esta CPI é em relação a esse tema.

Então, o senhor não precisa pular. Acho que todos concordam. A gente está aqui à disposição para poder ouvir.

O SR. DEPUTADO ESPERIDIÃO AMIN - Poderia voltar dois eslaides? Explica para nós isso aí.

O SR. STÊNIO SANTOS - Aqui neste gráfico nós temos os dois terminais: o terminal de Ferreira e o terminal de Barbosa. Vinculados a eles, um telefone, cada um com um telefone, e um terminal de conexão. Então, eles utilizaram uma conexão com a Internet e, a partir dessa conexão com a Internet, invadiram diversas contas.

Então, no caso de Ferreira, nós temos 35 contas que foram vitimadas. Ele está aqui atrás do computador, invadiu o sistema da Internet Banking e acessou essas contas. A partir do momento em que ele acessa essas contas, ele consegue agir como se fosse o cliente da instituição bancária. Então, ele pode fazer transferência desse dinheiro, pode fazer uma recarga de celular, pode fazer pagamento de boletos bancários. Isso é feito de forma relativamente fácil, como se fosse o próprio cliente realizando essas transações, e aí os critérios de limitação são os que as instituições bancárias estabelecerem. Às vezes tem um critério de até mil reais por dia e às vezes, dependendo da situação, ele não tem limite. Então, isso vai facilitando para o criminoso, para o suspeito, obter esses recursos.

Então, a partir dessas 123 novas vítimas, a Polícia Federal continua fazendo a ampliação dessas informações que foram inseridas na base. Então, descobrem-se novas vítimas, novos endereços IPs, novos telefones, novos boletos bancários e assim sucessivamente.

É a partir dessas ampliações que vão surgindo novas pessoas envolvidas: laranjas que aparecem lá recebendo dinheiro, o telefone foi recarregado. Tudo isso

vai gerando, então, novas pesquisas. A polícia vai à base e depois confirma na rua se aquilo realmente aconteceu.

Então, no caso do pagamento de títulos... Aqui a gente está só mostrando mais claramente aquela mesma tela do Ferreira e do Barbosa.

Acho que já passou. Volta um pouquinho.

O SR. DEPUTADO ESPERIDIÃO AMIN - Volta, porque há novos personagens.

O SR. STÊNIO SANTOS - Aqui a gente está só mostrando mais claramente aquela mesma tela do Ferreira e do Barbosa.

(Intervenção fora do microfone. Inaudível.)

O SR. STÊNIO SANTOS - À medida que a gente vai ampliando, vão surgindo outros nomes.

A partir daqui a gente só está demonstrando graficamente as ampliações que vão gerando novos terminais. Então, a partir desses dois terminais...

(Intervenção fora do microfone. Inaudível.)

O SR. STÊNIO SANTOS - Então, a partir desses dois terminais iniciais, encontram-se sete novos terminais que também estavam realizando o mesmo tipo de conduta típica, totalizando nove terminais de conexão.

O SR. DEPUTADO ESPERIDIÃO AMIN - Com outra conexão?

O SR. STÊNIO SANTOS - Com outras pessoas. No caso, outros terminais, só que muitas vezes um terminal acaba invadindo, interligado com o outro. Então, ele é incluído...

(Intervenção fora do microfone. Inaudível.)

O SR. STÊNIO SANTOS - Facilitou a descoberta. Exatamente. Então, a gente vê a conexão de um terminal com outro a partir de uma invasão de uma conta, a partir da recarga de um mesmo celular e aí se entende que ele são conexos em algum momento.

(Intervenção fora do microfone. Inaudível.)

O SR. STÊNIO SANTOS - Exatamente. Então, a rede vai aparecendo a partir disso.

Então, aqui a gente vê os vários terminais de conexão vinculados, no caso, a Barbosa e a Ferreira. Duzentos e cinquenta e sete endereços IPs foram identificados aqui.

Então, a partir dali foram descobertos 32 telefones que tinham recebido recargas fraudulentas provenientes de 53 contas vítimas. Nessa modalidade recarga de telefone foram fraudados 2.704 reais dessas 53 vítimas. E aí alguns telefones que se destacavam. Então, à medida que se destaca, a Polícia Federal dá uma verificada mais pormenorizada em relação àqueles terminais, porque, provavelmente, eles têm uma proximidade maior com quem é responsável pela fraude.

No caso de pagamentos de títulos, os endereços IPs utilizados por esses nove terminais acabaram identificando 62 títulos bancários cujos pagamentos foram efetuados em desfavor dessas 53 contas vítimas. Só em relação a título, naquele período, identificaram-se 89.741 reais e 71 centavos, num total de 84 transações fraudulentas. No caso de contas que foram beneficiadas, identificaram-se 367 que receberam transferências dessa origem fraudulenta.

Então, o cliente, na medida em que ele é vítima da fraude, comunica à Caixa: *"Fui vítima da fraude".* Realiza-se um processo de contestação. Geralmente se faz um registro de ocorrência na Polícia Civil e toda essa informação vai para essa base que permite identificar quem foi vítima, onde está o endereço e quem foi o beneficiário. No caso dessas transferências, detectaram-se, nesse período, mais de 2 milhões de reais transferidos fraudulentamente.

(Intervenção fora do microfone. Inaudível.)

O SR. STÊNIO SANTOS - Tem valores pequenos e tem valores um pouco mais amplos também.

(Intervenção fora do microfone. Inaudível.)

O SR. STÊNIO SANTOS - Mas são valores pequenos, só que somados eles terminam chegando a esse número bastante elevado. Alguns são bem pequenos, outros são um pouco maiores.

No caso, então, de contas beneficiárias, foram encontradas 367. Foi realizado um mapeamento dos endereços e se obteve 348 endereços disponíveis na base, excetuando 19 que estavam em outras instituições financeiras. Então, a grande

maioria dessas fraudes estava vinculada com a Caixa Econômica Federal, até porque o convênio, a princípio, é com a Caixa Econômica Federal. Se nós já tivéssemos o convênio amplamente realizado com as outras instituições, provavelmente esses valores seriam bem maiores.

Em relação a contas beneficiárias, no DF, identificaram 222, em Goiás, 114, mas também tiveram em outros Estados, não se limitou à região do DF.

Então, 114 endereços em Goiás e 222 no DF. A maioria das contas beneficiárias das fraudes pertencia a agências que estavam aqui no DF, num total de 276, seguido de Goiás, com 63, e nove pertencentes a outros Estados, no caso Minas Gerais, Pará, Rio de Janeiro e Piauí.

Então, o valor parcial da fraude, somando contas fraudadas, pagamento de boletos e recarga de telefone, chegou a mais de 2 milhões de reais entre novembro de 2012 e julho de 2013.

A conclusão da análise é a seguinte: por que a Internet Banking? Porque essa modalidade de crime permite que as fraudes se espalhem no País inteiro. Ela não fica localizada num local. Por quê? O sujeito está atrás de um computador, com facilidade pode acessar qualquer conta do País, e as vítimas estão espalhadas no País inteiro. Mas, no caso específico dessa organização criminosa, a maior parte das contas beneficiárias dos créditos estava no Distrito Federal, seguido de Goiás.

Os terminais de conexão fixos também estavam localizados no DF. A maior parte dos terminais de conexão móveis estava vinculada à empresa Claro e possuíam DDD do DF. Ou seja, não necessariamente estavam no Distrito Federal, porque há a região do Entorno, que também tem o DDD 61. Também detectamos em São Paulo.

Então, 28 telefones celulares que receberam recarga pertencem ao DF, com exceção de dois que estavam em Goiás, um em São Paulo e um no Pará.

Em relação à metodologia criminosa, está aqui só o desdobramento: a partir dessa análise, naturalmente é instaurado o inquérito policial, que, nesse caso, foi o 1.262/2013, e a polícia consegue, a partir da instauração desse inquérito policial, realizar medidas um pouco mais graves, para se poder alcançar a materialidade delitiva e a autoria, no caso, interceptações telefônicas e telemáticas e prorrogações,

visando a chegar ao cume da organização criminosa e não ficar simplesmente no laranja.

Isso é um processo dinâmico. Cada vez que novas informações vão chegando, a base continua recebendo informações em tempo real. Então, a quadrilha está realizando as fraudes, e a polícia está realizando a interceptação, as informações continuam alimentando a base de fraudes. Isso é um processo dinâmico de pesquisa na Internet, pesquisa na base e pesquisa de rua, pesquisa de campo, para se poder mapear toda a quadrilha.

E qual é a metodologia criminosa, senhores? Para o criminoso poder chegar e ter acesso, invadir a conta do cliente da instituição bancária, em regra, em geral, ele utiliza a metodologia de enviar *spam*. Ou seja, ele encaminha diversos *e-mails*, ele coleta *e-mails* de pessoas que, às vezes, deixam... Por exemplo, mandam uma mensagem para diversos contatos e, em vez de colocarem no oculto, colocam para todo o mundo ver quais são aquelas mensagens.

Então, muitas vezes essas mensagens trocadas são disponibilizadas em fóruns, em locais abertos, vem um robozinho vem e coleta esses *e-mails*. Essa coleta de *e-mails* vai subsidiar essa base do suspeito, do criminoso, para poder mandar os *spams.* Então, ele não descobre do nada, é porque houve uma falha na cautela do próprio internauta — isso é um exemplo — de enviar mensagens para outras pessoas. Então, é importante tomar alguns cuidados para se prevenir, e esse é um deles.

Então, o *hacker* vai e encaminha diversas mensagens. A nossa experiência tem demonstrado que aproximadamente 20% das pessoas que recebem terminam caindo no golpe. Então, muitos recebem esse *e-mail*, não conhecem o destinatário e apagam, não vão nem saber o que é. Outros vão lá, abrem o *e-mail*, veem aquela mensagem e aí são enganados e, ao serem enganados, às vezes, eles clicam no *link,* e o vírus infecta a máquina dele.

Então, ao ser a máquina infectada, o criminoso passa a ter o controle do computador do cliente. Então ele pode, às vezes, obter os dados do cliente, tanto do banco como outras informações pessoais, pode obter fotos, por exemplo, que o cliente tenha no computador, documentos, etc. Ele passa a ter acesso ao computador e, com isso, ele consegue realizar a fraude.

Muitos dos ataques de negação de serviços que nós vimos principalmente durante os grandes eventos também se basearam nessa metodologia. O sujeito passa a controlar o computador, o que a gente chama de "redes zumbis", as *botnets*, e ali ele consegue derrubar um *site* do Governo, consegue criar uma conta no Facebook, por exemplo, no Google, no Twitter, etc. Ele pode fazer tudo o que a vítima faria com o computador, só que dá a impressão de que é a vítima. Então, o perigo, o problema está exatamente na cautela inicial que se deve ter para se preservar o internauta.

Então, no caso da IB2K, o sujeito pega uma página do banco, simula que é uma página verdadeira e, em alguns casos, obtém os dados do cliente; em outros, ele faz com que o cliente informe quais são as informações bancárias. O cliente entra lá na página, acha que é a página da instituição bancária, digita o número da conta, da agência e a senha, e essas informações, em vez de irem para a Caixa, vão para o computador, para um servidor que está dominado pelo suspeito. Com essas informações, ele passa a ser dono da conta. Isso aqui é só um exemplo. Há diversas formas de realizar esse tipo de *phishing*, que é como é chamado tecnicamente, e é como o criminoso passa a ser dono das informações e realiza a primeira fase do crime. Só que o criminoso não consegue ir muito além somente com as informações do cliente. É por isso que geralmente esse tipo de delito precisa de associação criminosa. O que acontece? Ele precisa que alguém informe uma conta para poder receber aquele dinheiro fraudulento. Então eu tenho que ter o laranja. Eu preciso de alguém que queira pagar o título bancário. Então, às vezes, acontece de o sujeito não querer pagar o IPVA inteiro. Então, ele vai lá, ele tem um boleto de IPVA de mil reais. Ele chega, e o *hacker* ou o *cracker* informam para ele: *"Eu pago o teu boleto, pago mil reais, me dá 500 reais que eu pago o teu boleto de mil reais"*. Então, ele pega esse dinheiro fraudulento, paga mil reais, o dinheiro é dos outros mesmo, e recebe um dinheiro limpo de 500 reais — limpo, entre aspas, não é? —, exatamente da pessoa que não quis pagar. Então, essa pessoa, que entregou o boleto para ser pago também tem alguma responsabilização nesse tipo de crime.

No caso do telefone é a mesma coisa. Alguém vai lá e informa: *"Faça uma recarga, coloca a recarga no meu telefone para eu poder utilizar"*. Então, o *hacker,*

ou o *cracker* não consegue ir muito além se ele não tiver a participação de terceiros. Então, sem essa participação a fraude não se concretiza.

A partir dessa análise, terminada a dinâmica da operação, ela não conseguiu chegar a todas as pessoas que estavam envolvidas. Algumas pessoas, em razão da volatilidade dos dados, da fragilidade dos vestígios que estão na Internet... Por um motivo ou outro, não se consegue dar continuidade às investigações iniciais em relação a elas. No caso daqueles dois terminais iniciais, por exemplo, a Polícia Federal descobriu que não eram essas pessoas, efetivamente, que eram os suspeitos. Então, tinha um terceiro, que criou um documento falso, documento de identificação falso, e se fez passar por esses dois para poder colocar mais uma dificuldade na identificação da autoria. E a dinâmica das investigações termina gerando isso. A gente muitas vezes não tem o quantitativo suficiente para atender a essa enorme quantidade de fraudes que estão aí disponíveis.

No caso do Tavares, ele terminou se destacando nesse segundo momento, após a instauração do inquérito. E aí a investigação acabou se centrando mais nessa segunda parte, que está vinculada ao Tavares. Então a gente consegue identificar recargas, pagamentos de boletos e pessoas que estavam vinculadas ao Tavares, para focar no que foi possível.

A partir daí, já fechando aqui os trabalhos, foram feitos pedidos de prisão preventiva das pessoas que estavam mais próximas a esse indivíduo, que foi a princípio identificado como o principal responsável desse núcleo ou da organização criminosa, prisões temporárias, que servem para auxiliar a investigação policial, e buscas e apreensões. Foram feitos, então, quebras de sigilo bancário, sequestro de ativos, indisponibilidade de bens, e essa investigação foi submetida à apreciação judicial. O Ministério Público já denunciou parte da quadrilha, e estamos nesse pé. Obviamente que as investigações não cessam, nós temos diversos outros casos que estão em andamento, mas, em relação à IB2K, que é um caso específico, a Polícia Federal continua à disposição da Justiça para auxiliar nas investigações em curso ainda na ação penal. Em relação às pessoas que não foram identificadas, a investigação permanece meio que em aberto. Na medida em que chegarem informações novas, as investigações são reiniciadas. Então, basicamente, o que eu tinha para falar da IB2K é isso.

Coloco-me à disposição dos senhores caso haja uma necessidade de intervenção ou esclarecimento maior.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Sr. Stênio. Eu gostaria de já pedir ao senhor a disponibilização de toda a apresentação à nossa CPI, para que possamos passá-la a todos os nossos membros também, se for possível.

O SR. STÊNIO SANTOS - Claro.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Concedo a palavra ao Dr. Elmer Coelho Vicente, Chefe do Serviço de Repressão a Crimes Cibernéticos.

O SR. ELMER COELHO VICENTE - Boa tarde, eu queria agradecer o convite para compartilhar um pouco da nossa experiência na repressão aos crimes cibernéticos. A minha contribuição vai ser um pouco do que a gente tem enfrentado, do que a gente tem passado na repressão aos crimes cibernéticos.

Pegando um gancho na apresentação do Stênio, a conclusão desse modelo de notícia-crime, desse termo de cooperação com a Caixa Econômica é que, por estarmos inseridos hoje numa sociedade de informação em que a tecnologia está cada vez mais sendo massificada, o acesso à Internet cada vez aumentando mais, cada vez mais teremos incidências de crimes cibernéticos, cada vez mais os bens jurídicos que a nossa Constituição, que as nossas leis visam proteger vão ser mais lesados, e essa informação cada vez mais vai chegar para as autoridades.

Hoje não é preciso ir até uma delegacia para fazer a notícia de um crime. Hoje, a pessoa, na sua casa, com a Internet — a gente sabe de algumas delegacias virtuais, ou até o próprio *e-mail* de algumas instituições —, encaminha notícias-crime as mais diversas. Com isso, há um entupimento, não tem outra palavra para caracterizar isso, de informações a serem tratadas pelos órgãos de segurança pública.

Se não houver uma força-tarefa, uma união de esforços para que todas essas informações que chegam sejam tratadas, a gente, na verdade, estará fazendo uma exclusão de alguns crimes que a gente consegue enfrentar. A gente está, na verdade, segregando e priorizando alguns outros crimes.

A dificuldade toda começa na questão de quem vai investigar. É a questão da determinação territorial de quem vai investigar. Eu vou dar um exemplo: existe um perfil no Facebook que proferiu uma ameaça, que está ofendendo determinada pessoa ou praticando um certo crime de preconceito. A gente tem lá um nome na Internet, a gente não sabe onde aquela pessoa está. Quem vai começar a investigar? Bom, existe esse nome da Internet, mas a gente precisa de um IP, pra gente começar a tratar da identificação real do sujeito. Hoje, para a gente saber quem é esse sujeito, a gente precisa instaurar um procedimento, solicitar ao Judiciário e, com a ordem judicial, ir até o provedor do serviço — essas empresas que fornecem esse serviço na Internet são caracterizadas como provedores de serviço —, que nos fornece uns *logs* de IP. Bom, nesse lapso de aguardo de tempo o crime já vai ficando velho, a gente vai já perdendo um pouco da oportunidade da investigação em que os indícios estão mais evidentes...

O SR. DEPUTADO SANDRO ALEX - Quanto demora esse tempo?

O SR. ELMER COELHO VICENTE - Depende da localidade em que você está. Mas não é uma coisa rápida, pode chegar a meses — depois o Dr. Stênio pode até voltar para dizer quanto tempo demorou a IB2K —, porque, nessa dialética de que eu chego a alguém na Internet, mas eu preciso de um IP para a investigação andar, ela, hoje, não atende à velocidade de resposta do Estado. E enquanto eu estou esperando eu já recebi outras mil notícias.

E, voltando à questão: quem vai investigar? Eu tenho lá um nome “João” na Internet. A Polícia Federal? Isso é um crime federal ou um crime interestadual? Não, não é. Está o.k. Para quem você vai mandar? Eu não sei, porque para eu instaurar eu vou ter que deflagrar algum ato de Polícia Judiciária, que é pedir, judicialmente, esses *logs*. Ou seja, eu não vou atuar na atribuição que me foi determinada legalmente, constitucionalmente, para que eu tenha que fixar uma determinação territorial.

Hoje em dia, até as empresas têm um papel proativo na identificação de alguns crimes, nessa detecção de abuso de perfis ou abuso de mensagens, mas elas não sabem para quem enviar. Antes do Marco Civil, algumas empresas, já sensíveis a essa necessidade, forneciam, mediante requisição policial, os *logs* dos serviços, e isso dava uma agilidade muito grande para a investigação. Mas, com o

Marco Civil, houve um retrocesso. Dom isso, nós temos que judicializar a questão da obtenção dos *logs*. E essa judicialização dos *logs* chega até a criar assim uma incongruência na própria proteção da sociedade.

Existe um crime acontecendo na Internet. Ele está acontecendo, nós estamos vendo, ele está lá, está sendo publicado. Se fosse no mundo real, eu poderia prender a pessoa em flagrante, quiçá até entrar no seu domicílio. Mas, no crime cibernético, eu não consigo. Se qualquer um dos senhores chegar e falar que foi ameaçado por um perfil no Facebook, se soubermos qual é o perfil daquela pessoa, se a ameaça está lá, está no ar, está proferindo as ofensas, não conseguimos saber quem ela é e não conseguimos chegar até ela se não tivermos um procedimento judicial prévio para ir atrás. Isso vai contra toda a sistemática da própria prisão em flagrante.

Então, hoje em dia, se alguém chega à delegacia e fala *"Olha, há um vídeo da minha filha que foi sendo divulgado, e eu gostaria que fosse presa essa pessoa. Essa pessoa está aqui, ó. Eu estou num grupo, no WhatsApp, e essa pessoa está constantemente postando um vídeo da minha filha. Você consegue prender essa pessoa?"*, respondo: *"Não. Eu vou demorar um tempo para chegar e prender essa pessoa"*.

Bom, seguindo nessa questão da dificuldade de obtenção de *logs*, nós passamos também por uma dificuldade, às vezes, de comunicação com as próprias empresas. Se nós obtemos um *log*, vamos atrás do provedor de conexão, que é quem vai me dizer: *"Olha, esse IP é de determinada pessoa"*. Então, mais ou menos são duas partes básicas do crime cibernético, num raciocínio bem simples, que é uma receita de bolo. Nós precisamos do provedor de serviço, que nos fornece o IP, e do provedor de Internet, que são as telefonias, dizendo a quem foi atribuído aquele IP.

Com o avanço da legislação, uma vitória para a sociedade, hoje nós conseguimos requisitar, em alguns crimes, a questão do dado cadastral do IP. Só que, por incrível que pareça, algumas empresas não aceitam que eu forneça essa requisição de forma eletrônica. Eu tenho que mandar via papel. Algumas não aceitam nem *e-mail*. Eu tenho que mandar por fax. Você fala: *"Bom, isso é tranquilo"*. Tranquilo, se você tiver uma pequena incidência de crime. A partir do

momento em que estamos numa sociedade de informação, em que todo dia está chegando denúncia e em que os números de IP são milhares, isso se torna um transtorno muito grande.

Na questão da fraude bancária e na questão da pornografia infantil, em que nós temos uma base de ofensores muito grande, já tentamos, com as operadoras, sensibilizar para essa otimização da resposta. Foi em vão.

O ano passado nós recebemos cerca de 50 mil relatórios de potenciais casos de pornografia infantil envolvendo brasileiros. Otimizamos essa análise, e não vimos outra saída a não ser como esse modelo da Tentáculos, que é você jogar numa base para fazer um correlacionamento. Tentamos fazer uma quebra de todos esses IPs e pedimos às operadoras: *"Por favor, nos encaminhem isso de forma eletrônica, numa tabela, para que tenhamos condições de correlacionar e trabalhar"*. Foi feita uma reunião, mas não se teve eficácia no resultado.

O SR. DEPUTADO SANDRO ALEX - Judicialmente ou extrajudicialmente que o senhor fez isso?

O SR. ELMER COELHO VICENTE - Extrajudicialmente, porque a lei permitia. Era questão de dado cadastral. Nós precisávamos isso de uma tabela, da forma como a operadora tivesse mais facilidade. Mas, se vier em papel, imagine alguém com 200 mil IPs de pornografia infantil! É possível trabalhar isso no papel, no País, para distribuir às autoridades em cada local? É inviável, porque, enquanto eu estou digitando no papel, eu estou perdendo um analista que poderia estar analisando um caso ou fazendo a rastreabilidade de um criminoso.

Avançando na questão dos *logs*, um outro ponto muito importante é a questão do respeito.

O SR. DEPUTADO SANDRO ALEX - Presidente, pela ordem. Desculpe-me, mas é que o senhor falou das operadoras. O senhor fez uma reunião extraoficial. Quais as operadoras?

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Deputado, nós poderíamos deixar as perguntas para depois das exposições.

O SR. DEPUTADO SANDRO ALEX - Eu entendo. É que realmente é um assunto...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Senão, vamos acabar perdendo e atrapalhando a linha. Terminadas as exposições, todos fazem perguntas.

O SR. DEPUTADO SANDRO ALEX - Bom, eu...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - V.Exa., como Sub-Relator, vai ter prioridade logo depois. Nós ainda temos mais um convidado para fazer a sua exposição.

O SR. DEPUTADO SANDRO ALEX - Não farei mais. É que, realmente, quais são as operadoras?

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - É só para guardar. Já deixe essa sua pergunta. Quando abrirmos para as perguntas, V.Exa., como Sub-Relator, tem prioridade logo no início.

O SR. ELMER COELHO VICENTE - Um outro ponto muito importante é a questão do respeito à soberania brasileira. É diário o desrespeito. O Marco Civil conseguiu, de uma forma muito brilhante, normatizar esse respeito, de forma que, passando o fluxo de conexão na Internet pelo Brasil, se esse fluxo corresponder a uma ação criminosa, deve haver respeito às leis e às autoridades brasileiras. Pois bem, sabemos que muitas empresas não estão sediadas no Brasil, nem têm representantes no Brasil. E aí é que vem a dificuldade concreta de respeito a uma ordem judicial brasileira e a uma lei brasileira.

Eu vou trazer um caso que já foi muito divulgado na mídia de uma empresa que nos traz constantes problemas: WhatsApp. Pois bem, o WhatsApp realmente é uma maravilha tecnológica, que trouxe benefícios para toda a sociedade. Fazem parte dessa sociedade grupos de extermínio, organizações de tráfico de droga, facções criminosas, produtores de pornografia infantil, e, não diferentemente da sociedade em que eles vivem, eles usam o WhatsApp. Não chegamos ao extremo de falar que não é mais possível o uso do WhatsApp pela sociedade. Não. É. Mas tem que haver um ponto de equilíbrio para, quando houver uma situação criminosa, respeitar-se a lei brasileira.

Isso nós tentamos diariamente, porque sabemos que alvos em grupos de extermínio são passados via WhatsApp, locais de entrega de entorpecentes são combinados via WhatsApp, toda a movimentação policial é passada, às vezes, via

WhatsApp, para algumas facções criminosas e vídeos de pornografia infantil são passados via WhatsApp.

Já tentamos, inúmeras vezes, através de investigações, fazer culminar interceptação telemática do WhatsApp; já tentamos inclusive via MLAT, só que em vão. Hoje em dia o WhatsApp é um ambiente a que as autoridades não chegam. Então, se existe um mecanismo no ordenamento jurídico brasileiro de municiar, em casos excepcionais, os órgãos da persecução penal desse conteúdo das mensagens, que é o caso da lei de interceptação, para o WhatsApp ela não vale.

O WhatsApp foi comprado recentemente pelo Facebook. E apesar de o Facebook ter representante no Brasil, o Facebook Brasil tem respondido, nas investigações em andamento, que ainda não tem condições de responder pelo WhatsApp, porque a fusão ainda não foi total em suas operações.

A questão nem se ultima na interceptação. Se nós quisermos bloquear um determinado conteúdo, como um vídeo, ou fazer a rastreabilidade de um conteúdo, como no caso de vazamento de provas públicas, vamos ter uma dificuldade muito grande, porque não conseguimos falar com o WhatsApp. O WhatsApp não nos respeita. Temos ordem brasileira, mas ineficaz.

Então, nós temos uma dificuldade muito grande nessa questão da soberania. Alguns *blogs* foram recentemente divulgados na imprensa com ofensas às mulheres. O *blog* está nos Estados Unidos, não tem representante no Brasil. A interpretação americana da liberdade de expressão é tão grande que, aqui no Brasil, chega a haver uma diferença de interpretação. Se para nós é crime e aquele conteúdo tem que ser retirado do ar, se um juiz dá a ordem, não interessa. Se a empresa responsável por aquele serviço é americana, ela vai dizer: *"Olha, não temos condições de tirar. Submeta-se ao processo do MLAT".* E o processo do MLAT é muito lento e às vezes examina a questão da dupla incriminação. Nessa questão de transnacionalidade, é necessário aí um debate para se chegar a mecanismos mais eficientes para a persecução penal.

Hoje em dia são diversas tecnologias que vão chegando à nossa sociedade e que vão se distanciando da regulamentação. Um exemplo disso é o *bitcoin*. São moedas virtuais, em que hoje o dinheiro do criminoso não precisa estar no banco. A polícia pode chegar a ter uma investigação bem-sucedida, ela pode chegar ao

criminoso, e uma das medidas mais eficientes para que esse criminoso não volte a delinquir é a tomada do seu patrimônio.

Hoje em dia nós temos percebido cada vez mais que alguns têm se utilizado dessas moedas virtuais para guardar seu dinheiro, em proveito do crime. Não existe ainda uma regulamentação, as empresas são as mais diversas, e elas ainda não têm claramente qual o seu papel de informação junto às autoridades sobre o montante que cada cliente tem lá. O cliente pode ter lá coisa de 1 milhão de reais, e a Receita não vai ser informada. O cliente pode depositar mil reais, mandar de um país e sacar em outro em *bitcoin*, e ninguém ser informado. Então, a lesividade, a possibilidade de evasão de divisas é muito grande.

Encerrando, realmente existe uma necessidade de capacitação dos órgãos envolvidos na persecução penal. Nós aqui estamos trabalhando diariamente. Só que é muito pouco para a quantidade de crimes, para a quantidade de denúncias e para o tamanho do enfrentamento do problema. Se a carência de efetivo técnico na Polícia Federal é grande, nós percebemos uma maior proporção nos Estados, que enfrentam uma maior incidência de crimes e têm outras prioridades a enfrentar.

A questão da capacitação específica para crimes cibernéticos é muito importante, porque a partir daí é que nós vamos começar a dar uma resposta mais eficiente.

Quero agradecer e estou à disposição para maiores esclarecimentos sobre o que foi dito.

A SRA. PRESIDENTE (Deputada Mariana Carvalho) - Obrigada, Dr. Elmer.

Tem a palavra o Dr. Carlos Eduardo Miguel Sobral, Assessor da Coordenação-Geral de Projetos de Tecnologia da Informação da Secretaria Extraordinária de Segurança em Grandes Eventos, do Ministério da Justiça.

O SR. CARLOS EDUARDO MIGUEL SOBRAL - Deputada Mariana Carvalho, da minha querida Rondônia, onde tive oportunidade de começar a minha carreira, em 2003, muito obrigado; agradeço a V.Exa., em nome da Comissão, o convite para participar desta audiência pública; Deputado Esperidião Amin, obrigado pelo convite; nobres colegas delegados, colegas de trabalho com quem atuamos nos últimos 7 ou 8 anos, é um prazer reencontrá-los nesta oportunidade; senhoras e senhores, bom dia a todos.

Eu vou trazer uma breve contribuição, ratificando as palavras do Dr. Elmer e do Dr. Stênio. São tantos os problemas que nos acometem e durante as falas dos colegas me veio um filme. Eu comecei a trabalhar nesta área em 2008, quando vim a Brasília, removido de Rondônia, para assumir a Coordenação do Combate aos Crimes Cibernéticos, na Polícia Federal.

Em 2008, nós realizamos uma operação de combate à pornografia infantil, que foi denominada Operação Carrossel, uma operação de âmbito global, mais de 110 álbuns no Brasil, mais 230 álbuns mundo afora. O resultado dessa Operação, além das ações que foram realizadas, foi a consciência, naquela oportunidade, de que a nossa legislação para proteger a criança e o adolescente em ambiente virtual era falha. Faltavam-nos instrumentos legais, normativos, para proporcionar uma ação mais efetiva na proteção à criança e ao adolescente.

O Senado, de forma muito oportuna, aprovou e conduziu uma CPI, a chamada CPI da Pedofilia, e nós tivemos a oportunidade de também participar da primeira audiência pública daquela CPI e trazer os fatos, trazer as situações que nos afligiam como autoridade de investigação e repressão a ilícitos, permitindo à sociedade um maior conhecimento e um maior debate.

Os resultados daquela iniciativa foram muito profícuos. Nós conseguimos avançar em termos legislativos, o Senado e o Parlamento. Depois virou uma lei sancionada pelo então Presidente Lula, a Lei nº 11.829, de 2008, que criminalizou algumas condutas envolvendo pornografia infantil na Internet, como a posse, a comercialização, a aquisição e a produção da pornografia infantil, melhorando, aperfeiçoando o Estatuto da Criança e do Adolescente. Conseguimos realizar um termo de cooperação técnica com o Google, que na época detinha os maiores problemas envolvendo a pornografia infantil.

A SRA. PRESIDENTE (Deputada Mariana Carvalho) - Eu gostaria de pedir silêncio, para que possamos ouvir o nosso expositor, por favor!

O SR. CARLOS EDUARDO MIGUEL SOBRAL - Na época, a rede social de maior uso pelo brasileiro era a Rede Orkut, e realmente havia muitos problemas envolvendo pornografia infantil nessa rede social. Nós conseguimos realizar um acordo de cooperação técnica com o Google e passamos a receber informações que nos permitiram agir. Fizemos a Operação Turko. Dr. Stênio era assessor da CPI, e

eu também fui assessor da CPI durante algum tempo, por quase 2 anos. Nós conseguimos realizar a Operação Turko, que é um anagrama do Orkut. Realizamos um acordo de cooperação técnica com as companhias telefônicas, para que nos passassem os dados de conexão, dados cadastrais, de forma organizada, de forma automatizada. Infelizmente, pelas palavras do Dr. Elmer, vejo que esse acordo de cooperação técnica não teve bom andamento, os problemas se repetem 6 anos após. E conseguimos, pelo menos na parte de direito material, na parte tipo penal, melhorar bastante a legislação envolvendo a proteção à criança e ao adolescente.

No campo da estrutura, a Polícia Federal montou um Grupo Especial de Combate à Pornografia Infantil e aos Crimes de Ódio, o GCOP. O Dr. Stênio teve a oportunidade de chefiar, e hoje o Dr. Elmer é o chefe desse grupo. Montamos unidades nas unidades da Polícia Federal, e o andamento, as investigações tiveram realmente um avanço.

Em 2009, nós passamos a enfrentar um novo problema, que eram os crimes bancários. Nós tínhamos diversas investigações em andamento na Polícia Federal, e cada investigação tinha uma parte pequena da informação que nos permitiria enxergar a atuação de quadrilhas. Só sabemos que esses crimes bancários são praticados por quadrilhas. Não temos uma pessoa isolada furtando uma conta. Nós temos um grupo organizado que pratica furto qualificado no Brasil inteiro, de pequenos valores cada um, mas que, somados, alcançam milhares, milhões de reais, como o Dr. Stênio mostrou na Operação IB2K. No mínimo, foram 2 milhões de reais, mas a experiência disso são de 10 a 15 a 20 milhões, cada grupo criminoso.

É muito dinheiro, tanto que a FEBRABAN anuncia que o prejuízo do sistema bancário brasileiro alcança 1 bilhão, às vezes mais de 1 bilhão de reais por ano, que são desviados do sistema que nós pagamos, ou seja, todo mundo que tem conta paga esse custo e esse dinheiro é desviado para grupos criminosos que o utilizam para todo tipo de ilícito.

Então, nós fizemos, a Polícia Federal com a Caixa, que é empresa pública — e nós temos a obrigação constitucional de apurar os ilícitos praticados contra ela —, com o apoio do Ministério Público, desenvolvemos um sistema que nos permitiu, em 2009, montar uma grande Base Nacional de Fraudes Bancárias Eletrônicas, dentro do que nós denominamos de Projeto Tentáculos, tentando o quê? Aglutinar, reunir

as informações que estavam espalhadas no Brasil inteiro; pegar as peças que estavam em cada investigação, juntar tudo em uma base de dados e, através de ferramentas de inteligência, como a que o Dr. Stênio mostrou, conseguir enxergar a atuação de uma quadrilha e não mais investigar fato a fato, fraude a fraude, mas, sim, investigar a atuação de um grupo criminoso. E, além de montar essas informações, nós aperfeiçoamos a antiga Unidade de Repressão a Crimes Cibernéticos. Ela foi elevada em nível de serviço dentro da Direção-Geral da Polícia Federal, e criamos 15 grupos especializados para combater fraudes bancárias eletrônicas. Nós já tínhamos os grupos para combater a pornografia infantil e criamos os 15 grupos para combater a fraude bancária eletrônica. Capacitamos — foram mais de 2 milhões de reais investidos em capacitação — e treinamos mais de cem policiais federais para atuar nessa área.

E quais foram os resultados? Quando nós conseguimos unir informações, que antes estavam espalhadas e foram concentradas, quando nós conseguimos estruturar as unidades de investigação, quando nós conseguimos qualificar o policial federal que promove a investigação, os resultados foram imediatos. A partir de 2011, quando o sistema passou a estar em pleno funcionamento até 2014, as fraudes contra a Caixa Econômica Federal, fraudes bancárias, tiveram uma redução de 67%. Foram realizadas dezenas de operações nos moldes da IB2K. Foram presos mais de 200 criminosos, desarticuladas mais de 40 quadrilhas.

Antigamente, quando nós tínhamos uma investigação isolada, quando se levava à Justiça para fins de responsabilização, quando olhávamos só aquele fato, o juiz não tinha a consciência de todo o grupo criminoso. Então, a punição era muito pequena. Às vezes, nem se conseguia uma punição, era uma fraude de mil reais, dois mil reais. Então, na verdade, dava quase uma insignificância. Mas, quando você consegue reunir, quando é um grupo organizado, atuando de forma organizada, que desvia milhões de reais, utilizados para todo tipo de crime, inclusive tráfico de armas e drogas, você demonstra a periculosidade daquele grupo criminoso, e as punições são maiores, o que leva, necessariamente, a um sentimento, dentro do sistema criminoso, de que há uma reação forte do Estado e, necessariamente, o número de crimes cai.

Então, nós conseguimos reduzir o número de fraudes no Estado brasileiro, o número de crimes contra a Caixa Econômica Federal em 67% em 4 anos. Por quê? Porque nós investimos em tecnologia, investimos em capacitação e investimos em informação. Se nós não tivéssemos as informações disponíveis em tempo real, seria impossível realizar uma boa investigação criminal; sem uma boa investigação criminal, não temos uma boa denúncia; sem uma boa denúncia, não temos um bom processo penal; e, sem um bom processo penal, não temos uma boa responsabilização, não temos uma justa responsabilização dos autores.

Além do combate à fraude, também conseguimos avançar em outro campo que nos preocupava muito, que preocupava muito o Estado brasileiro. Nós conseguimos colocar no Direito Penal a proteção a alguns outros bens, como a informação. Nós conseguimos trazer para o Direito brasileiro a proteção da informação armazenada em dispositivos computacionais. Foram muitos anos de debate, mas em 2012 conseguimos avançar, e o Parlamento e a Presidência da República trouxe ao Direito brasileiro a Lei Carolina Dieckmann, que estabilizou a proteção da informação. Há discussão se há espaço para aperfeiçoamentos. Isso é natural do processo e sempre haverá, mas conseguimos avançar, destravando mais esse nó.

Então, hoje, na minha opinião, nesta contextualização, nós temos uma boa legislação para a proteção da infância, da criança e do adolescente na rede. A nossa lei, o ECA, é um bom instrumento e permite que a polícia, no campo material penal, tenha atuação. Nós temos uma boa legislação para reprimir a fraude bancária, também no Direito material; nós temos uma boa legislação para proteger as informações armazenadas em dispositivos computacionais, que é a Lei Carolina Dieckmann; nós avançamos com a edição do Marco Civil da Internet, que também foi um processo, uma discussão iniciada em 1998, que ganhou corpo em 2008 e foi transformada em lei em 2013. Há algumas ressalvas do aparato estatal de investigação que se entende no Marco Civil como algumas amarras, mas isso é um fato que deve ser trazido à discussão.

Eu queria fechar assim a minha exposição, para permitir o início do debate. Repito: sem uma boa estrutura de investigação, não há como promover uma boa segurança pública. Não há como se realizar qualquer tipo de investigação se as

polícias judiciárias não estiverem devidamente preparadas para investigar esse tipo de delito. E é um delito que não é de fácil elucidação. É um delito que envolve tecnologias e técnicas complexas, que envolve a necessidade de conhecimento do policial, um conhecimento especializado, e, se as polícias não estiverem preparadas para receber a notícia de crime pelo cidadão ou por instituições do Estado, se elas não tiverem condições de promover uma boa investigação, o crime organizado e a criminalidade geral se sentirão muito à vontade para continuar praticando as suas ações.

Eu nem entro na questão da punição, se deve ser punido com reclusão, com detenção, mas o que acontece hoje é que, na verdade, nem sequer as pessoas são identificadas. E isso é muito grave. Quando o Estado não tem a capacidade de encontrar o autor de um delito, as portas estão abertas para a criminalidade, que se utiliza de técnicas e se utiliza de uma estrutura da Internet que permite dificultar a atuação do Estado.

Então, é muito fácil para o criminoso estar localizado aqui no Brasil e praticar as suas ações através da rede espalhada no mundo inteiro. É muito fácil para o criminoso estar aqui no Brasil e utilizar um WhatsApp. É muito fácil para o criminoso estar aqui no Brasil e utilizar um Telegram, que, além de estar fora do País — o Telegram está hospedado na Rússia —, ele está encriptado, ou seja, há uma camada a mais de obstáculos e dificuldade para o Estado.

É muito fácil para o criminoso montar uma rede virtual, um disco virtual e armazenar as suas informações no Leste Europeu. É muito fácil ele usar redes de computadores controlados para mascarar a sua conexão, o que nos obrigaria a rastrear essa conexão mundo afora. E é muito difícil para nós enfrentarmos essa situação num ambiente de uma cooperação internacional ainda pensada para o início do século, sendo que, na tecnologia, o que é pensado para ontem já está atrasado.

A técnica do crime atualiza-se muito rápido. Só um exemplo: nós estamos acostumados a fazer uma busca e apreensão, a ir a um local, a uma residência, a uma empresa e encontrar os documentos ou apreender o computador usado lá. Só que, se o criminoso for um pouquinho preparado para a prática criminosa, ele vai deixar a informação armazenada dentro do dispositivo dele, dentro do computador,

na casa ou na empresa dele? Não. Ele vai colocar nas nuvens ou vai colocar num disco virtual fora do País. E nós podemos buscar essa informação fora do País, através de técnicas de acesso ao computador dele? A nossa legislação permite? O outro país vai se sentir ofendido e invadido na sua soberania se nós Estado brasileiro formos buscar a informação que está lá armazenada? Essa prova é legal?

Se nós não fizermos isso e buscarmos imediatamente essas informações, o criminoso pode dar um comando e apagar tudo, todas as informações, que vão estar encriptadas. Se nós conseguirmos chegar, a informação vai estar segura, vai estar protegida, nós vamos ter de desenvolver tecnologia para decriptar, quebrar aquela informação que está protegida.

Eu trouxe só essas nuances da dificuldade para demonstrar que se nós não tivermos uma estrutura de investigação pronta, que seja treinada, que tenha à sua disposição o que há de mais moderno no mundo em tecnologia de investigação, nós não conseguiremos desenvolver boas investigações. E eu não falo nem da Polícia Federal — nós temos uma condição hoje muito melhor do que tínhamos alguns anos atrás —, mas falo de toda a estrutura de investigação no Brasil, de toda a estrutura de investigação de todas as polícias judiciárias, que hoje, realmente, estão aquém daquilo que nós necessitamos para promover uma boa ação estatal.

Isso foi previsto. Durante os debates de 2008 a 2014, isso estava previsto. Essa dificuldade nossa, do Estado brasileiro, estava prevista, tanto que, se me permitem, eu vou fazer a leitura do art. 4º da Lei nº 12.735, de 2012, que diz:

> *"Art. 4º. Os órgãos de polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado."*

Ou seja, a Lei 12.735/12 já determina que toda instituição de Polícia Judiciária tenha delegacia especializada em repressão a crime cibernético, ou seja, ação delituosa praticada em rede de computadores, e essa realidade ainda não acontece. Então, se nós tivéssemos avançado mais nos últimos anos, com certeza, o cenário de crimes praticados na rede poderia ser melhor, porque uma boa investigação gera

uma boa denúncia; uma boa denúncia gera um bom processo e a identificação dos autores.

Hoje, nós temos essa carência. Então, se teria algo a contribuir neste debate é nesse sentido. A nossa legislação avançou muito no campo penal, tem espaço para avançar no campo processual, como Dr. Elmer abordou, mas nós temos uma carência imensa no campo estrutural. A nossa estrutura de investigação ainda é muito carente e não permite que o Estado atue da forma que deveria atuar.

Obrigado.

A SRA. PRESIDENTE (Deputada Mariana Carvalho) - Obrigada, Dr. Carlos. Agora, encerradas as exposições, passaremos aos debates.

Concedo a palavra ao Deputado Esperidião Amin, nosso Relator, para dar início aos debates.

O SR. DEPUTADO ESPERIDIÃO AMIN - Bom dia a todos. Eu quero, em primeiro lugar, cumprimentar nossos três expositores, os Srs. Stênio, Elmer e Sobral.

Eu considero que esta reunião é o marco zero da nossa busca de um relatório. Temos aqui três dos quatro Relatores Setoriais. Eu vou procurar otimizar o tempo, vou ser o mais conciso possível, até para abrir espaço para que os Relatores Setoriais satisfaçam os quesitos inerentes ao campo em que vão atuar.

Por isso, muito mais do que indagações, vou abordar alguns tópicos para os quais eu peço a atenção dos nossos expositores. Primeiro, a minha pergunta para o Dr. Stênio é associada aos dois outros expositores, especialmente ao Dr. Sobral: onde ocorreu a primeira intervenção do Judiciário na operação? Estou sendo claro, Dr. Stênio? Ou seja, quando é que vocês obtiveram autorização judicial, em que momento, em que etapa, houve a intervenção do Ministério Público e do Judiciário para legalizar a escuta, por exemplo? Formulo a questão bem sinteticamente.

Segundo, os senhores têm atuação também na fraude contra tributos? Ou seja, não estou falando de COAF; estou falando de *"Te cobro 500 para anular uma dívida de mil"*, em matéria tributária, porque aí o dinheiro é um pouco mais grosso, como lembrou o nosso... E essas leis, tirar o dinheirinho todo dia, também gostaria de uma breve visão sobre esse aspecto, e se esse aspecto foi contabilizado nos 67% de redução de crimes financeiros, até remetendo o assunto depois para o nosso Relator Setorial, Deputado Sandro Alex.

Sr. Elmer, eu entendi bem quando o senhor disse que a judicialização atrapalhou? Não. Fale um pouquinho sobre isso, porque a demora a que o senhor se referiu é que enseja as tentações para procurar atalhos. Quando eu falo atalhos, falo em práticas extralegais. E tenho ainda uma indagação para o senhor: o senhor falou que é difícil quando a sede do *blog*, por exemplo, está nos Estados Unidos, mas eu faço minhas as palavras do Dr. Sobral. Pior é se elas estiverem no Tadjiquistão, com todo respeito ao Tadjiquistão ou a qualquer outra república integrante da ex-União Soviética, onde a questão legal é mais desconhecida, não quero dizer que não exista, mas é muito mais desconhecida. Os senhores se lembram onde estavam os primeiros *sites* de pornografia? No Leste Europeu, aproveitando-se dessa obscuridade legal.

É por isso que eu acho muito importante olharmos para o futuro. O nosso relatório — nós sabemos — tem a parte retrospectiva e tem a parte prospectiva, especialmente na questão das leis. A minha pergunta ao Sr. Sobral é: quando estrutura os sistemas, o senhor não fala em Forças Armadas. Quem organizou todo o aparato de segurança na Copa foi o Ministério da Justiça e/ou o Ministério da Defesa? Nós tivemos aqui as exposições do Ministério da Defesa, em 2014 e 2013, até porque nós estamos aqui abordando crimes cibernéticos civis. Os militares, segurança de transporte aéreo, são bem mais perigosos. Estruturação é isso.

Finalmente, eu acho que nós temos, com a ajuda dos nossos Relatores Setoriais, de tratar da avaliação das leis. Nós tivemos aqui um breve inventário das leis. Não estou falando de Código Penal, mas das leis sobre cibernéticos, desde a Lei do ECA, passando pela Lei Carolina Dieckmann e passando pelo Marco Civil da Internet. Eu acho que nós deveríamos começar a pensar em um seminário de avaliação, porque a lei mais antiga é de 2008, mas as duas que eu considero principais são de 2012 e de 2014. É muito difícil você saber se elas pegaram e medir o grau da sua eficiência.

O último tópico que eu considero, pessoalmente, o mais importante: estruturar e qualificar. Onde é que vocês estudaram? Individualmente? Ou seja, onde vocês aprenderam ou pensam que vão aprender mais para se atualizar? Deu para entender? Eu fui analista de sistemas no final dos anos 60. De lá para cá, eu procurei me atualizar, mas eu sou um jurássico, e vocês também vão ficar jurássicos

em menos de 6 meses. Hoje está mais rápido ficar jurássico. Então, como é que nós vamos qualificar, não uma vez, mas estabelecer uma estrutura que conte com um processo de qualificação?

Era isso, Sra. Presidente. Eu acho que os nossos Relatores Setoriais complementarão as minhas colocações.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Gostaria que as respostas fossem iniciadas pelo Dr. Stênio, depois pelo Dr. Elmer e depois pelo Dr. Carlos.

O SR. STÊNIO SANTOS - Obrigado pelas perguntas, Deputado. Para responder especificamente em relação à IB2K, é preciso contextualizar rapidamente, também não vou tomar tempo.

No caso específico da Operação IB2K, a primeira intervenção judicial ocorreu após a instauração do inquérito. Nós não podemos, em momento algum, realizar interceptação telefônica e telemática sem inquérito policial. Daí...

O SR. DEPUTADO ESPERIDIÃO AMIN - Telemática também?

O SR. STÊNIO SANTOS - Telemática também.

O SR. DEPUTADO ESPERIDIÃO AMIN - Não há uma tentaçãozinha aí?

O SR. STÊNIO SANTOS - No meu caso, não. *(Risos.)* Pessoalmente, não, até porque ela não vai ter validade alguma depois, e o...

O SR. DEPUTADO ESPERIDIÃO AMIN - Nós queremos ser um *hacker* do bem.

O SR. STÊNIO SANTOS - *(Risos.)* Só que no nosso sistema não há essa permissão. Então, a intervenção policial nesse caso não teria validade alguma. Então, estaríamos, na verdade, dando um passo para trás. Mas, fora desse aspecto processual, existe essa possibilidade de tentação.

Especificamente no caso da IB2K, em 2009, com esse termo de cooperação que foi feito com a Caixa Econômica Federal, as informações dessa prestadora de serviço, no caso a Caixa Econômica Federal, foram encaminhadas de forma automática para a nossa base.

Então, com esse primeiro pedido que foi feito a partir de 2014, com o Marco Civil da Internet, os provedores deixaram de ser necessários. Eu vou tomar a

liberdade de ler o art. 10 do Marco Civil da Internet, Lei nº 12.965, de 2014, no § 1º, que passou a dizer o seguinte:

> *"Art. 10.....*
>
> *§ 1º O provedor responsável pela guarda* — no caso dos registros de conexão e de acesso a aplicações de Internet — *'somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial (...)"*

Então, até o Marco Civil da Internet, os grandes provedores de Internet, as telas, estavam fornecendo, de forma espontânea ou a pedido, esses registros. A partir do Marco Civil da Internet, então, houve esse retrocesso.

No caso, como o § 1º diz *"somente será obrigado"*, o nosso entendimento é: se quiser colaborar, não há problema algum, até porque o que a Constituição exige é o que está lá no art. 5º, XII. Então, a intervenção judicial é obrigatória no art. 5º, XII, que fala:

> *"Art. 5º.....*
>
> *XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas..."*

Então, nessas hipóteses em que a polícia, o Judiciário ou o Ministério Público podem ter acesso ao conteúdo das comunicações, e, aí sim, invadir a privacidade do suspeito ou do cidadão, é que a Constituição exigiu a ordem judicial. Nos demais casos, essa ordem não é necessária.

Quando a gente judicializa isso previamente, a tendência é que haja uma desaceleração natural: em vez de a polícia obter diretamente, ela, primeiro, representa para o Judiciário, que solicita o parecer do Ministério Público, que se manifesta e, aí sim, há uma requisição do juiz. Esse processo pode durar 6 meses, às vezes até 1 ano, enquanto que o Código de Processo Penal requer que a investigação seja concluída em 30 dias. Então, essa exigência aqui é incompatível com a exigência de conclusão da investigação em 30 dias.

Como no caso das fraudes bancárias eletrônicas se ultrapassou essa fase de se pedir a primeira intervenção, somente depois da instauração do inquérito, e, aí sim, seguindo estritamente o que exige a Constituição Federal, é que houve essa necessidade de intervenção judicial. E, mesmo assim, a investigação demora. Então, quando se cria mais uma fase de intervenção judicial, ela, no mínimo, vai demorar duas vezes mais. E aí, no caso de crimes cibernéticos, a demora sempre corre contra o Estado.

O suspeito, o criminoso, a pessoa que praticou a conduta ilícita ou típica vai estar sempre na vantagem, porque ela vai estar se escondendo e o Estado tem que correr atrás. Os vestígios são voláteis e, muitas vezes, quando se vai solicitar essa informação, ela não está mais em lugar nenhum, ela já foi destruída. Então, esse é o risco.

No caso das fraudes tributárias, temos uma unidade especializada para cuidar de desvio de recursos públicos e crimes financeiros. Então, não seria...

(Intervenção fora do microfone. Ininteligível.)

O SR. STÊNIO SANTOS - Isso, eventualmente, quando ocorre a necessidade, a unidade de crimes cibernéticos presta o apoio necessário.

O SR. DEPUTADO ESPERIDIÃO AMIN - Onde estudou? Quem que lhe formou? Quem que lhe deu formação?

O SR. STÊNIO SANTOS - Então, eu tenho formação em Direito, na Universidade Federal do Maranhão; tenho especialização em Ciências Criminais; tenho especialização em Ciências Policiais; tenho mestrado em Ciências Policiais, esse último no Instituto Superior de Ciências Policiais e Segurança Interna em Lisboa, Portugal.

O SR. DEPUTADO ESPERIDIÃO AMIN - Na parte de crimes cibernéticos?

O SR. STÊNIO SANTOS - No caso de crime cibernético, a Polícia Federal tem a nossa Academia Nacional de Polícia, tem as unidades especializadas e há as cooperações policiais internacionais. Então, vamos obtendo experiência de outros países.

(Intervenção fora do microfone. Ininteligível.)

O SR. STÊNIO SANTOS - Como?

O SR. DEPUTADO ESPERIDIÃO AMIN - Estudou fora daqui também?

O SR. STÊNIO SANTOS - O mestrado foi feito em Portugal, e também fizemos treinamento em outros países.

O SR. DEPUTADO ESPERIDIÃO AMIN - Por exemplo?

O SR. STÊNIO SANTOS - Por exemplo, FBI.

O SR. ELMER COELHO VICENTE - Bom, iniciando a questão da obtenção do dado cadastral pelo IP, se a judicialização atrapalha, a minha opinião é que retarda, e muito, a investigação. Ela transfere para o Judiciário um controle que ele vai ter, porque esse pedido de dado cadastral é feito dentro do inquérito. O inquérito é um instrumento amplamente controlado, tanto *externa corporis*, pelo Ministério Público Federal, como pela Corregedoria da Polícia Federal. Então, não há muito espaço para desvios, pedidos fora da investigação.

A própria empresa, quando exige alguns dados mínimos para que ela forneça a resposta, um dos principais dados é qual o número da investigação. Ela quer ter a certeza de que se trata de uma investigação oficial, institucionalizada, e que vai passar sob o crivo de todos os controles.

O debate se distanciou um pouco da verdadeira natureza jurídica do IP. Se você está na rua e o policial tem suspeita de que um determinado carro está envolvido em uma atividade criminosa, ele tem acesso, tem como saber quem é o proprietário daquele veículo através da placa? Tem. Então, o número vai lhe dar uma pessoa. Se um policial na rua considera que aquela pessoa é suspeita, ele pode fazer uma abordagem e pedir o documento para aquela pessoa? Com certeza, — *"seu documento, por gentileza"* —, e fazer a checagem. Agora, imaginem se estivéssemos na rua, víssemos um carro e falássemos assim: *"espera; vamos pedir para o juiz para saber de quem é aquele carro"*, para saber se a gente pode continuar na nossa atividade de repressão ou prevenção do crime. Estamos na rua. A pessoa está andando; o carro está indo embora. Imaginem se falássemos assim: *"Não, não, não, acompanha* — se você conseguir — *porque eu vou ter que pedir para o juiz autorização para saber quem é".* Então, esse comparativo tem que se ter em mente sempre quando se leva para a questão do IP.

Os abusos vão existir sempre porque somos seres humanos, em qualquer instância, e eles têm que ser profundamente repreendidos para que uma mácula não

contamine todo o sistema e prejudique a eficácia do processo que venha a ser estabelecido a bem da sociedade.

Sobre a capacitação, como o Dr. Stênio, a minha formação é jurídica e, na parte de crime cibernético, foi individual, caminhando sozinho. Sou um curioso e, às vezes, quando tropeçava em algumas dificuldades, procurava algum curso extracurricular, mas só de grandes... Isso foi no começo, porque depois que se pega uma certa experiência, a capacitação individual, a busca por um conteúdo, procurar uma orientação nos cursos a distância, isso é bem proveitoso.

O SR. CARLOS EDUARDO MIGUEL SOBRAL - Sobre as Forças Armadas e a segurança da Copa, a segurança cibernética... Para a Copa do Mundo, foi montada o que a Secretaria e o Governo chamaram de Matriz de Responsabilidades. Então, se definiu qual o papel de cada instituição dentro da promoção da segurança pública e da defesa nacional para os grandes eventos — Copa do Mundo, Olimpíadas. Essa liderança não significa uma atuação isolada; significa uma liderança no processo, que trabalha em coordenação e cooperação com as várias outras instituições do Estado brasileiro.

No campo da segurança cibernética, como o enfoque era a proteção das infraestruturas estratégicas do País — sistema de energia, transporte, aeroportos, enfim, sistemas estratégicos da Nação —, a liderança da promoção da segurança coube ao Exército Brasileiro, que montou uma unidade, o CDCiber, que é o Centro de Defesa Cibernética, para liderar o processo de defesa e segurança cibernética, e a Polícia Federal atuou nesse processo. A Polícia Federal montou um centro de segurança cibernética, que atuava em coordenação, em parceria com o Exército Brasileiro.

O Exército Brasileiro teria a responsabilidade de realizar investigação criminal, combater crimes, fraudes, pornografia, invasão de sistemas que não fossem das estruturas estratégicas na qualidade de proteção? Não. Essa atribuição sempre coube à Polícia Federal, e era realizado no nosso centro de segurança cibernética. Então, o Exército promovia a política de proteção das informações e a Polícia Federal atuava com inteligência e investigação as ações contra a infraestrutura estratégica, mas também crimes normais, crimes comuns, como fraudes, pornografia, crimes contra a honra, enfim, toda a gama de crimes que competem à

Polícia Federal. Se não fossem da nossa competência, se não fosse de competência federal, isso seria repassado, como se repassou, à Polícia Civil.

Então, essa foi a estrutura, a governança da segurança cibernética para grandes eventos. E hoje atuamos cada uma na sua atribuição: a Polícia com a sua área de crime cibernético, segurança cibernética, chefiada pelo Dr. Elmer, e o Exército com o CDCiber, que promove a proteção, em âmbito nacional, contra invasões estrangeiras, ações militares, e também desenvolve políticas de proteção da informação junto com o GSI, o Departamento de Segurança da Informação e Comunicação do GSI, e junto também com a Polícia Federal, atuando de forma conjunta.

Essa é a estrutura da proteção da informação e das estruturas estratégicas no País. Espero que tenha...

O SR. DEPUTADO ESPERIDIÃO AMIN - Formação.

O SR. CARLOS EDUARDO MIGUEL SOBRAL - Formação. Eu sou formado em Direito, me formei na Universidade de Ribeirão Preto, em 1999, e quando vim a Brasília, em 2007, participei de uma especialização de 2 anos, na Universidade de Brasília, promovida pelo GSI, pelo DSIC, para a formação de gestores da segurança da informação.

Além dessa especialização na Universidade de Brasília, nós tivemos a oportunidade, nesses 7 anos em que ficamos na área, de participar de diversos cursos, palestras, tanto nacionais como internacionais, como, por exemplo, do FBI, da ICE, que é a agência de imigração e alfândega dos Estados Unidos, a qual cuida da pornografia infantil extraterritorial daquele país; do Serviço Secreto, que cuida das fraudes bancárias; da INTERPOL, da Rede Nacional de Ensino e Pesquisa, que é um instituto do Governo Federal que promove capacitação; da EUROPOL; cursos da Polícia Montada do Canadá, uma referência na proteção à infância e à juventude; da OEA — Organização dos Estados Americanos, que promove também ações de segurança cibernética, junto com o CICTE — Comitê Interamericano Contra o Terrorismo — e com a REMJA — Reuniões de Ministros da Justiça e de Outros Ministros ou Procuradores-Gerais das Américas, que são duas estruturas da OEA; da Polícia espanhola, tanto a Polícia Civil quanto a Polícia Nacional Espanhola, que também são referência no combate aos crimes cibernéticos. Fui um dos doze

representantes brasileiros no estudo da ONU sobre crimes cibernéticos, realizado pela UNODC — Escritório das Nações Unidas sobre Drogas e Crime, sediado em Viena, nos anos de 2011 e 2012; participei também, representando a Polícia Federal, no IGF, que é o Fórum de Governança da Internet da ONU, em cinco oportunidades, e também das discussões sobre a Convenção de Budapeste e outras ações promovidas pelo Conselho da Europa, de 2008 a 2013.

Essas são, que me lembre, minhas capacitações. Eu tive muita oportunidade de qualificação dentro da Polícia Federal.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Sra. Presidente, aqui...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Pois não, Delegado Éder.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Como se iniciou a Ordem do Dia e como pode haver coincidência nas perguntas dos colegas Deputados, eu queria sugerir à Mesa que os colegas fizessem as perguntas pela ordem de inscrição, que todos falassem fazendo as suas perguntas, os palestrantes anotavam e respondiam em seguida.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Ótimo. Vamos fazer, então, esse primeiro bloco com os Sub-Relatores, depois abrimos para os autores dos requerimentos e para os membros, e fazemos blocos desses segmentos.

Agora com a palavra o Deputado Daniel Coelho, Sub-Relator.

O SR. DEPUTADO DANIEL COELHO - Sra. Presidente, Deputada Mariana Carvalho, Srs. Elmer, Stênio, Carlos Eduardo, Deputado Esperidião Amin, Sras. e Srs. Deputados, primeiro, eu gostaria de parabenizar a todos. Tinha aqui uma lista grande de perguntas e indagações a fazer porque esperava, inclusive, que fôssemos falar, em específico, apenas do caso IB2K, que não é necessariamente a única pauta que nós vamos ter na CPI, mas os senhores expositores já nos deram a oportunidade de avançar um pouco mais em outros temas que vão ser extremamente importantes ao longo dos trabalhos desta Comissão. Muitas das perguntas, inclusive, começam a ser esclarecidas.

Eu acho que esta audiência, Deputada Mariana, vai dar a base para os trabalhos desta CPI. Começamos a ter aqui um pouco também da leitura da Polícia Federal sobre todos os crimes que ocorrem no mundo virtual.

Na instalação da CPI, ao usar da palavra, cheguei a fazer o comentário de que não é tão difícil determinar o que é crime no mundo virtual. Se uma prática é crime no mundo físico e ela ocorre no mundo virtual, ela é um crime cibernético. Então, por exemplo, se o racismo é crime no Código Penal brasileiro, ele vai ser crime também no mundo virtual. Não há dificuldade nessa compreensão.

Pelas exposições feitas pelos senhores... E eu acho que o Deputado Esperidião Amin, Relator da CPI, ele coloca de forma correta, no início da sua fala, que esta CPI vai olhar para trás, para tentar punir casos já ocorridos, mas também tem que olhar para frente, tem que olhar para o futuro. E é nesse sentido que eu faço a sugestão à Presidente, Deputada Mariana, de que possamos aprofundar a conversa com os representantes da Polícia Federal no sentido de estudar que aperfeiçoamento é possível ser feito na legislação.

Por exemplo, o Dr. Elmer disse que há uma lentidão ao identificar os IPs daquelas pessoas que estão cometendo, principalmente, crimes contra a honra, de pedofilia, de racismo, que estão presentes de forma aberta na Internet, mas efetivamente há uma dificuldade de fiscalizar isso. Então, é importante buscar mais agilidade.

Para mim ficou muito claro que essa falta de agilidade ela contribui para a impunidade. No momento em que há uma demora muito grande para identificar um IP, dá tempo, inclusive de o agressor, de o criminoso fechar aquela conta e abrir outra; ele atua em um Estado e, daqui a pouco, ele está em outro, ele está no exterior. Quer dizer, é impossível rastrear se não se tem agilidade, ainda mais nesse mundo virtual.

Ficou muito claro aqui, pela fala do Dr. Carlos Eduardo, que há dificuldades de estrutura. Eu acho que seria importante também para a Câmara dos Deputados termos a informação de quantos profissionais hoje estão dedicados aos crimes virtuais, se temos problemas de contingenciamento no orçamento para esse tipo de fiscalização — porque eu acho que cabe também ao Congresso Nacional discutir orçamento especificamente para o combate aos crimes cibernéticos. Não podemos ficar com essa sensação de que o crime compensa. É evidente que é muito difícil a fiscalização da Internet pela sua própria característica. Ela é transnacional; há a dificuldade de o crime poder ser cometido em qualquer país do mundo e acontecer,

do ponto de vista virtual, em território brasileiro. Então, são evidentes as dificuldades. Mas não é por isso que vamos desistir ou deixar de fiscalizar e de fazer as cobranças.

Uma das questões que eu gostaria de abordar e não foi abordada ainda, e eu queria um comentário dos expositores. A legislação atual, e isso vem da chamada Lei Carolina Dieckmann, fala que os provedores devem guardar as informações com prazo determinado de apenas 6 meses. Isso já é apontado por alguns como uma dificuldade na fiscalização, porque se há essa lentidão da judicialização para se obter um IP e se o provedor não é obrigado a guardar os dados por um prazo mais longo — 3, 4, 5 anos —, isso resulta numa dificuldade de se identificar principalmente nos crimes de pedofilia, onde há uma utilização, já comentada, da nuvem para guardar essa informação. A nuvem já é transnacional, já está normalmente no exterior, e se não houver a obrigação local de guardar essas informações, isso dificulta, e bastante, a fiscalização.

Também gostaria de um comentário em relação às técnicas e às tecnologias hoje possíveis para mascarar os IPs. Sabemos que quando o crime cibernético é feito de forma mais organizada e planejada, dificilmente o criminoso utiliza o computador doméstico e o seu próprio IP Ele, além de tentar utilizar técnicas para mascarar o seu IP, vai tentar também utilizar pontos abertos de *wi-fi*, *lan houses.* Ele vai tentar, além de mascarar o IP, também não utilizar o seu próprio equipamento. Como podemos identificar, nesses casos, o agressor?

E também mais um comentário...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Só para concluir.

O SR. DEPUTADO DANIEL COELHO - Vou concluir, Sra. Presidente.

Também foi comentado aqui que cabe à Polícia Federal a proteção das redes do Governo, mas gostaria de registrar a importância da fiscalização das redes do Governo, seja a Câmara dos Deputados, o Senado, o Executivo Federal, Estadual e Municipal.

Há dois casos que, inclusive, vão ser debatidos por esta CPI: o do jornalista Carlos Sardenberg e da jornalista Miriam Leitão, que sofreram agressões na Internet, e essas agressões elas foram provenientes do Palácio do Planalto.

Então, é importante também que haja fiscalização do próprio Governo. Se nós não podemos admitir os crimes contra a honra partindo de indivíduos, muito menos podemos permitir isso partindo do próprio Governo, que tem que dar o exemplo.

Finalizando, eu deixo uma pergunta bem específica: se temos estatísticas da quantidade de crimes cibernéticos. Eu sei que isso é muito complexo, mas apenas para nos nortear, pergunto se há algum tipo de estatística de crimes e do que se consegue solucionar; considerando a dificuldade estrutural, mas o que é que foi solucionado nesse período.

No mais, eu queria parabenizar os três expositores, porque percebemos a dedicação e o amor com que tratam o tema. Então, ficamos satisfeitos ao ver que há um núcleo na Polícia Federal preocupado com o crime cibernético.

Eu peço desculpa por extrapolar o tempo.

O SR. DEPUTADO JEAN WYLLYS - Sra. Presidenta, eu tenho que sair agora para gravar o *Havana Connection*. Se V.Exa. concordar, eu poderia deixar as minhas perguntas. Não vou ficar para ouvir as respostas — a Lizi vai anotar, mas eu gostaria de fazer as perguntas porque o companheiro não vai conseguir elaborar da maneira como eu vou fazer. Serei bem breve, se possível.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Temos, na frente o bloco dos autores dos requerimentos, os Sub-Relatores.

O SR. DEPUTADO RODRIGO MARTINS - De minha parte, não tem problema, Sra. Presidente.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Se os Sub-Relatores não...

O SR. DEPUTADO RODRIGO MARTINS - De minha parte, não tem problema.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Deputados João Arruda, Deputado Delegado Eder, Delegado Alexandre...

O SR. DEPUTADO LEO DE BRITO - Sou autor também. Da minha parte, acato.

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

O SR. DEPUTADO JOÃO ARRUDA - Hoje, tudo bem. Mas é uma coisa que não pode ser. Todos nós temos compromisso. Estamos esperando aqui há 2 horas.

O SR. DEPUTADO JEAN WYLLYS - Não, Deputado, estou pedindo, estou pedindo a...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Eu estou até pedindo a opinião aqui de todos. Se todos concordarem com essa exceção... Mas que não se repita nas próximas também.

O SR. DEPUTADO JEAN WYLLYS - Em caráter de exceção, porque, como eu falei para V.Exa., eu vou gravar. Então, não tem...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Se todos concordarem...

(Não identificado) - Já dava tempo de ter feito.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Com a palavra o Deputado Jean Wyllys.

O SR. DEPUTADO JEAN WYLLYS - Bom, obrigado, Sra. Presidente e aos demais que concordaram com que eu fizesse as perguntas.

As minhas perguntas são dirigidas ao Dr. Carlos e ao Dr. Elmer, especificamente.

O Dr. Elmer falou da necessidade, reclamou da judicialização. Mas nós tivemos uma conquista importante no Marco Civil da Internet, que tem a ver com a privacidade do usuário, com a liberdade de expressão. Então, eu não acho que tenhamos que retroceder em relação a essas conquistas. E mesmo a comparação feita, da placa do carro, com o ambiente virtual é uma comparação que não se justifica, na medida em que no ambiente real nós não temos os mecanismos de propagação imediata e veloz que podem destruir reputações, como temos na Internet.

Esse é um primeiro ponto: acho grave se reclamar de que a Justiça, apenas a Justiça, conceda as informações, porque para mim isso atenta contra a privacidade, que é o que conquistamos, e contra a liberdade de expressão. E olha que quem está falando aqui é uma pessoa que é, todos os dias, difamado nas redes sociais por uma série de mentiras e calúnias feitas. Então, mesmo eu sendo vítima desses crimes, eu não sou a favor de que se solape esse direito à privacidade e à liberdade de expressão.

Acho que também nós corremos um risco, assim... Porque há sempre vazamentos seletivos. sabemos disso, não é? Há sempre vazamentos de dados. A própria polícia se encarrega disso, de vazar seletivamente de dados, e sabemos que esses vazamentos podem, sim, destruir reputações antes mesmo que se prove a culpa ou não das pessoas. Temos sempre que manter as garantias jurídicas e a presunção de inocência. Isso é importante.

O Dr. Carlos falou da dificuldade de localizar IPs, determinados *sites*, a origem de determinados *sites,* porque estão hospedados em computadores ou base de dados fora do País. Há as questões legais, de soberania, que não podem ser vencidas de imediato. Porém, eu acredito que a polícia dispõe de outros mecanismos de investigação e da possiblidade de interpelar outras pessoas que não as pessoas que deram origem ao conteúdo. Por exemplo, os senhores podem não localizar o IP que deu origem a um conteúdo criminoso, mas sabem que existem figuras-chaves, que são fundamentais no compartilhamento, que, em geral, botam a cara, que não se escondem.

Por exemplo, identificamos que aqui na Casa há inclusive Deputados Federais — e não um, nem dois, nem três —, em seus gabinetes, em seus computadores, responsáveis por propagação de calúnias, difamação e outros crimes.

Então, se não se acha a origem do vídeo fraudado; a origem da mensagem homofóbica, xenofóbica, de ataque a lésbicas, enfim, se não acha a origem desse conteúdo, se acha quem propagou, quem foram os primeiros a propagar abertamente. A polícia não pode interpelar essas pessoas? Nós não dispomos, não há dispositivos legais que possam arrolá-las como cúmplices desses crimes, ainda que não sejam os criadores originais do conteúdo? Essa é uma pergunta a ser feita.

Nas denúncias que eu fiz à Polícia Federal, eu dei um conjunto de dados e de relações entre diferentes perfis que têm relações entre si e que são sempre responsáveis por propagação desses conteúdos. A pergunta é: essas pessoas não podem ser interpeladas sequer a prestar depoimento sobre de onde veio esse conteúdo, como é que foi parar no computador delas?

Essas são as minhas duas perguntas.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Eu vou passar para as respostas, já que está havendo votação nominal, enquanto os outros Deputados voltam, para podermos encerrar e fazer mais um bloco.

O SR. STÊNIO SANTOS - Como não foram direcionadas, vou tentar dar uma resposta que contemple algumas das questões do Deputado Daniel Coelho.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Eu pediria, se possível, que o senhor respondesse primeiro às perguntas do Deputado Jean Wyllys e, depois, às do Deputado Daniel Coelho.

O SR. ELMER COELHO VICENTE - Excelência, a sua pergunta é fantástica, porque trata do eterno debate sobre a privacidade nos *logs*. Sabemos que a privacidade deve sempre ser protegida, e que as conquistas, ao longo da história dessa proteção ao cidadão, principalmente da proteção contra as ações do Estado, devem ser protegidas e mantidas. É uma conquista da sociedade. Contudo, nenhum direito é absoluto. Vemos isso na própria discussão sobre o sigilo telefônico, a liberdade.

Na questão específica dos *logs,* eu acho que merece um aprofundamento a definição do que é privacidade e se o *log* representa uma esfera de privacidade do indivíduo. Porque eu já sei o que ele fez na Internet; eu já sei o ato, eu já sei que ele frequenta determinado *site*, eu já sei que ele proferiu determinada palavra. Agora, só a identificação da pessoa já é uma lesão à privacidade?

Sobre os vazamentos, isso sempre vai ocorrer. Veja que há vazamento de grampos. Então, isso independe de haver autorização judicial ou não haver autorização judicial. Eu acho que temos que pensar, na verdade, em dar uma resposta para a sociedade que não vimos dando.

Esse assolamento de apreciações do Judiciário retarda inclusive a decisão final do processo. Eu acho que tem que se ver a questão da privacidade, que foi muito discutida no Marco Civil, mas, de novo, como o senhor falou, às vezes, a pessoa é identificada não só pelo IP.

Sobre o fato de que não se pode chegar à origem, ou a quem propagou, realmente, a pessoa pode ser penalmente responsável. Tem que haver uma análise casuística do crime e do dolo, mas, com certeza, o caso deve ser submetido à análise do Judiciário para ver se aquela conduta é criminosa.

O SR. STÊNIO SANTOS - Quero fazer um adendo em relação à privacidade, porque há uma má compreensão do que é o *log*. Acho que esse foi o problema maior.

O que é esse *log* do qual estamos falando? É o endereço IP com a data, a hora e o fuso horário. Então, não estamos falando de conteúdo de privacidade, do que o sujeito fez e com quem ele conversou. Nada disso é pedido. O que estamos querendo saber é um dado que, na verdade, revela a conexão de uma máquina com outra na Internet. Esse dado vai simplesmente indicar não quem é o suspeito do crime, mas quem é o responsável pela conexão. Mesmo quando o provedor do serviço de conexão à Internet informa o nome com endereço, vai informar quem é o responsável por aquela conexão. Uma série de outros procedimentos tem que ser feita depois disso para podermos imputar a responsabilidade a alguém.

O Deputado Esperidião Amin comentou sobre a rede aberta. O sujeito é dono da conexão e deixou a rede *wireless*, sem fio, aberta. Veio um terceiro e usou aquela conexão. Então, a polícia não vai tomar nenhuma medida em relação a essa pessoa sem antes averiguar quem efetivamente foi responsável por aquilo, mas se não tivermos essa medida, não vamos chegar ao culpado.

O senhor foi vítima, mas às vezes não conseguimos chegar ao culpado porque não obtivemos o *log*. Para pedir o *log*, o Marco Civil determina um prazo. Às vezes, o pedido chega, vai para uma pessoa que não é exatamente a que vai responder por aquilo... Quer dizer, existe uma burocracia nesse trâmite, e, quando chega a hora de instaurar o inquérito, já passou o prazo do Marco Civil. Ao passar esse prazo, se pede, por via judicial ou diretamente, e a resposta do provedor é que já passou xis tempo, não tem mais o *log*, já foi apagado.

Há situações excepcionais para as quais não vamos depender do IP, mas há muitas que vão depender do IP. Do contrário, a investigação já nasce morta. Quer dizer, não tem IP, não existem outros elementos, arquive-se. Aí o criminoso vai continuar praticando essa conduta em prejuízo da sociedade.

É uma discussão rica, mas vamos ter que escolher: muita privacidade, menos segurança, e muita segurança também é um equívoco. Temos que achar um equilíbrio, porque, quando se vê as estatísticas, a impressão é de que o criminoso está vencendo a luta.

Era isso é que eu queria colocar. Obrigado.

O SR. PRESIDENTE (Deputado Leo de Brito) - Com a palavra o Sr. Carlos Eduardo.

O SR. CARLOS EDUARDO MIGUEL SOBRAL - Eu queria dar uma breve contribuição sobre a questão do acesso a dados cadastrais, para deixar uma visão muito clara.

Eu acredito que ninguém defende que o nosso País institua a mesma metodologia ou sistemática que ouvimos falar que aconteceu nos Estados Unidos no caso da NSA, onde se tem acesso a dados cadastrais e *logs* de todo o mundo, de toda situação, de toda circunstância para, a partir desses dados, minerar e encontrar criminosos. Acredito que ninguém pensa em fazer isso no País. É uma coisa que, particularmente, acho que é impossível, inviável, indesejável, e ofenderia todos os princípios de direitos humanos e de privacidade que todos nós defendemos. O debate é se, numa investigação específica, cujo conteúdo já seja conhecido, seria possível à autoridade policial, ao delegado de polícia, ter acesso a essa informação num procedimento formal, que vai ser depois controlado pelo juiz e pelo Ministério Público. Inclusive, se houver algum tipo de abuso, a pena para a autoridade normalmente é maior do que a do crime investigado.

Nesse cenário é que se promove esse debate, que é sensível, é polêmico. Nós passamos os últimos 10 anos discutindo. O Marco Civil deu um norte e há posições favoráveis e contrárias. É um debate que segue vivo.

Sobre a outra pergunta, Deputado, é muito difícil falar em termos gerais de casos específicos. É fato: quando nós tratamos de crimes em quadrilha, temos um facilitador, apesar de todas as dificuldades. O facilitador é que os crimes continuam acontecendo, e são vários crimes. Se nós, porventura, perdermos uma informação em determinado momento, nós temos a oportunidade de rastrear o grupo criminoso através de outras informações disponíveis. Então, apesar da dificuldade de ser um crime organizado, há a facilidade de o crime ser contemporâneo, de estar acontecendo. Isso facilita a investigação.

Como tratamos normalmente de crimes contra a honra, difamação, injúria e calúnia, o crime é um ato isolado, único, no passado, e a possibilidade de se reconstruir o passado é muito mais difícil do que a de se investigar algo que

acontece no presente. Por isso, no caso de investigações de crimes praticados no passado, qualquer informação perdida pode ser fundamental e essencial para a investigação. Se nós perdermos uma informação, pode ser que não cheguemos ao culpado, apesar de, no caso concreto, tentar se buscar outros caminhos.

Para tudo que acontece na Internet nós temos que ter uma cautela a mais, porque o meu dispositivo pode ser invadido remotamente — isso acontece, e acontece de forma muito comum. Quando a informação chega até nós, a primeira alegação da pessoa é esta: *"O meu dispositivo foi invadido, e na invasão ele praticou um crime contra a honra"*. Então, isso gera, na presunção de inocência, a obrigação de o Estado provar que aquela pessoa que detém o dispositivo foi efetivamente quem o utilizou; que não foi um terceiro que pegou o computador, o *tablet* ou o celular e fez a propagação do pensamento de forma indevida. Por isso nós temos a obrigação de provar que aquela pessoa, naquela data, naquele horário fez a comunicação que imputamos ilegal.

Esses detalhes, na prática, são complicadores da investigação. Se a pessoa que fez a comunicação para cometer um crime contra a honra usou uma técnica como a rede Tor, por exemplo — que é uma rede de anonimato de conexão, que nasceu como proteção da privacidade e é utilizada para proteção em regimes de exceção, mas também é usada por criminosos para a prática de ilícitos —, e nós não tivermos outro mecanismo para perseguir a comunicação, realmente, dificultará bastante.

É lógico que, no crime concreto, pode ser que haja suspeitos, às vezes, a vítima desconfia de alguém, e nós vamos fazer uma investigação para apurar se pode ser. Se for possível, vamos aprofundar, ouvir pessoas, fazer buscas, fazer perícia em documento apreendido; é possível, mas nada é 100%. Pode ser que, efetivamente, aquela comunicação perdida pelo IP represente o fim da investigação, pode ser que não, mas que é um dificultador, é.

A responsabilidade de quem compartilha um pensamento ilícito passa pela análise do dolo, do *animus* de difamar, de injuriar e de caluniar, que também deve ser apurado no fato concreto. Nós temos responsabilidade sobre aquilo que publicamos e aquilo que compartilhamos. Na esfera cível, a responsabilidade é mais simples de ser configurada, porque a culpa é suficiente para a responsabilização; na

esfera penal, não. Na esfera penal, nós temos que ter o dolo. Na esfera cível, se se compartilha algo ofensivo, se é responsabilizado com indenização. Se não se adotou mecanismos para apurar se aquele conhecimento é verdadeiro ou se ofendeu outra pessoa, se é obrigado a indenizar. Mas, na esfera penal, temos que provar que a pessoa teve a vontade de divulgar um pensamento criminoso, calunioso, injurioso ou difamatório. Então, há essas vertentes, mas isso é enfrentado...

O SR. DEPUTADO JEAN WYLLYS - Quando se trata de uma autoridade da República, ele tem responsabilidades no papel que cumpre ao usar seus espaços, seus perfis públicos para isso. Ainda assim?

O SR. CARLOS EDUARDO MIGUEL SOBRAL - O caso a caso tem que ser apurado. É difícil falar em tese, em geral, pensando num caso concreto, Deputado.

O SR. PRESIDENTE (Deputado Leo de Brito) - Obrigado, Dr. Carlos.

Concedo a palavra ao Sub-Relator Deputado Sandro Alex.

O SR. DEPUTADO SANDRO ALEX - Obrigado, Sr. Presidente. Cumprimento o Relator Esperidião Amin, o Dr. Stênio, o Dr. Elmer e o Dr. Sobral, a quem agradeço pela presença aqui na nossa CPI.

Aliás, o primeiro trabalho que eu fiz no mandato anterior foi com o Dr. Sobral. Eu era Presidente da Frente Parlamentar de Combate a Crimes na Internet e, naquele momento, estávamos ainda discutindo a legislação sobre a qual hoje os senhores estão debatendo conosco, como Lei Carolina Dieckmann e o Marco Civil, na Comissão que o nosso companheiro João Arruda presidiu.

Naquele momento, a dificuldade que tínhamos na audiência pública era que a Polícia Federal fazia a solicitação desses *logs* e a empresa atendia se quisesse, porque poderia dizer que não tinha. Ela não era obrigada a guardar. É claro que todos nós sabíamos que ela guardava até para uso comercial, mas isso não era obrigatório. E nós iniciamos um trabalho cuja discussão era justamente sobre liberdade de expressão, privacidade e investigação. Inicialmente, nós defendíamos o *log* de conexão, porque, naquele momento, nem o da conexão era permitido. Alguns partidos e Parlamentares trabalhavam em contrário, dizendo que, se nós guardássemos a conexão, já estaríamos invadindo a privacidade. Quando eu defendi no Marco Civil os aplicativos, se não se tem o *log* do aplicativo, pode-se ter o da conexão, mas não o da aplicação.

Foi uma batalha até o final — o Deputado João Arruda sabe disso —, mas nós conseguimos vencer e incluir no Marco Civil a guarda dos *logs* de aplicação. Inicialmente, nós pedimos mais de 1 ano, mas isso não foi possível dentro do acordo, e é o questionamento que faço: esses 6 meses já não comprometem pela dificuldade que nós temos de acelerar o processo, enfim, a demora do processo já não está comprometendo o fato de termos apenas 6 meses da guarda, prazo que pretendíamos fosse muito maior?

Outra coisa que eu gostaria de colocar: Dr. Stênio, quantos profissionais da Polícia Federal trabalham na repressão aos crimes cibernéticos no País? Qual é o tamanho do efetivo que temos para trabalhar contra essas quadrilhas que atuam atrás de um computador? Os senhores nos falaram que é insuficiente. Quantos profissionais atuam nessa área no País na Polícia Federal?

Dr. Elmer, o senhor se referiu aqui à força-tarefa contra a pornografia infantil no País, um trabalho conjunto para o combate, ainda que extrajudicialmente...

E faço até um parêntese: defendo que a Polícia Federal tenha o acesso; que isso não precisasse ser feito judicialmente — não conseguimos isso no Marco Civil, fomos voto vencido —, mas defendo que a autoridade constituída também é a Polícia Federal, que está na investigação, e isso não tem a ver com liberdade de expressão. Ninguém impede ninguém de escrever ou praticar qualquer ato na Internet. Nós estamos falando em investigação.

Mas, enfim, o senhor anunciou que fez uma força-tarefa e que, no diálogo com empresas, com operadoras, elas não foram, enfim, elas não auxiliaram o trabalho da Polícia Federal.

Nós estamos falando aqui de pornografia infantil no País. Então, eu pergunto objetivamente: quais foram as empresas que não auxiliaram a Polícia Federal no combate à pornografia infantil, ainda que de forma extrajudicial? Quais foram pontualmente? Nós queremos, na CPI, neste momento saber quais foram as empresas.

Dr. Sobral, entre alguns relatos que V.Sa. fez sobre os crimes contra o sistema financeiro, nos trouxe um levantamento de 1 bilhão, mas, em números do ano de 2011, 2009. O senhor tem a informação atual do tamanho, da soma de recursos envolvidos nos crimes contra o sistema financeiro? O senhor tem

conhecimento, através do trabalho que faz não sei se é com a FEBRABAN, mas, enfim, com o sistema financeiro, de qual é o tamanho, qual é a soma dos crimes contra o sistema financeiro — inclusive V.Sa. disse que isso é pago pelo próprio usuário? O senhor disse que esse 1 bilhão está sendo pago pelo próprio usuário. Então, eu gostaria que o senhor se aprofundasse sobre isso.

Também quero fazer aqui um destaque sobre a vingança pornô. Parece-me que, ainda no Marco Civil, o cidadão pode solicitar à empresa que retire; não é necessário que isso passe pela Justiça. Ele pede à empresa que retire imediatamente aquela imagem, que é sua, e a empresa é obrigada a retirar. Foi um bom trabalho que fizemos lá no Marco Civil. Esse encaminhamento deveria se dar também para outros crimes, segundo o que V.Sas. acreditam ser benéfico?

Obrigado, Sra. Presidente. Obrigado, Relator.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Para fechar e concluir esse bloco dos Sub-Relatores, com a palavra Deputado Rodrigo Martins.

O SR. DEPUTADO RODRIGO MARTINS - Obrigado, Presidenta.

Primeiro, quero externar que a nossa vontade nesta CPI é que, ao término, além do relatório, nós tenhamos conseguido melhorar a legislação do ponto de vista do combate e prevenção do crime cibernético.

Eu, mais especificamente, fiquei na Sub-Relatoria de Segurança, e ouvi o Dr. Stênio falando que cerca de 20% das pessoas que recebem um e-mail falso ou algum tipo de aliciamento tendem a cair no golpe. Eu pergunto se esse dado é atual, se está atualizado, ou se é um dado antigo.

Também faço aqui uma pergunta aos três — os três são reconhecidos, competentes na área. Qual é, hoje, a maior dificuldade em relação à segurança cibernética? É o fato de não dispormos de estrutura para combater esse tipo de crime? É a própria dificuldade por conta de alguma legislação ou por conta de alguns avanços tecnológicos em que esses criminosos estão à frente?

Também queria fazer uma pergunta sobre tempo. Sei que cada caso é um caso, mas vamos falar sobre o caso de calúnia ou de difamação na Internet. Do momento em que se recebe a denúncia até o momento em que é concluída a investigação, transcorre quanto tempo, hoje? Existe uma morosidade muito grande da Justiça no sentido de liberar o IP ou dados referentes àquele IP?

Eram essas as considerações.

O Bruno fez algumas considerações sobre estatística, no que diz respeito à criminalidade. Quero falar da necessidade de obrigarmos as operadoras a cooperarem cada vez mais com as investigações, da possibilidade de criarmos mecanismos para facilitar o acesso a esses IPs.

Entendo eu, discordando um pouco do Deputado Jean, que buscar o IP não quer dizer que você está invadindo a privacidade. É como se você estivesse pedindo uma carteira de identidade da pessoa. Em alguns casos, iria facilitar, como no caso de flagrante delito. Iria facilitar até mesmo a conclusão e a punição de alguns culpados. Eu fico feliz em iniciar a CPI, Presidente, com uma audiência dessas, que irá realmente nos nortear na conclusão dos nossos relatórios.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Concederei a palavra ao Dr. Stênio, ao Dr. Elmer e, logo em seguida, ao Dr. Carlos, para responder o primeiro bloco do Sub-Relator.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Sra. Presidente...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Pois não, Delegado.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Como são poucos os Deputados, sugiro novamente... Vamos tentar fazer com que os Deputados façam logo as perguntas. De repente, elas coincidem com a deles, e aí os colegas palestrantes já...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Como houve as primeiras perguntas do Deputado Daniel, do Deputado Rodrigo e do Deputado Sandro, que são os nossos Sub-Relatores, vamos deixar para o próximo momento, para fazer as perguntas aos outros três que responderam as perguntas do Deputado Jean Wyllys. Logo em seguida, o outro bloco: V.Exa., Deputado Marchezan e Deputado Leo de Brito.

O SR. STÊNIO SANTOS - Vou tentar dar uma resposta que abranja o máximo possível os pontos levantados.

Um dos aspectos que eu gostaria de frisar inicialmente é que existe no País a impressão de que leis penais materiais resolvem o problema da criminalidade. Nós, tanto pela experiência prática, quanto pelas leituras, entendemos que o problema

não está na criação de um tipo penal, de uma pena, de um tipo penal secundário elevado, mas sim na efetividade da resposta estatal.

O Prof. Claus Roxin, uma das maiores autoridade em Direito Penal no mundo, falando direto da Alemanha, diz exatamente isso. Muitas vezes, criam-se leis penais pesadas. Só que o criminoso, o suspeito da conduta ilícita típica tem a mais plena convicção de que não será pego. E é exatamente essa convicção de que não será pego, não será processado que faz com que ele continue realizando a conduta ilícita típica. É exatamente a impunidade que vai gerar a estatística de criminalidade.

Então, se nós pensarmos que o que vai mudar, ou seja, o que vai reduzir a estatística são políticas que deem mais efetividade à investigação criminal e ao processo penal em sentido amplo, começaremos a pensar, vinculado a isso, nas medidas que podem ser tomadas para aperfeiçoar essa investigação.

Quando fazemos esse tipo de debate, estamos sempre trabalhando no terreno movediço, perigoso da discussão entre liberdade de expressão, privacidade e investigação eficiente, Estado mais eficiente.

Todo mundo quer que o Estado dê a resposta. Só que, muitas vezes, não se quer dar os meios para que o Estado dê a resposta. E aí se coloca a culpa na investigação criminal, coloca-se a culpa no inquérito policial, coloca-se a culpa na Justiça, no Ministério Público. Só que é preciso avaliar exatamente quais são os instrumentos disponíveis, qual é a legislação disponível, qual é o Estado Democrático de Direito que nos encontramos para poder trabalhar, também — sopesando, equilibrando direitos e garantias constitucionais —, com um direito e garantia fundamental, que é a segurança.

Para isso, senhores, eu trouxe aqui algumas proposições, algumas ações que poderiam contribuir com o Legislativo e com a sociedade, na medida em que... Quando falamos em investigação cibernética, nós temos o aspecto do IP — talvez seja o meio mais conhecido —, mas existem outros meios que estão disponíveis, que podem ser realizados e que facilitariam também a investigação. Por exemplo: todo dispositivo que se conecta na Internet possui um número, que se chama MAC Address. Esse número, em algumas conexões, é preservado. Então, muitas vezes, o provedor informa o IP e informa também o MAC Address. Esse MAC Address vai identificar um dispositivo específico. Então, se ele se conectou de um iPhone, um

MAC Address daquele iPhone foi utilizado. Isso, em uma investigação, é extremamente valioso para se definir a autoria. Se eu chego em uma rede aberta e alguém se conectou a essa rede dentro daquela residência, eu tenho o titular da conexão, mas eu tenho o MAC Address, durante a apreensão daquele material. A perícia pode identificar quais são os MAC Address de cada um dos dispositivos apreendidos, e, a partir daí, eu identifico exatamente qual foi o dispositivo utilizado. E aí eu indago: *"Quem é o responsável por esse dispositivo?" "Fulano."* Então, provavelmente, foi fulano que utilizou — se ele não emprestou para alguém.

Então, a regulamentação — isso pode ser feito por meio de legislação — na comercialização dos dispositivos... Se há uma legislação prevendo que, ao comercializar o dispositivo, ele deve armazenar, registrar o MAC Address e disponibilizar isso em uma base acessível ao órgão de investigação policial, muitas vezes, com a resposta do provedor, eu acesso a base e já sei quem está com esse dispositivo, onde ele está. Eu posso perder o endereço IP, mas pelo MAC Address, às vezes, eu vou chegar ao responsável pelo dispositivo. Essa medida poderia auxiliar na investigação.

Além disso, não adianta eu fazer uma legislação que preveja o MAC Address, que o comerciante informe em uma base vinculando o dispositivo ao MAC Address, se eu também não regular a forma de filtragem dessa conexão. Então, é possível fazer uma legislação que preveja que, quando a conexão for feita, o provedor faça esse filtragem, armazene o MAC Address vinculado ao endereço IP.

Na medida em que nós ultrapassarmos a versão atual do IP, que já está praticamente vencida — é a versão 4, o IPV4 — e passarmos a utilizar a versão 6, que é o IPV6, muitos desses problemas serão sanados, porque cada usuário da Internet poderá ter o seu próprio endereço IP. Mas, até lá, talvez essa seja uma medida paliativa.

Nesse aspecto, também acredito que o Legislativo pode colaborar, pode contribuir para dar uma reforçada nessa modificação, para que nós passemos a usar mais o endereço IP na versão 6, que é a atual, e deixemos aos poucos a versão 4, que tem trazido mais dificuldades na identificação da autoria.

Além disso, nós vemos que há um problema sério no cadastro dos domínios no NIC.br. Muitas vezes a pessoa faz o cadastro, e não se tem a confirmação de

que os dados que foram apresentados no NIC.br, lá no registro.br, são verídicos. Isso colabora com os registros de domínios falsos, utilizando-se documentação falsa. Talvez seja o caso de se tentar, também, regulamentar o cadastro desses domínios eletrônicos. Isso vai facilitar a investigação.

Há outras proposições, como, por exemplo, melhorar a questão do acesso direto às informações — não o que foi comprado com o cartão de crédito, mas onde ele foi utilizado. Se o sujeito utilizou o cartão de crédito para cometer um delito, a informação de onde foi utilizado esse cartão é muito relevante. Geralmente, quando vamos fazer uma investigação, vemos que a pessoa usou o cartão em uma loja que tem circuito fechado de televisão, que vai filmar aquela ação do sujeito pagando com o cartão clonado. Se conseguirmos ter essa informação em menos de 30 dias, é possível obter essa imagem. Então, é um dado a mais, que vai apontar exatamente quem estava usando o cartão clonado naquele momento. Passados os 30 dias, regra geral, o comércio vai responder: *"Não temos mais as imagens".* Então, seria uma medida para tentar acelerar o processo de identificação da autoria.

Um outro aspecto, também semelhante, é regulamentar o acesso direto ao local em que foi utilizado o telefone celular. O sujeito está fazendo ligação, e, muitas vezes, temos como localizá-lo pela Estação Rádio Base — ERB. Só que isso, muitas vezes, demora muito tempo, principalmente se o pedido tiver que ser feito por via judicial.

Nesse intervalo de tempo, se for necessária uma medida mais contundente, mais rápida, principalmente em casos que envolvem, por exemplo, violência sexual contra crianças e adolescentes... Por exemplo, a criança está sendo vítima de abuso — temos essa informação por *e-mail. S*e tivermos a informação de onde está o sujeito, é possível deslocar uma equipe exatamente para o local e fazer cessar aquela violência.

Em 2010, salvo engano, nós conseguimos fazer uma operação, que foi nomeada Operação 24 Horas. Vieram informações por *e-mail* de que estava sendo abusada uma criança de 6, 7 anos, na época. Vieram as imagens no *e-mail* e alguns dados que permitiram a localização por outros meios. Mas, para conseguir isso, a equipe teve que parar tudo o que estava fazendo, e todo mundo teve de focar na identificação do sujeito.

Quando é um caso, a polícia consegue fazer isso. Mas, quando são 100, 200, 300... Em São Paulo e no Rio de Janeiro, 700 casos são investigados simultaneamente. Não é possível dar o tratamento que a Constituição exige. A Constituição Federal exige que, no caso de pornografia infantil, haja prioridade absoluta. Mas isso não é possível, se você tem 700 casos prioritários. Então, precisamos tentar averiguar da forma mais célere, diminuir um pouco esse trâmite de burocracia, para poder dar uma resposta que a sociedade precisa e merece.

Dentro, ainda, desse aspecto, uma dificuldade que estamos tendo é na interpretação das legislações que foram produzidas por essas Casas Legislativas. Então, a Lei nº 9.613, de 1998, a Lei nº 12.850, de 2013 — a Lei 9.613/98 é a que fala de lavagem de ativos; a Lei 12.850/13, de crime organizado, o próprio Marco Civil da Internet —, todas essas legislações vêm reiterando — isso me parece bem claro — que o Poder Legislativo quer que a autoridade policial tenha celeridade na investigação e, com isso, efetividade e eficiência.

Só que há uma interpretação das empresas no sentido de que esse poder de requisitar dados cadastrais só vale para as condutas ilícitas típicas vinculadas a essas leis. Então, há um entendimento generalizado, que não é o da Polícia Federal, de que, se a requisição de dado cadastral está na Lei 9.613/98, eu só posso pedir dado cadastral de crime envolvendo lavagem de ativo. Se a requisição está na lei de combate à organização criminosa, eu só posso requisitar dados cadastrais quando o crime envolver organização criminosa. Esse entendimento tem prejudicado as investigações em geral. Então, mesmo com a expressa autorização de requisição de dados cadastrais — a maior parte dos provedores das telecomunicações tem acatado isso —, isso ocorre com este entendimento: só vale se for para esse tipo de legislação.

Propusemos colocar na Lei 12.830/13, que é a lei de investigação criminal, essa requisição direta de forma bem explícita, para que nós não precisemos ficar justificando para o provedor o conteúdo da investigação. Então, se o art. 20 do Código de Processo Penal prevê que a investigação precisa ser sigilosa, parece-me que é um paradoxo ter que informar para o provedor de Internet ou o provedor de telefonia qual é o conteúdo da investigação, para que ele forneça um dado cadastral. É totalmente equivocado, no meu entendimento.

A própria requisição de dado cadastral já está prevista de forma genérica no Código de Processo Penal, desde 1941, mas até hoje, século XXI, essa discussão permanece e, em vez de a autoridade policial, o delegado de polícia estar preocupado com o conteúdo da investigação, a preocupação termina se voltando para questões jurídicas — se pode ou não pode requisitar um mero dado cadastral. Já estou falando demais? *(Riso.)*

Há outras propostas aqui, mas eu acho que nós podemos deixar isso para um segundo momento...

O SR. DEPUTADO NELSON MARCHEZAN JUNIOR - Deixe-me fazer uma pergunta. Qual é o artigo do Código Penal em que está prevista a requisição de dados cadastrais? O senhor se lembra de cabeça?

O SR. STÊNIO SANTOS - Genericamente, no art. 5º, inciso III, do Código de Processo Penal.

O SR. DEPUTADO SANDRO ALEX - Dr. Stênio, qual é o número de profissionais da Polícia Federal que atuam na repressão a crimes cibernéticos?

O SR. STÊNIO SANTOS - O Dr. Elmer, responsável pela unidade central, vai ter maior propriedade de dar essa informação. Eu posso dizer que, no Grupo de Repressão a Crimes Cibernéticos, aqui no Distrito Federal, nós temos, hoje, um delegado de polícia, que sou eu, quatro agentes de polícia e um escrivão de polícia. No caso do DF.

O SR. DEPUTADO SANDRO ALEX - O Dr. Elmer vai responder, então? *(Pausa.)* Obrigado.

O SR. DEPUTADO DANIEL COELHO - Dr. Stênio, essa unidade aqui no DF... O crime de Internet não é regional, não atinge o DF, ou São Paulo, ou Pernambuco. Vocês atuam nacionalmente ou apenas em crimes que são territorialmente localizados no DF?

O SR. STÊNIO SANTOS - Em razão da peculiaridade do crime cibernético, quando a notícia chega, nós não temos ainda a identificação da autoria. Por não ter a identificação da autoria, nós partimos do pressuposto de que não é conhecido o local do crime cibernético, ele está difundido. Em muitos dos casos — e talvez, proporcionalmente, o DF seja o que mais tem investigações —, a vítima vai encaminhar para a unidade mais próxima dela. Então, todos os Deputados,

Senadores, Ministros do Supremo, Ministros do Executivo, Juízes etc., todas as autoridades públicas que estão aqui no DF terminam encaminhando isso para o GRCC — Grupo de Repressão a Crimes Cibernéticos, e nós temos que, num primeiro momento, identificar onde o crime é praticado. Ao identificar isso, é feito, num segundo momento, o encaminhamento para a unidade em que o suspeito está. Então, há esses dois caminhos.

O SR. DEPUTADO DANIEL COELHO - E existe, nos Estados, estrutura para receber esse encaminhamento de vocês? Quer dizer, cada Estado da Federação tem também um núcleo para tratar de crimes cibernéticos, para dar esse retorno e o encaminhamento?

O SR. STÊNIO SANTOS - Essa informação eu vou deixar para o Dr. Elmer, que é o responsável pela...

O SR. DEPUTADO DANIEL COELHO - Se puder anotar, Dr. Elmer, para nós tentarmos esclarecer...

A SRA. PRESIDENTE (Deputada Mariana Carvalho) - Solicito, Dr. Elmer, que o senhor seja direto nas respostas. Há ainda cinco Deputados inscritos para fazerem perguntas.

O SR. ELMER COELHO VICENTE - O.k. Vou, então, afastar-me um pouco da questão do espaço de otimização da legislação, de tudo isso que já vimos falando sobre a questão de robustecer o processo, que vai ser o verdadeiro diferencial para nós termos o combate que a sociedade tanto clama.

O prazo de guarda é suficiente? Hoje eu tenho dificuldades tão grandes a respeito dos *logs* dentro do prazo que nem vou entrar na questão do prazo — se é insuficiente ou suficiente.

Quanto à desorganização do fornecimento desses *logs* e ao que o Dr. Stênio mencionou, nós estamos enfrentando um grande problema, que é o “jeitinho” que foi dado para serem atribuídos IPs a tantas coisas que estão conectadas à Internet sem ter um número suficiente para ser atribuído. O provedor precisa logar, além do IP, a porta, porque, hoje, se o provedor só tem dez IPs — vamos fazer a proporção —, mas ele pegou 50 clientes, além da questão do IP dinâmico, ele divide o mesmo IP dinâmico, através da porta lógica, que é o NOT.

Hoje em dia, além da dificuldade de se ter o IP ou não, de estar no prazo ou não, nós temos de discutir sobre logar a porta lógica. Então, dentro dos seis meses... A questão, hoje, já é complicada, nós já enfrentamos muita dificuldade. Vamos enfrentar a questão do prazo, quando passarmos a solucionar essas questões sobre o que nós temos hoje de informação, não sobre o que nós não temos.

O Deputado Sandro fez uma pergunta muito importante: quais empresas? Elas auxiliaram num prazo não satisfatório e em uma apresentação não satisfatória — a forma de apresentação não foi satisfatória. O encaminhamento não foi satisfatório. Apresentamos a seguinte dificuldade: *"Nós temos 20 mil IPs para uma determinada empresa. Você só recebe por fax".* A empresa disse: *"Então, traga pessoalmente".*

(Intervenção fora do microfone. Ininteligível.)

O SR. ELMER COELHO VICENTE - Sim, todas.

(Intervenção fora do microfone. Ininteligível.)

O SR. ELMER COELHO VICENTE - Acho que as empresas precisam...

O SR. DEPUTADO ESPERIDIÃO AMIN - A Casa Civil tem um setor institucional, do Governo, que trata disso, que já homologou o *e-mail*.

O SR. ELMER COELHO VICENTE - Eu acho que cai um pouco nessa liberdade de a empresa aceitar ou não, independentemente de conferir a validade jurídica ou não. Então, quais empresas?

O SR. DEPUTADO SANDRO ALEX - Quais empresas, Dr. Elmer?

O SR. ELMER COELHO VICENTE - Todas.

O SR. DEPUTADO SANDRO ALEX - Todas?

O SR. ELMER COELHO VICENTE - Todas.

O SR. DEPUTADO SANDRO ALEX - Vamos lá. Cite-as, por favor.

O SR. ELMER COELHO VICENTE - Todas as empresas que nós... Nós fizemos uma reunião com o SINDITELEBRASIL — Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal, em que ele enfeixa uma série de empresas. O SINDITELEBRASIL encaminhou nossa deliberação, e todas as empresas não atenderam de forma satisfatória.

O SR. DEPUTADO SANDRO ALEX - Só de conexão? O senhor fez pedido de aplicação?

O SR. ELMER COELHO VICENTE - Não, não, de aplicação, não, porque eu não posso. Só a respeito da conexão, só a respeito da conexão.

O SR. DEPUTADO SANDRO ALEX - Por que o senhor não pode?

O SR. ELMER COELHO VICENTE - Por causa da questão da judicialização dos serviços eletrônicos.

Então, nós fizemos o pedido. Já tínhamos o IP. Só queríamos o cadastro desses IPs. A partir desse momento... Por quê? Porque, nessa questão da pornografia infantil, houve a análise de que, proativamente, as empresas já identificaram quais eram os usuários que estavam compartilhando pornografia infantil. Com isso, elas fizeram a notícia já com o usuário e com o IP. Eu precisava, para complementar e até para distribuir, do cadastro. Até porque, em 50 mil, eu acredito que haveria muitas repetições de pessoas. As pessoas criam diversos usuários. Eu não preciso ter dez investigações só porque tenho dez usuários. Às vezes, esses dez usuários são uma pessoa.

Então, essa prévia de obtenção do cadastro foi para otimizar o próprio recurso policial, que é escasso. Daqui a pouco eu vou dizer quantos policiais estão entrando. É preciso otimizar todas.

A maior dificuldade que nós temos hoje é a organização da informação na iniciativa privada. O efetivo é pouco? É pouco. O processo é ruim e poderia ser melhorado? Poderia. Nós poderíamos ter mais tecnologia? Poderíamos. Só que, com o que eu já tenho hoje, com o processo que é vigente, com o efetivo que eu já tenho, a informação não é apresentada com uma qualidade boa. Então, com tudo que eu já tenho, se pudéssemos uniformizar, se pudéssemos padronizar as formas como essas informações devem chegar às autoridades públicas, teríamos um ganho muito grande.

A questão do efetivo, realmente, é deveras complicada. Nós criamos o grupo em 15 Unidades da Federação. Não existe hoje uma atribuição exclusiva para o crime cibernético. Se o superintendente entender que aquele determinado grupo vai atuar num outro crime fazendário, vai atuar num outro crime de *(ininteligível)*, que aquela pessoa vai acumular função, vai acumular. Então, nós encontramos uma

realidade diversa nesses 15 grupos. Há grupo em São Paulo em que eu tenho, sim, policiais lotados. Eu tenho dois delegados lotados, eu tenho cerca de seis policiais analistas lotados, recebem policiais de outro país. Mas eu tenho, por exemplo, na Bahia, um grupo que não tem nenhum analista. Eu só tenho um delegado, que acumula. Tenho um grupo em Rondônia em que há um delegado acumulando, fazendo operações de outros crimes. Então, a questão do efetivo não é uniforme e não há a atribuição exclusiva de presidir os inquéritos de crime eletrônico.

O SR. DEPUTADO SANDRO ALEX - Não há um núcleo, então?

O SR. ELMER COELHO VICENTE - Existem 15 grupos constituídos na Polícia Federal; e não só formalmente; de fato, eles existem. Só que, às vezes, esses grupos acumulam outras funções que não são necessariamente de crime cibernético.

O SR. DEPUTADO SANDRO ALEX - Então, não é um núcleo específico...

O SR. ELMER COELHO VICENTE - Não é um núcleo específico.

O SR. DEPUTADO SANDRO ALEX - A Polícia Federal não tem um núcleo específico de combate a crimes cibernéticos?

O SR. ELMER COELHO VICENTE - Nós temos, mas ele pode acumular. Por exemplo, existe um grupo específico de crime cibernético no Rio Grande do Sul? Existe. Existe em São Paulo? Existe. Existe em todos os Estados. Mas ele pode acumular, por exemplo, uma operação de meio ambiente? Pode. Ele pode acumular uma repressão ao crime eleitoral? Pode. Ele pode acumular um crime fazendário de moeda falsa, contrabando? Pode. Então, apesar de existirem núcleos específicos, em razão da carência de efetivo, eles acabam acumulando com outros grupos específicos.

O SR. DEPUTADO SANDRO ALEX - O.K. Então, não há um grupo específico que atue, hoje, no País, na Polícia Federal, somente em crimes na Internet. Sim ou não?

O SR. DEPUTADO RODRIGO MARTINS - Exclusivamente.

O SR. DEPUTADO SANDRO ALEX - Pergunto ao senhor: sim ou não? Especificamente em Internet.

O SR. ELMER COELHO VICENTE - Há um grupo exclusivo para Internet em Minas Gerais, no Rio Grande do Sul e em São Paulo. O resto do País passa por uma dificuldade muito grande para acumular.

O SR. DEPUTADO SANDRO ALEX - Em três Estados são específicos?

O SR. ELMER COELHO VICENTE - São específicos.

O SR. DEPUTADO SANDRO ALEX - O senhor tem o número do total do efetivo no Brasil?

O SR. ELMER COELHO VICENTE - Da Polícia Federal?

O SR. DEPUTADO SANDRO ALEX - Para esses crimes na Internet. O senhor disse que são três Estados. Quantas pessoas trabalham nesses três Estados para esses crimes específicos?

O SR. ELMER COELHO VICENTE - Não passam de 20.

O SR. DEPUTADO SANDRO ALEX - Então, a Polícia Federal tem 20 pessoas que trabalham especificamente com *cybercrimes* no Brasil?

O SR. ELMER COELHO VICENTE - Além dos grupos nos Estados, existe o órgão central, que é a coordenação nacional. Na coordenação nacional, 28 pessoas trabalham especificamente com crimes cibernéticos. Só que nós cuidamos da coordenação. Não fazemos a repressão específica, porque a repressão não fica no órgão central, ela é distribuída para as superintendências. O Dr. Stênio é do Distrito Federal. Eu também sou do Distrito Federal, só que eu sou do órgão central. Eu vou atrás de melhorar o processo, de novas tecnologias, de buscar capacitação. Então, todas...

O SR. DEPUTADO ESPERIDIÃO AMIN - Eu vou interromper o Dr. Elmer para pedir ao Deputado Sandro Alex que não compare com o efetivo da Agência de Segurança Nacional — NSA nem com o do Exército chinês.

O SR. DEPUTADO SANDRO ALEX - Quantos profissionais o senhor acha que deveria haver na Polícia Federal para o combate a crimes na Internet? O senhor disse que há 20, em três grupos. Quantos?

O SR. ELMER COELHO VICENTE - Se nós tivéssemos efetivo para compor exclusivamente os grupos que já são criados — e já existe um normativo que define o efetivo mínimo —, já teríamos um avanço muito grande.

(Intervenção fora do microfone. Inaudível.)

O SR. DEPUTADO SANDRO ALEX - Nós queremos auxiliar a Polícia Federal.

O SR. ELMER COELHO VICENTE - Quanto à questão do papel ativo das empresas na vingança pornô, por exemplo, que foi citada, as empresas têm, cada vez mais, aberto um canal com a população para que denuncie abuso de conteúdo e para que ela, proativamente, o retire. Isso é insuficiente, diante do tamanho das reclamações, para que a empresa dê conta.

Eu vou dar o exemplo do Facebook. O Facebook tem um grupo específico para analisar esses reportes de quando você diz: *"Olha, esse perfil é meu. Estão duplicando, estão falando mal de mim, estão me difamando"*. Não é suficiente, não é efetivo esse papel proativo das empresas, tanto que as pessoas se socorrem do Judiciário para ter uma prestação mais célere.

Acredito que tenha coberto... Se faltou alguma coisa, se eu estiver devendo...

A SRA. PRESIDENTA (Deputado Mariana Carvalho) - Com a palavra o Dr. Carlos Eduardo.

O SR. CARLOS EDUARDO MIGUEL SOBRAL - Vou ser bastante direto e breve.

Em relação ao prejuízo de fraude bancária, eu usei um dado aproximado de 1 bilhão, mas esse dado é de 2009. Eu acho que o último de que tive conhecimento é de 2012, de 1,4 bilhão de fraude bancária, só na transferência, clonagem em cartão de crédito e débito e em fraude no Internet Banking — 1,4 bilhão, em 2012. Esse dado não é divulgado, não é repassado para todo mundo, porque é uma informação reservada que os bancos têm. Às vezes, eles divulgam. O último, de 2012: 1,4. Não me lembro de ter visto o de 2013 e o de 2014. Não sei se aumentou ou reduziu. Não me lembro desses números.

Quando nós fizemos o acordo com a Caixa, sabíamos que, ao receber as fraudes sofridas pelos correntistas da Caixa, iríamos enxergar parte do problema. Enxergar parte do problema não é suficiente. Nós queríamos enxergar todo o problema, para que pudéssemos, então, desenvolver uma política nacional de repressão a esse tipo de delito.

Nós fizemos um acordo de cooperação técnica com a Federação Brasileira de Bancos — FEBRABAN para que os bancos interessados em participar desse

esforço repassassem os dados à Polícia Federal. Todos os grandes bancos assinaram esse acordo de cooperação técnica. Nós estamos na fase de implantação do sistema que vai permitir à Polícia Federal receber, de forma instantânea, toda comunicação de crime sofrida pelo correntista do banco. Como funciona? O correntista detecta a transferência ilícita, comunica ao seu banco, autoriza o repasse das informações à Polícia Federal e, via sistema, via *web service*, ou seja, de forma automática, essa informação sai do banco e entra nos sistemas da Polícia Federal, para que possamos, então, ter conhecimento de tudo o que acontece relacionado à fraude — à fraude praticada, não é à fraude tentada, não é informação de correntista — praticada contra aquele que foi vítima e autorizou o repasse, de forma oficial, à Polícia Federal, e, a partir daí, sabendo de tudo o que acontece, agir no âmbito da Polícia Federal e também em cooperação com as Polícias Estaduais, com a Polícia Civil.

Nós estamos agora na fase de recebimento das informações. Por que eu disse que o prejuízo é nosso? Porque, na verdade, em alguns países, os bancos não ressarcem o prejuízo sofrido pela vítima. A vítima sofre o furto e arca com esse prejuízo. No Brasil, não. Nós envolvemos, no nosso arcabouço jurídico, a decisão de que o banco é responsável por ressarcir, salvo se não for uma vítima, se ela for, realmente, autora do crime — é uma autofraude. Se não for caso de autofraude, a vítima será ressarcida.

O banco, então, coloca esse prejuízo como custo operacional, como custo-negócio, que é compensado com as taxas, que é compensado com os recursos que entram para o sistema. Ou seja, na verdade, quem paga 1,4 bilhão de prejuízo somos nós, é toda a sociedade que usa o sistema financeiro. Então, não é um problema do banco. Talvez o menor problema seja o do banco, porque ele é ressarcido pelo sistema, e o nosso dinheiro vai para o crime organizado. Ou seja, nós estamos alimentando o crime organizado. Então, o problema não é do banco, é nosso, porque estamos perdendo e passando dinheiro para alguém que vai usá-lo contra nós. Essa é a análise que fazemos da fraude bancária.

Quais seriam as prioridades? Hoje eu estou cedido para o Ministério da Justiça, não estou mais atuando diretamente na área. Então, o sentimento de quem está de fora, um pouco mais afastado, é de que a prioridade 01 é a estrutura. Se nós

não tivermos estrutura de investigação, não adiantará passarmos aqui mais 10 anos melhorando as leis. Teremos leis excelentes, leis perfeitas, só que não haverá ninguém para aplicá-las, não haverá operador da lei.

Então, nós defendemos, desde 2012, que o Brasil tenha uma estratégia nacional de combate ao crime cibernético nos mesmos moldes da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro — ENCCLA, que cuida da corrupção e da lavagem de dinheiro. Nós precisamos saber o que temos, nós precisamos saber o que precisamos ter e nós precisamos definir como e quando vamos chegar àquilo que nós precisamos ter. Hoje nós não temos isso definido. Nós não temos planos de ação nacional, nós não temos algo desenhado, pensado e instituído.

Então, seria, primeiro, a estruturação; e segundo... A questão dos *logs* é algo que poderia vir a agregar. Em 2008, nós já tratamos disso no âmbito da CPI da Pedofilia. A CPI apresentou um projeto na Casa. No Senado, ele recebeu o nº 494, de 2008. Ele foi aprovado no Senado recentemente. Acho que chegou à Câmara no mês passado. É o Projeto de Lei nº 2.514, de 2015, que trata da regulamentação dos *logs*, do acesso aos *logs*, para o combate à pornografia infantil. O projeto foi defendido pela Polícia Federal. É uma proposta que atende a essa demanda específica da Polícia Federal, mas está inserida naquele debate de *logs*, de prazo, de acesso, que realmente vem sendo feito aqui na Casa há algum tempo.

Então, seria neste sentido: prioridade 01 — estrutura. O Dr. Elmer falou dos números. Estamos avançando. Em 2008, nós tínhamos duas pessoas trabalhando na área. Duas, no Brasil! Conseguimos montar os grupos, conseguimos montar uma estrutura aqui em Brasília para coordenar. Agora, o nosso desafio é estruturar os grupos, não só na Polícia Federal, onde conseguimos avançar — não é o ideal, mas houve avanços —, mas também nas Polícias Estaduais. Acho que se nós conseguirmos estrutura, poderemos, daqui a algum tempo, fazer uma análise mais profunda e mais concreta daquilo que deu certo e daquilo que vem dando errado na nossa atuação de combate aos crimes cibernéticos.

A SRA. PRESIDENTA (Deputado Mariana Carvalho) - Para concluir a última rodada de perguntas, passo a palavra ao Deputado Leo de Brito.

Solicito aos Deputados que se restrinjam ao tempo de 3 minutos, para dar tempo de ouvirmos as respostas e as considerações finais.

O SR. DEPUTADO LEO DE BRITO - Obrigado, Sra. Presidenta. Gostaria de agradecer também, como autor dos requerimentos, a contribuição de todas as autoridades presentes.

Eu acho que um dos grandes desafios desta CPI é fazer a apuração dos casos e, ao mesmo tempo, fazer o aperfeiçoamento da legislação; obviamente, sem que haja um retrocesso.

Eu acredito que a lei do Marco Civil da Internet foi uma grande conquista da sociedade brasileira. Inclusive, ela está sendo copiada pelo mundo. Aqui há vários Deputados que participaram desse momento, quando as várias forças políticas do Congresso Nacional tiveram consenso em relação a uma lei que estabelece os direitos civis relacionados aos usuários da Internet.

Eu queria fazer algumas perguntas que considero pertinentes. A primeira é para o Delegado Elmer. Além da Operação IB2K, que outras operações relacionadas ao sistema bancário foram realizadas pelo Serviço de Repressão a Crimes Cibernéticos? Nós temos conhecimento de algumas outras, como a Operação Sheik, a Operação Darkode. Eu queria saber não só quais as demais operações, mas também o quantitativo disso. Vocês estimam como está essa situação relacionada aos crimes do sistema bancário?

Dr. Stênio, a respeito da Lei 12.737/13, Lei Carolina Dieckmann, o senhor considera que ela tem contribuído para as investigações da PF? Em que medida? Faça uma avaliação dessa lei que surgiu naquele momento de clamor social. Talvez seja uma das pioneiras, digamos assim, do ponto de vista dessa questão dos crimes cibernéticos.

Peço ao Dr. Sobral que fale um pouco, por gentileza, sobre a pedofilia na Internet. Como o Estatuto da Criança e do Adolescente tem contribuído para as investigações e como a SaferNet tem colaborado com as investigações.

Mais uma pergunta. Eu vi que surgiu aqui uma preocupação muito forte em relação às atribuições dos entes federados, na questão da organização. O Dr. Sobral já falou um pouco sobre essa questão da cooperação. Que sugestão V.Sas. dariam, relacionada a essa questão das atribuições, para termos, de maneira muito

mais clara, as atribuições dos entes federados nas questões investigatórias relacionadas aos crimes cibernéticos?

Seria isso, Sra. Presidenta.

Obrigado.

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

Com a palavra o Deputado João Arruda.

O SR. DEPUTADO JOÃO ARRUDA - Sra. Presidente, Deputada Mariana, cumprimento V.Exa., o Relator — ele está ausente agora, mas cumprimento o Deputado Federal que o representa —, os Relatores e Sub-Relatores presentes na Comissão, os nossos convidados: Dr. Stênio, Dr. Elmer e Dr. Carlos Eduardo.

Eu queria fazer uma pergunta bem objetiva para cada convidado, sobre o que estamos discutindo aqui hoje. A primeira é sobre a segurança daqueles usuários dos bancos. Nós estamos falando de 32 milhões de contas bancárias que são movimentadas pela Internet. Fala-se em um avanço importante. Eu queria saber a opinião do Dr. Stênio sobre o *smartphone* e a biometria, pontos importantes que poderiam auxiliar na segurança de quem movimenta contas bancárias. Eu queria saber se o Dr. Stênio confia no sistema.

Eu mesmo fui vítima, ontem, de uma movimentação que aconteceu na minha conta do Smiles. Eu nem sabia que poderíamos fazer compras com esse cartão. Tentaram comprar quatro aparelhos de telefone celular iPhone, no Rio Grande do Sul. Quem vendeu pela Internet achou estranho, ligou para o gabinete e conferiu que não era uma compra feita por mim. Eu queria saber se o Dr. Stênio faz compras pela Internet e se ele usa o sistema bancário de Internet Banking.

Queria perguntar ao Dr. Carlos Eduardo sobre Edward Snowden. Agora, vimos que houve uma conciliação entre a Presidente Dilma e o Governo do Brasil, em relação ao que aconteceu no passado. Enfim, colocaram panos quentes e superaram o que aconteceu.

A revista *The New York Times*, na edição do mês de fevereiro, afirma que existe investigação no Brasil e que empresas estão sendo monitoradas pelo Governo norte-americano. Ou seja, eles têm o privilégio da informação, o que nos coloca em desvantagem na concorrência. Isso de fato acontece? Tem como afirmar

que sim ou que não? Que providências o Governo brasileiro está tomando para proteger essas empresas?

A indagação que faço ao Dr. Elmer é mais um comentário. E vou concordar com o Deputado Jean Wyllys em relação ao avanço que tivemos. Talvez tenha sido um retrocesso. Eu compreendo que a Polícia Federal quer investigar, quer buscar resultados rápidos para crimes cometidos através da Internet. Não é culpa da Internet, mas de quem comete esses crimes.

Quanto ao direito à privacidade, nós avançamos muito. Discutimos, naquele momento, a questão da judicialização — que todo processo passe pela Justiça antes de uma atitude tomada pelo provedor de aplicativo ou mesmo pelo provedor de conexão — exatamente para preservar os direitos dos usuários. Um provedor de conexão, a qualquer momento, poderia fazer uma denúncia e esse provedor de conexão, que não tem a capacidade de julgar, não está lá para isso, poderia retirar esse *blog* do ar, sendo que a acusação poderia não ter realmente subsídios suficientes para sofrer um processo judicial e ser condenado.

Essa independência, dentro da Internet, essa privacidade que cada um tem de comentar, essa liberdade que cada um tem de participar e de comentar é essencial para que ela se torne uma ferramenta verdadeiramente democrática.

O Deputado Daniel falou aqui sobre crimes cometidos muitas vezes por usuários que são servidores do Governo. No meu Estado, por exemplo, isso acontece com muita frequência. O Governo tem centenas de *cybers* comissionados que atacam os seus adversários. Eles até deram um nome para isso, criaram uma tenda digital, algo ligado ao partido do Governador, e centenas de usuários *cybers* comissionados atacam os seus adversários e defendem o Governador diariamente. Se eu fizer uma denúncia, por exemplo, para a Polícia, sem que se discuta na Justiça, a Polícia é um órgão ligado ao Governador, não estou tirando aqui a independência do órgão e a legitimidade para investigar, mas ela é ligada ao Governo do Estado, e a denúncia será feita contra os servidores do Governo. Na minha visão, é até um crime muito mais de improbidade administrativa do que qualquer outra coisa. Isso é algo em que nós precisamos também avançar na legislação.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Por favor, conclua, Deputado.

O SR. DEPUTADO JOÃO ARRUDA - Nós devemos ter esse cuidado, porque, se colocarmos em cada cidadão brasileiro uma tornozeleira, por exemplo, vai ser muito mais fácil e muito mais rápido de desvendar um crime. O WhatsApp é uma ferramenta importantíssima, pois eu posso passar para o pediatra do meu filho uma fotografia de uma alergia que ele tem. Portanto, temos de ter o cuidado na hora de criminalizar algumas ferramentas da Internet e a própria Internet.

Eu queria perguntar ao Dr. Elmer quantos crimes, no Brasil, investigados pela Polícia Federal não tiveram resultado. Qual a proporção de crimes que foram resolvidos pela Polícia Federal, através de uma investigação, e crimes que estão investigando e ainda não conseguiram resultados, nem buscar os culpados, enfim, não têm o resultado que nós gostaríamos? Em que proporção estão aqueles que já foram investigados e superados e aqueles que não foram superados?

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Com a palavra o Deputado Delegado Éder Mauro.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Sra. Presidente, Srs. Deputados, Dr. Stênio, Dr. Elmer, Dr. Carlos Eduardo, nós agradecemos a presença de todos. Serei rápido.

Eu queria iniciar dizendo que sou delegado de polícia há 30 anos, estou Deputado Federal e sei das dificuldades que nós policiais temos nas investigações, muitas das vezes pelo distanciamento em alguns setores entre Polícia e Judiciário, para que se consigam autorizações para investigação, para grampo, esse tipo de coisas. Gostaríamos inclusive que isso fosse bem mais estreito. Sei que a CPI apura crimes cibernéticos, mas nós gostaríamos de, além disso, poder ver as dificuldades que a Polícia e os organismos têm em poder investigar.

Nós sabemos da questão dos *fakes*, das pornografias infantis, de transferências bancárias utilizando os *hackers* de todas as maneiras — inclusive eu também já fui vítima disso e tive de trocar o cartão —, dos estelionatários, etc.

Eu gostaria realmente de poder saber isso, porque na Civil nós temos esses problemas, com exceção de alguns outros membros do Judiciário. A grande maioria tem uma aversão na questão do grampo, do rastreamento. Quando fazemos o

grampo, nós conseguimos as ERBs conseguimos as azimutes, para poder fazer a localização, mas na questão do computador, as dificuldades são muito maiores, tenho certeza, porque muitos registram, ativam com identidades de terceiros, *fakes* também, para que se dificulte a investigação.

Eu gostaria de saber sobre as dificuldades que têm em relação a isso, para que esta Casa possa também criar mecanismo nesta CPI que facilite, já que sabemos que as nossas questões são de fora do País, são muito abstratas, e é muito difícil identificar e trazer as coisas para cá. Eu gostaria muito de saber desse posicionamento de todos os três.

Aproveito para deixar registrado, Sra. Presidente, que, graças a Deus, em geral, eu só tenho elogios à Internet, não tenho problema algum com ela. Agora, diferente de muitas pessoas que, às vezes, por terem posicionamento de destruição familiar, de quererem fazer até cirurgias em crianças para mudança de sexo, para liberação de drogas, para tornar a atividade de venda de drogas como uma atividade profissional, com carteira assinada e até para que traficantes criem um sindicato, essas pessoas deveriam parar de se vitimizar, de se tornar coitadinhos e manter os seus posicionamentos. Eu não tenho esse problema, graças a Deus.

Isso era o que eu queria dizer.

Obrigado, Sra. Presidente.

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

Com a palavra o Deputado Nelson Marchezan Junior.

O SR. DEPUTADO NELSON MARCHEZAN JUNIOR - Obrigado, Deputada Mariana. Vou tentar ser breve aqui, em virtude do adiantado da hora.

Os delegados me perdoem se eventualmente, nessas saídas para votar ou ir ao toalete, tenha perdido alguma resposta e eu seja repetitivo.

Presidente Mariana, é crucial, pois que estamos iniciando a CPI e temos pouco tempo, que os delegados possam nos dizer quais os principais crimes cibernéticos que ocorrem no Brasil, se há dados estatísticos disso, de número, de volume, de reflexos, para que possamos, quem sabe, direcionar a CPI para o que mais interessa e não para aquilo que representa, dentro dos crimes cibernéticos,

eventualmente, 1% ou 2%. Importa saber se temos esses dados, para orientar os trabalhos da CPI naquilo que mais interessa aos brasileiros.

A segunda questão é quanto à existência de taxa de elucidação desses crimes. Por exemplo, no Rio Grande do Sul, a taxa de homicídios que se tornam denúncia, processo criminal é em torno de 2%, se não me engano. Então, qual é a taxa de elucidação dos crimes que efetivamente chegam até a Polícia Federal, desde o seu início até a sua finalização? Essa estatística existe?

Terceiro, desejo saber se há taxa de reincidência, para que possamos avaliar onde a legislação é mais solta, mais frouxa, se ela combate efetivamente a reincidência, onde o criminoso se sente mais liberado em virtude da realização de crimes cibernéticos.

Quarto, eu procurei aqui no Código de Processo Penal, art. 5º, inciso III, e não localizei; quais são as sugestões de alteração legislativa, seja no marco civil da Internet, seja na legislação pertinente, vigente, para que possamos facilitar essas investigações? Particularmente, eu acho que aqui não buscamos criminalizar a Internet, mas encontrar meios de localizar o criminoso, que é criminoso fora ou dentro da Internet. Hoje, temos mecanismos de câmeras de filmagem, de pardais, para identificar as placas de veículos nos pedágios, o que facilita, no mundo real, o acesso às informações. Então, o que poderíamos ter de alteração para criminalizar no mundo virtual e localizar o criminoso?

Quinto, se os senhores podem sugerir em que a CPI deve focar — isso vem contribuir com a primeira pergunta. Qual seria o foco da CPI? Os senhores, se puderem, deem uma sugestão em que deveríamos focar os nossos trabalhos. São só 120 dias de investigação utilizando as ferramentas legais que as CPIs têm para efetivamente contribuir nessa elucidação do que é realmente importante.

Eu teria mais algumas questões aqui, mas faço a última: o que teriam para colocar sobre a *deep web*? Teriam uma colocação específica sobre a investigação, se deveria ser diferenciada, se deveria ser alterada a legislação? O que se poderia fazer com relação ao que acontece na *deep web*? Quais os seus comentários?

Muito obrigado, Deputada Mariana.

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

Com a palavra o Sub-Relator, Deputado Rafael Motta.

O SR. DEPUTADO RAFAEL MOTTA - Primeiro, boa tarde a todos.

Serei também breve. O Deputado Marchezan já adiantou algumas das minhas perguntas.

A temática da Internet, do mundo virtual, é incrível. Nós avançamos 50 anos comparados a 5 anos do século passado.

Eu parafraseio o Deputado João Arruda, que disse que o mundo virtual — não sei se foi o Deputado Sandro Alex ou o Deputado João Arruda — é uma praça pública, onde existem crianças, idosos, pessoas que estão ali para ter relações pessoais com outras, pessoas que estão ali para ampliar o seu conhecimento. Só que essa praça pública tem uma diferença do mundo real, digamos assim: essa praça está envolta em uma neblina muito carregada. Fica difícil identificar aquele cidadão que se encontra muitas vezes ao seu lado. Eu acho que é essa a dificuldade que a polícia enfrenta.

Sabemos que a legislação pode ser perfeita, modelo — Dr. Carlos citou aqui muito bem —, mas de que adianta, se nós não temos infraestrutura e pessoal para elucidar esses crimes?

Então, na nossa sub-relatoria, que não é menos importante que as demais, sabendo, por exemplo, que os crimes financeiros... Os bancos têm dificuldade, criam investimentos nessa área por serem os mais prejudicados e terem também condições de contratar trabalho de consultoria. O Dr. Carlos falou também que quem financia esses criminosos são os próprios usuários do banco, visto que isso recai nos custos operacionais. Então, nós acabamos, por contrapartida, financiando o crime na Internet, principalmente os crimes virtuais.

Na pedofilia, o que me preocupa é saber quem são os prejudicados. Não são os grandes conglomerados, os bancos. É única e exclusivamente a vítima, que vai passar por um período de dificuldades, de trauma, e a família, que, muitas das vezes, inclusive, dão o consentimento para a prática da pedofilia com aquelas crianças. No Norte, por exemplo, há famílias que oferecem suas crianças para os balseiros terem relações sexuais. Enfim, é algo inimaginável nos dias de hoje.

Mais diretamente, a dúvida em que incorre a nossa sub-relatoria é em relação à dificuldade de identificar — como o Deputado Nelson Marchezan Junior já citou,

esperamos que a Polícia Federal possa nos dar o mapa — onde ocorrem esses crimes. Onde se encontra o criminoso que pratica o ato de pedofilia, o criminoso que distribui esse material e o criminoso que pode ser tido como usuário desse material? Quais são as circunstâncias em que isso ocorre? Como rastrear esses IPs, esses logs? O que esse criminoso faz para dificultar a investigação da Polícia Federal? É a mudança de IP? Existem programas que alteram o IP, a identificação do computador? Existem programas que alteram portas de conexão em relação a esse mundo? Os logs podem ser alterados por esses criminosos, visto que hoje a tecnologia para o mal avança tanto quanto a tecnologia para o bem?

Por exemplo, no Estado do Rio Grande do Norte, que eu represento, em 2013, foi fechado o NICAT, que é o núcleo da polícia civil que investiga esses crimes de alta tecnologia. Existe uma relação hoje, Dr. Elmer, entre a Polícia Federal e os Estados, as Policias Civis de cada Estado? Ainda abranjo mais um pouco essa temática: existe uma relação com as demais polícias mundiais? Existe uma relação com as polícias americanas — FBI, NSA?

A CPI tem um poder muito forte na mão, o poder de abrir inquérito. Como nós podemos realmente auxiliá-los, visto que o tempo é muito curto? Temos que dar uma resposta à sociedade. O Poder Legislativo não pode se furtar a debater essa temática e buscar realmente penalizar esses criminosos.

Então, as nossas dúvidas são essas.

Deixamos a nossa CPI à disposição de todos. Em especial, precisaremos muito da Polícia Federal, para que possamos dar um resultado e mostrar à sociedade que nós estamos trabalhando para fazer um Brasil melhor.

O SR. DEPUTADO NELSON MARCHEZAN JUNIOR - Sr. Presidente, sugiro que seja suspensa a sessão por 5 minutos.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Vamos aguardar.

Enquanto V.Exas. vão, eu faço as minhas perguntas. Será o tempo de voltarem.

O SR. DEPUTADO NELSON MARCHEZAN JUNIOR - Ótimo.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Só para justificar: há mais uma votação nominal. Vou pedir desculpa pela saída de todos.

Eu gostaria de aproveitar, enquanto os Deputados voltam, para fazer algumas perguntas também.

A *deep web* foi citada pelo Deputado Nelson Marchezan Junior. Eu queria que os senhores falassem um pouquinho tambémda *dark net*.

Sabemos que nesse mundo, como disse o Deputado Rafael Motta, é preciso ter um pouco mais de conhecimento. Nesse mundo virtual, que sabemos que existe, eu queria saber se há outros meios e outras formas para investigação e, em relação a esses equipamentos, como foi dito, se é algo mais profundo de que se precise e de que forma podemos fazer.

Nas explanações dos senhores, falou-se sobre a questão de que com o próprio IP conseguimos chegar muitas vezes às pessoas que estão cometendo o crime. Então, eu gostaria de saber se apenas com o IP conseguimos iniciar essas investigações e ter um resultado positivo.

Outra dúvida, também, é em relação a essas redes, por exemplo*, lan houses*, quando se usa o mesmo IP, e o local não tem uma câmera, não se sabe se as pessoas que por ali passaram. Como os senhores conseguem chegar a essas pessoas para iniciar uma investigação? Porque eu acredito que até mesmo os criminosos têm conhecimento de que podem ser reconhecidos por esse IP, então, acabam cometendo os crimes em locais que não podem ter essa identificação, muitas vezes locais públicos. Essa é uma pergunta.

Eu gostaria de saber se V.Sas. poderiam indicar também as principais ações ou medidas de prevenção a serem adotadas no caso dos correntistas, como foi o caso da Operação IB2K, e outros usuários da Internet também, para evitar a obtenção de senhas, arquivos digitais e dados bancários por *hackers*. Como vocês enxergam essa questão para termos uma segurança maior, a partir desta CPI, não apenas para os bancos, mas também para as pessoas.

Eu só pediria para aguardarem alguns minutos enquanto os Deputados voltam da votação nominal para darem uma resposta a todos.

Mais uma vez, quero agradecer, até mesmo porque este é um tema tão atual. Sentimos, nos discursos, a falta de pessoas realmente ligadas ao tema, um número que muitas vezes, como foi dito, 20 pessoas, acaba sendo insuficiente. Quanto aos casos de pedofilia no ano passado, o Dr. Elmer comentou que houve mais de 50 mil

denúncias. Isso fora as denúncias que não chegam. Quantos casos há também de pedofilia de que não temos conhecimento, não ficamos sabendo? Como se disse, há até casos profundos, além dos grupos de WhatsApp, também ligados a isso. Muita gente fica com medo mesmo de denunciar. O que podemos sugerir para que as pessoas se sintam seguras nessas denúncias e aproveitem a oportunidade desta CPI no combate a esses tipos de crime? Queremos apenas que a CPI mostre resultados para o Brasil, porque esse tipo de crime vem cada vez mais aumentando.

Como eu disse no início da nossa CPI, hoje, no nosso País, os usuários brasileiros ficam na rede 750 minutos, enquanto a média mundial é de 356 minutos. Então, estamos cada vez mais vulneráveis, ainda mais as mulheres, os jovens, as crianças, que têm muito mais disponibilidade de estar perante o crime.

Esta semana eu tive a oportunidade de ver um vídeo na Internet, em que os pais mesmos fizeram questão de ver se os filhos abririam a porta da própria casa pelas redes. E através do Facebook, no bate-papo, as crianças abriam a porta da própria casa para pessoas estranhas, colocando a vida da família em risco. Então, sabemos dessas questões e dos riscos.

Eu vou passar a Presidência para o Deputado Leo de Brito, só pelo tempo de eu votar. Já volto para poder ouvir também todas as respostas.

(Pausa prolongada.)

O SR. PRESIDENTE (Deputado Leo de Brito) - Bem, vamos passar a palavra agora ao Dr. Stênio Santos para as respostas e considerações finais por até 5 minutos.

O SR. STÊNIO SANTOS - Em relação ao percentual, informo que 20% das pessoas tendem a cair no *phishing* — esse é um dado aproximado. Nós não temos esse dado de forma matemática, calculado, para poder afirmar. Então, é baseado no que temos visto ocorrer. Geralmente, o *spam* encaminha 1 milhão de mensagens para diversas pessoas, e o percentual aproximado que temos percebido é este: 20%, um número bastante elevado. Daí essa incidência alta de criminalidade cibernética.

Em relação à maior dificuldade, nós já colocamos aqui em algumas oportunidades, é de estrutura; é preciso ter mais policiais. É preciso também ter um orçamento específico. Hoje não dá para se fazer segurança pública sem se ter uma

previsão orçamentária específica para aquilo. Muitas vezes, é preciso utilizar-se de criatividade para realizar a investigação, porque falta o recurso. E olha que nós estamos falando de uma polícia que é considerada de elite. Se na Polícia Federal nós sentimos a necessidade de ter orçamento específico para planejar, com base nesse orçamento, quais são as ações que nós podemos efetivamente realizar, eu fico imaginado nos Estados que têm muito menos recursos que a União.

A legislação, eu acredito, tem como ser melhorada. Apresentei algumas sugestões de modificações que vão acelerar a investigação e coloco-me à disposição para depois encaminhar também por escrito, para não exceder o tempo.

Obviamente, em relação a crimes cibernéticos, a tecnologia está sempre avançando. Então, é imprescindível que se tenha meios tecnológicos e também capacitação permanente. A troca de experiência com outros países nesse sentido é essencial. Muitos problemas que vão chegar ao Brasil já aconteceram em outros países e já foram solucionados lá. Então, essa troca de experiência, a cooperação policial internacional é essencial. Já existe, mas pode ser aperfeiçoada. Acredito que o Legislativo tem uma ótima oportunidade com esta CPI de identificar essas boas práticas que existem no mundo e tentar trazer isso para o Brasil.

Existe morosidade na Justiça para liberação de dados? Existe morosidade. Por quê? Porque o Judiciário está com excesso de processos. Ele tem uma função essencial, que é dele e ninguém pode realizar, e, aliado a isso, colocam-se outras atribuições que não seriam necessárias. Dá uma garantia maior, mas não é imprescindível. Todas as vezes em que se coloca uma atribuição a mais, quando não é imprescindível, repercute nas decisões — o juiz é o único que vai poder condenar ou absolver —, o juiz é trazido prematuramente para a fase preliminar e precisa estar também decidindo nessa fase. Então, se eu preciso dar um passo para obter a informação, eu vou ter uma resposta mais rápida para submeter à fase judicial o processo; se eu preciso dar quatro passos, ele vai naturalmente demorar mais. Há morosidade e é preciso, então, estabelecer prioridades. A prioridade deve ser, no meu entendimento, que o Judiciário atue naquilo que é imprescindível; e, naquilo que ele pode não atuar, que seja dado um voto de confiança aos órgãos de investigação e submeta-se a controle para que possamos ter efetividade na ação.

Em relação à Lei 12.737/13, lei apelidada de Lei Carolina Dieckmann, nós temos que pensar da seguinte maneira: até a Lei Carolina Dieckmann, nós fazíamos as investigações de crimes cibernéticos impróprios — aqueles crimes que já ocorriam antes de haver Internet, antes de se falar em sistema computacional —, mas não podíamos fazer nada em relação aos crimes que atacam diretamente o sistema computacional. Então, com essa lei, nós passamos a poder fazer esse tipo de investigação também.

O SR. DEPUTADO JOÃO ARRUDA - Ela tipifica crimes só, ela não trata diretamente da estrutura da polícia, não é?

O SR. STÊNIO SANTOS - Não, em princípio, ela vai trazer tipos de invasão, dispositivo informático, vai tipificar a falsificação de cartão clonado. Isso também facilitou o processo de investigação, porque muitas vezes nós íamos nos locais, encontrávamos cartões clonados e não podíamos fazer nada. Só podíamos fazer apreensão e tentar apurar. Hoje é um tipo autônomo de falsificação. Ela cria tipos penais, não está só aumentando a pena. Ela está criando, ou seja, ela está protegendo um bem jurídico que até então estava relegado a segundo plano nesse aspecto. Apesar de que, com isso, as estatísticas criminais tendem a aumentar, porque uma conduta que não estava prevista passa a estar. Por outro lado, era um comportamento desviante, como comenta a criminologia, e que afetava, de forma grave, as pessoas. Por conta disso, precisou ser tipificado criminalmente.

Em relação à segurança, o Deputado João Arruda questionou se eu utilizo o sistema bancário de *internet banking* e se eu confio nele. Eu, particularmente, utilizo todos os dias. Eu sou uma das pessoas que confia no sistema, utiliza o sistema. Isso não quer dizer que eu já não tenha tido intempéries também, mas em nenhuma delas eu fui efetivamente vítima, porque eu estou sempre fazendo o controle. Quem utiliza o sistema, tem que estar atento. Muitas vezes pode acontecer no caso, por exemplo...

O SR. DEPUTADO JOÃO ARRUDA - Qual controle?

O SR. STÊNIO SANTOS - O controle de estar olhando todos os dias as transações que estão sendo feitas; ter um equipamento com antivírus, com *firewall*, com *spyware*; não acessar determinados *sites*; utilizar serviços que a instituição bancária fornece, como, por exemplo, mandar um SMS toda vez que há uma

transação e, à medida que verifique que a transação é falsa, imediatamente entrar em contato com o banco para bloquear o cartão e contestar aquela transação, entre outras medidas. Se nós pensarmos em termos estatísticos, o número de transações seguras, válidas, sem nenhum problema, é muito superior ao daquelas que são criminosas. É óbvio que, quando se trabalha com delito, o que chega é o que está apodrecido, é o problema, mas isso não é a maioria do que está no sistema. O sistema funciona, precisa ser aperfeiçoado, com certeza, e acredito que esse aperfeiçoamento passa também por se colocar as instituições bancárias em cooperação, passa por essa troca de experiências. Algumas instituições têm respostas mais efetivas que outras. Talvez se possa tentar uniformizar um pouco a resposta de todas as instituições, porque dessa maneira as lacunas que surgem vão sendo sanadas.

Também muito importante é não só ver a questão do lado das instituições financeiras, mas o lado do usuário. É preciso haver prevenção, e, para haver prevenção, é preciso que as pessoas saibam o que podem fazer, quais são os seus direitos e quais as medidas que devem tomar quando estão naquela situação de vitimização. Muitos dos problemas que surgem no caso de fraudes bancárias são porque o usuário não sabe utilizar o serviço da melhor maneira. Então, ele permite que o criminoso acesse seu computador, invada a sua conta, clone o seu cartão e, a partir dali, comece a realizar os crimes cibernéticos.

Em relação à pontuação que eu achei extremamente pertinente, muitas vezes vai acontecer de a polícia ter que investigar o Governo. Isso é um fato. A polícia é um órgão do Governo. A Constituição, inclusive, no art. 144, § 4º ou 5º, fala que as polícias civis estão subordinadas ao Governador; e não só as civis, mas as militares e os bombeiros. Não há essa previsão explícita no caso da Polícia Federal, mas nós sabemos que ela está vinculada ao Ministério da Justiça. É óbvio que, na medida em que é um órgão do Governo, apesar de ser uma polícia republicana, não investiga. No caso da investigação, ela não vai investigar ou deixar de investigar porque é órgão do Governo. E a Polícia Federal tem demonstrado isso cotidianamente. Ela apura fatos venham de onde vierem, mas é um risco permanente que pode acontecer. Existe uma potencialidade de que, em algum momento e em algum Governo, coloque-se alguém que não queira agir de forma republicana. Luigi

Ferrajoli, pai do garantismo penal, já defendia, na sua magistral obra *Derecho y Razón,* a necessidade de independência da Polícia de Investigação, da Polícia Judiciária em relação ao Executivo. Ele coloca textualmente, na pág. 600 em diante, a necessidade de se dar garantias à Polícia Judiciária semelhantes àquelas que hoje tem o Judiciário.

Então, se não se dá essas garantias, vai-se permanentemente colocar a possibilidade de a Polícia Judiciária ser questionada quanto à sua imparcialidade e à sua condição de polícia republicana e polícia de estado.

Entendemos que se o pai do garantismo penal fala isso, e vemos na prática alguams situações peculiares, talvez seja importane repensar a questão da independência e da autonomia.

Aproveito a oportunidade para informar sobre um seminário na Academia Nacional de Polícia exatamente sobre a autonomia da Polícia Judiciária, para o qual convido todos a participarem, pois será bastante interessante.

Não vou me adiantar, até porque várias das questões podem ser respondidas pelos demais colegas. Acredito que em relação a este ponto é suficiente.

O SR. ELMER COELHO VICENTE - Sobre a questão de operações, fiquei muito feliz por terem citado a Operação Darkcode, uma operação na *deep web* contra um fórum de *underground* em que vimos criminosos brasileiros da mais alta *expertise* se relacionando mundialmente, e conseguimos chegar e identificar. Esse foi um trabalho de investigação muito forte, utilizando não só essa receita de bolo IP-usuário. Quando se fala de *deep web,* essa rastreabilidade do IP é uma conversa totalmente superada.

Então, a questão de ter outras técnicas e capacitação é muito importante. Contudo, a sensação de impunidade é tão grande, que o criminoso não está nem se preocupando em ir à *deep web*. Faço um desafio: vá ao Facebook e procure as palavras c*arder* e *banker.* Há verdadeiro comércio de artefatos maliciosos escancarado.

O SR. DEPUTADO DANIEL COELHO - Explique um pouquinho melhor para nós o que significam os termos citados.

O SR. ELMER COELHO VICENTE - Bom, a expressão adicionada de “er” é atribuída à pessoa que comete um crime. Por exemplo, *card* é cartão de credito;

carder é um especialista em fraude de cartões de créditos. *Banker* é um especialista em fraude de sistema bancário, em *internet banking*. Então, basta digitar esses termos em fonte aberta que se vai encontrar verdadeiro comércio, e não é nem na *deep web*, é na superfície. Vemos que esses criminosos não se preocupam sequer em mascarar o seu IP, não se preocupam em estar em uma rede aberta, não se preocupam em utilizar um dado falso para assinar uma conexão de Internet, não se preocupam em utilizar um servidor de anonimização para sua conexão.

Por isso, clamamos sempre pela obtenção dos *logs* do serviço, porque a resposta realmente tende a demorar. Quando já focamos num grupo, outros já surgiram. Não se trata de radicalizar o raciocínio e as analogias para se ter uma superproteção. É a própria sociedade, que, quando tem um problema e o apresenta às autoridades, clama para que ela seja bem instrumentada.

Mais do que a defesa da liberdade e da constituição do sistema democrático, sabemos quem são os eleitores de uma seção. Basta ir lá, há o número, os nomes. Por que isso é tão diferente para a questão da Internet, do *log*? E pelo *log* não se chega nem ao nome da pessoa, chega-se a uma máquina. Então, protege-se a privacidade de uma máquina? Além do mais, a obtenção vai, às vezes, inocentar uma pessoa.

Eu tenho certeza de que houve o convencimento dos que já saíram.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Na verdade, está havendo outra votação nominal. Então, acho que, se possível, poderíamos até aguardar aqui...

O SR. DEPUTADO NELSON MARCHEZAN JUNIOR - Se V.Exa. puder suspender a reunião por 5 minutos, Sra. Presidenta, acho que seria bom.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Vou suspender a sessão por 5 minutos. É o tempo de todos irem votar e voltarem.

(A reunião é suspensa.)

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Vamos reabrir a nossa reunião.

Dando continuidade à reunião, com a palavra o Dr. Elmer Coelho Vicente.

O SR. ELMER COELHO VICENTE - Ultrapassando a questão da privacidade, que outras operações a Polícia Federal realizou com relação a crimes eletrônicos?

Bom, foi realizada a Operação Ctrl C, de fraude bancária também. Houve 21 prisões. Houve a Operação Maracatu Virtual, em Pernambuco. Houve a Operação Araceli, referente à pornografia infantil.

A Polícia Federal sempre tem uma série de ações que, às vezes, também, não se chamam operação, não ganham notoriedade por não abrangerem, por não ganharem a rubrica de um nome, mas, paulatinamente, elas vêm cumprindo diversas ações ostensivas de Polícia Judiciária, de prisões e repressões.

Deixo bem claro um número: 20 policiais na Polícia Federal de crimes cibernéticos são 20 policiais nos grupos que atuam exclusivamente com crime cibernético. É óbvio que vai haver, por exemplo, um crime de venda de animal pela Internet, e vai atuar um policial da Delegacia de Meio Ambiente que cumula isso com outras funções. O próprio Dr. Stênio tem outras funções que dizem respeito não só ao crime cibernético. Ele recebe inquéritos de outras matérias. Então, essa questão de 20 policiais é do Grupo de Repressão a Crimes Cibernéticos dos Estados que conseguem atuar exclusivamente nessa matéria.

Quanto à questão falada da *deep web*, eu já comentei um pouco sobre ela. Realmente, existe uma tendência de a criminalidade migrar para a deep *web*. A partir do momento em que a criminalidade vai sendo descoberta, ela vai procurando verificar onde errou e o que poderia fazer diferente.

Temos visto cada vez mais a utilização de anonimização de navegação e a utilização de criptografia. A utilização de criptografia, às vezes, se o usuário não foi tão cauteloso em jogar nas nuvens as suas informações, e se vai a casa e se pega a informação dele criptografada, a quebra da criptografia demanda um poder computacional muito grande, e o ciclo de implementação da força dessa criptografia aumenta a cada ano, e isso importa em, a cada ano, aumentar o seu poder computacional para quebrar a criptografia.

Hoje em dia qualquer serviço vai ter criptografia nas nuvens também. Então, assim, precisamos de instrumentos para poder também quebrar a criptografia.

Na relação entre Polícia Federal e Polícias Estaduais, na verdade, isso cai na questão das atribuições dos crimes cibernéticos. Como eu comecei aqui minha participação, existe uma dificuldade muito grande de se fixar incialmente qual Polícia vai ser responsável pela investigação daquele delito. Geralmente, é feito como o Dr.

Sobral falou, onde é mais próximo da vítima. Sobrecarregam-se os grandes centros, e essa quantidade enorme de notícias-crimes que chegam, às vezes, a Polícia não consegue tratar. Para saber a destinação e de onde partiu aquela conexão, precisa haver quebra da judicialização. Realmente, isso precisa ser equacionado, porque, às vezes, a própria empresa, o serviço eletrônico tem a notícia de que está ocorrendo um crime, mas ela não sabe para quem mandá-la.

Na questão das redes abertas, das *wi-fis*, das *lan houses*, sente-se falta de uma legislação nacional de obrigatoriedade de cadastro, da qualidade desse cadastro ou, como o Dr. Stênio mencionou, no caso de uma *wi-fi,* de quais elementos, além do IP, podem ser logados para se fazer a rastreabilidade, como, por exemplo, o endereço MAC. Realmente, há essa questão quando nos deparamos com um IP e chegamos a uma *lan house*. Não existe segredo. Chegou a uma *lan house*, travou. Se não conseguirmos uma filmagem, se a pessoa não se lembrar, simplesmente falam assim: *"Olha, clientes entram e saem todos os dias daqui"*. Se não houver outros elementos de investigação, essa linha reta de rastreabilidade é encerrada ali.

Na questão da prevenção do setor bancário, o Brasil é um dos maiores países de *malware* bancário, de distribuição de *malware* bancário na Internet. Combate de *malware* bancário não tem, na questão da prevenção do usuário, é antivírus. Existe até hoje um esforço da indústria com os bancos de como os antivírus podem melhorar essa resposta para o usuário. Nem todo usuário instala antivírus, nem toda empresa de antivírus é brasileira. Ou seja, para os *malwares* do sistema bancário brasileiro, demora-se a se chegar a uma vacina para aquele sistema. Então, hoje existe uma preocupação para que haja uma melhor detecção desses vírus e uma mais rápida assimilação da vacina daquele vírus. Hoje em dia até empresas de *software* operacional têm buscado introduzir mecanismos para limpar o sistema contra os *malwares.* Na verdade, o saneamento do sistema passa também pela conscientização do usuário, passa pela criação de uma cultura de se proteger na questão do antivírus. Isso de uma forma muito sintética, muito rasa.

Foi mencionado o que se poderia seguir como atitude de sugestão. Eu gostaria de fazer uma sugestão: pesquisa, mapeamento de processo para saber efetivamente quanto tempo o processo está demorando na Justiça, quanto tempo a

resposta está demorando no provedor para chegar e se essa resposta atende ou não. Realmente, na hora de definir o nosso meio ambiente, o nosso cenário, existe uma carência muito grande. Eu já vi pesquisas muito boas. Consegue-se criar instrumentos muito bons para conhecer o cenário, só que isso nunca foi feito a respeito dos crimes cibernéticos, nem dos processos-crimes referentes aos crimes cibernéticos, até porque isso implica um pouco na falta de dados estatísticos de crimes cibernéticos. Não existe só a questão dos crimes cibernéticos puros, em que se conseguiria fazer uma estatística. Hoje, a maioria dos crimes é impura.

Foi perguntado sobre qual a maior incidência. Eu poderia citar que a maior incidência hoje é a fraude bancária, a distribuição de pornografia infantil, o crime contra a honra e a questão do crime contra o consumidor, principalmente nessa questão de comércio eletrônico, em que se veem muitas pessoas comprando de empresas que não entregam. *Sites* são criados só para atrair aquele consumidor, obter o seu dinheiro, mas não entregam a mercadoria. É um pouco o que o Dr. Stênio disse: hoje em dia qualquer um cria um *site.* Se você quiser criar um *site* para oferecer um computador, não precisa ser muito abaixo do preço, levemente abaixo do preço, para não chamar muito a atenção, aquilo vai ser atrativo. A população está atrás de qualquer desconto. Ela vai atrás do que puder economizar, não importando se aquele *site* é conhecido ou não. É um *site* bem feito, visualmente agradável, tem uma navegabilidade boa, isso já vai ganhando a confiança do usuário. Com isso, ele cai num estelionato. Esse estelionato é muito grande.

O SR. DEPUTADO NELSON MARCHEZAN JUNIOR - Fraude bancária, pedofilia, comércio eletrônico e...

O SR. ELMER COELHO VICENTE - Crime contra a honra. Não sei se eu fiquei devendo alguma resposta.

O SR. DEPUTADO JOÃO ARRUDA - Os números. Não sei se o senhor tem acesso a esses números, para sabermos quantos crimes, no Brasil, em média, ainda não foram desvendados pelo trabalho da polícia de investigação, o que se superou hoje, de tudo o que foi de pedido de investigação e o que ainda está por ser desvendado.

O SR. ELMER COELHO VICENTE - Bom, a questão da cifra, tanto de sucesso do inquérito policial quanto o que não foi investigado, nós não temos. A própria questão hoje...

O SR. DEPUTADO JOÃO ARRUDA - Do que foi investigado.

O SR. ELMER COELHO VICENTE - Quanto ao investigado, eu caio naquela dificuldade que eu vou lhe falar. Meu sistema de estatística hoje fala o seguinte: furto mediante fraude, tantos inquéritos. E nós temos uma indicação de porcentagem de sucesso daquele inquérito. Só que eu não consigo diferenciar se esse furto mediante fraude, hoje, é específico de fraude bancária ou não.

A Polícia Federal já está sensível a essa questão de refinamento da sua estatística. Nós já estamos trabalhando num sistema de inquérito policial em que vai haver uma camada gerencial para colhermos melhor esses dados estatísticos e, em breve, nós já vamos usá-lo. O piloto vai ser feito já neste ano, mas hoje eu não consigo fazê-lo.

O SR. DEPUTADO JOÃO ARRUDA - De cada dez crimes que chegam à polícia para serem investigados, quantos vocês conseguem resolver, em média? Você não consegue me responder isso?

O SR. ELMER COELHO VICENTE - Consigo responder.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Claro, Dr. Stênio Santos.

O SR. STÊNIO SANTOS - Em relação a esses dados estatísticos da Polícia Federal, de um modo geral, nós vamos ter, no dia 20 de outubro, uma palestra especificamente sobre estatísticas. O que eu posso adiantar é que nós temos uma taxa de elucidação de nível de país desenvolvido — talvez melhor, de um modo geral. Não chega a 90%, porque isso é irreal, 90% é quase impossível. Mas está para lá de 50% a 60%, que é uma taxa excelente, em termos de investigação criminal. Mas esses números vão ser informados, no dia 20, na Academia Nacional de Polícia, nesse seminário da Polícia Judiciária.

O SR. DEPUTADO JOÃO ARRUDA - Sra. Presidente, sem querer atrapalhar e estender muito, é importante saber o que não tivemos do sucesso, por que não tivemos o sucesso e se a legislação pode ser aprimorada no sentido de que haja sucesso.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Se o Dr. Carlos puder dar essa reposta para podermos concluir...

Passo a palavra ao Dr. Carlos Eduardo Miguel Sobral.

O SR. CARLOS EDUARDO MIGUEL SOBRAL - Vou ser bastante rápido, em virtude do adiantado da hora. É sempre delicado participar de uma audiência pública ou debate sobre problemas na Internet. Poderíamos passar dias e dias falando das virtudes da Internet, mas o nosso papel aqui é pontuar aquilo que não está dando certo.

Vou enfrentar as questões e entro na pergunta que V.Exa. fez. Sobre pedofilia na Internet, o Sr. Deputado Leo de Brito fez uma indagação. Hoje nós não temos notícia ou é muito pequeno o número de notícias informando que a falta de uma tipificação de uma conduta vem atrapalhando uma investigação ou punição. Então, não há, não tenho conhecimento disso, e, nos últimos anos, se aconteceu, vai ser exceção da exceção, um número muito pequeno.

A legislação, no caso da pornografia infantil, da pedofilia na Internet, nos atende. Uma mudança foi feita em 2008, criminalizaram-se algumas condutas, principalmente a posse de material pornográfico, que não era crime em 2008. Essa conduta foi criminalizada. Então, hoje é crime possuir, adquirir, assediar criança para que pratique ato libidinoso, inclusive através de meios de tecnologia da informação. Então, a legislação penal, com autorização do Estatuto da Criança e do Adolescente — ECA, atende a isso.

A SaferNet é uma ONG de proteção à criança e ao adolescente, nós a conhecemos na época da CPI da Pedofilia. A Polícia Federal fez um acordo de cooperação técnica, há uma parceria com a SaferNet e com a Secretaria Extraordinária de Direitos Humanos, a Secretaria Especial de Direitos Humanos, a Presidência da República.

A SaferNet tem uma central de notícias para crimes envolvendo violação a direitos humanos. Ela recebe as notícias dos usuários, que são feitas através de um sistema que eles disponibilizam na rede, e replica essa notícia de crime ao Ministério Público e à Polícia Federal. Então, começa um pouco o problema de atribuição, porque, tão ruim quanto não investigar é haver duas ou três instituições fazendo a mesma investigação. Também isso atrapalha bastante.

A notícia de crime que é encaminhada ao Ministério Pública Federal em São Paulo é encaminhada à Polícia Federal. Normalmente, gera-se uma investigação em São Paulo, o Ministério Público gera uma investigação na Polícia Federal. A nossa, na Polícia Federal, pode ser mandada para um local e a do Ministério Público, se não avançar, é encaminhada para a Superintendência da Polícia Federal em São Paulo. Isso também pode ser mandado para os Ministérios Públicos dos Estados. Ou seja, vira uma confusão imensa a multiplicação das investigações. Hoje, uma pessoa faz a notícia para a polícia e para várias instituições, para as Polícias Civis e para o Ministério Público. Então, nós podemos ter 50, 60 investigações sobre o mesmo fato.

Se formos discutir a atribuição, é lógico que vamos ver que a atribuição primária, para conhecer e investigar, é da polícia. Então, no caso, a Polícia Federal deveria ter prioridade para fazer a investigação, e, quando for exceção, o Ministério Público realiza a investigação, mas hoje ela é multiplicada. Então, a atribuição dos entes federados, também com relação aos Estados, gera um complicador, que é a multiplicidade das investigações.

Principais crimes cibernéticos que são praticados, em gravidade e em volume: a pornografia infantil é grave e tem volume; a fraude bancária é grave e tem volume. Outros crimes: estelionatos, crimes contra a honra, que tem gravidade para a pessoa ofendida. Para ela, talvez aquele crime seja mais importante do que todos os outros, pois é ela que está sendo ofendida e violada. Mas não há um volume, não há um crime organizado ou uma estrutura organizada para a prática desse delito. A mesma coisa ocorre com o estelionato. As pessoas vendiam em banquinha nas ruas, montaram um *site* na Internet, oferecem a venda do produto, e não o entregam. Muitas vezes, é venda de produto ilegal, como medicamento abortivo, anabolizante, droga. O que acontece nesses casos é que, normalmente, a vítima não reclama. Ela não procura a polícia e fala: *"Comprei um anabolizante, e não me entregaram"*. Então, esse crime não chega ao conhecimento das autoridades.

O SR. DEPUTADO NELSON MARCHEZAN JUNIOR - E quanto à propriedade intelectual, há um volume considerável?

O SR. CARLOS EDUARDO MIGUEL SOBRAL - Hoje, a sociedade já aceita isso. E o mercado também já se adequou a isso. Se nós formos analisar, de forma

literal, o art. 184 do Código Penal, que diz que violar direito do autor é crime, então, qualquer compartilhamento poderia, em tese, ser crime. Há um volume imenso. Hoje, houve uma acomodação, no entendimento nacional, de que determinadas condutas são socialmente aceitas e, nesse caso, o próprio mercado se adaptou. Desse volume, só é considerada a venda de material de forma ilícita. Se tirar o compartilhamento feito pelas pessoas, o volume é menor, mas ainda é um volume considerável, ou seja, também acontece. Se se considerar o compartilhamento, o volume é altíssimo, mas, se se tirar o compartilhamento por pessoa, sem intuito de lucro, a quantidade já é bem menor.

Quanto à taxa de elucidação, nós não temos esses dados de forma concreta, mas uma coisa é real: se nós não tivermos estrutura para investigar, a taxa de investigação é baixíssima, porque a notícia chega e fica parada, pois não há ninguém para investigar. Na investigação, as pessoas têm que agir. Nós temos que ir atrás das informações, às vezes, buscá-las fora ou dentro do País, com auxílio do Judiciário, e às vezes, não, mas é preciso que haja pessoas. Se houver cem investigações para um delegado e quatro agentes, a taxa de elucidação será baixíssima. Se houver uma investigação para um delegado e para quatro agentes, a taxa de elucidação será de 100%. Ela vai ser apurada, mesmo se a conclusão for de que não há crime; ou seja, ele foi investigado.

O que acontece muito é que há muitas investigações em andamento, mas nem sempre as mais importantes estão em andamento; elas se misturam com as menos importantes. Nós dividimos essas investigações com recursos extremamente limitados, pequenos. Quando há muitos casos para apurar e uma estrutura muito pequena, a tendência é que a taxa de elucidação seja baixa, mesmo porque, quando há um volume muito grande de investigação para fazer, o tempo dela é demorado. E, quanto mais longa é uma investigação, quanto mais distante ela é do dia zero do crime, mais difícil fica chegar à autoria e comprovar a materialidade do delito. Ou seja, a investigação tem que ser rápida, tem que ser instantânea. O fato tem que chegar e tem que se investigar. Se houver um volume muito grande, ele é colocado na fila, para se investigar o fato mais antigo. Aí, quando se chegar a essa investigação que chegou agora, ela já ficou velha, ou seja, já se perdeu a oportunidade de investigá-la.

Então, a taxa de elucidação é diretamente proporcional à estrutura de investigação. Isso vale para crime cibernético, para crime financeiro, para investigação de homicídio, ou seja, vale para qualquer tipo de delito. Se não houver estrutura, a taxa vai ser necessariamente baixa.

Quanto à taxa de reincidência, é incomum nós realizarmos uma investigação, principalmente no âmbito das fraudes bancárias, em que o autor já não tenha sido preso antes; é incomum. É comum que ele seja reincidente, às vezes, pela terceira, quarta, quinta vez. É comum; você o prende de novo, ele é punido, às vezes, com uma pena razoável de 1, 2 anos, ele sai, volta a delinquir, é preso de novo, é condenado de novo, sai e volta a delinquir, é preso de novo, é condenado de novo, sai e volta a delinquir.

Essa é uma constante no Brasil. A nossa taxa geral é de 70%. Na área de fraude bancária, ela vai para 90%. Ou seja, a pessoa é presa, e nós conseguimos recuperar parte do dinheiro. É uma ilusão achar que nós recuperamos todo o dinheiro. Não recuperamos. Isso é difícil, mesmo porque ele é pulverizado, é gasto.

Então, se a pessoa desvia 10 milhões de reais, e conseguimos recuperar 1 milhão de reais, ela sente que conseguiu ter lucro de 9 milhões de reais, passa um tempo presa e volta a fazer a mesma coisa. Ela teve lucro de 9 milhões de reais com a atividade, ela vai fazê-la de novo. Essa é uma realidade que nós temos que enfrentar.

Qual é a solução? Nós temos que estudar. Se o encarceramento não é uma medida viável, nós temos que ter outro mecanismo de monitoração eletrônica, de restrição à liberdade. Mas o fato é: a pessoa não pode ser presa, processada, condenada e voltar ao sistema criminal, voltar ao crime. Isso aí gera um ciclo vicioso que nós não temos condições de aguardar.

A investigação na *deep web* é necessariamente dependente de pessoas. Nós precisamos de policiais investigando a *deep web*. Não dá para fazer rastreamento de IP lá dentro. Nós vamos ter policiais lá para identificar quem está vendendo material pornográfico, quem está oferecendo prática de homicídio, quem está oferecendo droga e para se relacionar com essa pessoa, marcar o encontro, identificar, prender e promover a investigação. Não dá para fazer investigação via sistema, via IP, essas coisas. Então, para promover a investigação na *deep web*, é

necessário efetivo, são necessários recursos humanos. Se nós não tivermos recursos humanos, não vai haver investigação na *deep web*. Não há como fazer isso via quebra de IP, isso é humanamente impossível.

Quanto à dificuldade de mapear autores de pornografia infantil, como nós não temos as informações de *logs*, de acesso, de conexão, não conseguimos jogar essas informações no sistema, conforme nós fazemos com as fraudes bancárias.

No caso da fraude bancária, eu sei. Eu consigo lhe dar hoje as informações de onde está a vítima, para onde foi o dinheiro, quando aconteceu. Por quê? Porque nós temos um sistema.

No caso de pornografia infantil, nós recebemos as 50 mil comunicações dos Estados Unidos, por exemplo, mas não conseguimos ter acesso aos dados cadastrais, aos *logs*, de forma automatizada, em sistema, em lote. Nós não conseguimos jogar isso no nosso sistema de inteligência. Nós não conseguimos enxergar. Nós não sabemos se há um grupo organizado, onde estão as pessoas. Nós estamos no escuro, exatamente porque nós não conseguimos tratar essa informação.

O IP é suficiente para a elucidação do crime? Não! Às vezes, ele é o ponto de partida, mas nunca é o ponto de chegada. Ele pode ser o início de uma investigação, pode ser o ponto pelo qual vamos começar a puxar o fio do novelo, mas nunca é o ponto de chegada.

Então, na verdade, sem o IP, não se pode ter esse ponto de partida — pode ter outros —; ponto de chegada o IP nunca é. Assim, quando há dificuldade já para começar, chegar ao final é um desafio ainda maior.

Quanto à *lan house*, nós temos essas dificuldades que o Dr. Elmer apresentou, mas o número de crimes praticados em *lan house* não é alto. Normalmente, o crime organizado não usa *lan house* para agir. Ou ele monta a sua *lan house* — e é uma situação diferente —, ou ele usa uma conexão mascarada. Mas o crime organizado, normalmente, não usa uma *lan house*.

Pode ser que alguma pessoa que queira praticar um crime contra a honra — aí, sim — vá a uma *lan house*, abra um perfil e faça a sua ação ilícita. Isso acontece, pode acontecer. Mas, no crime organizado, em volume, a *lan house* não seria o

maior dos nossos problemas. É lógico que ela é um ponto de atenção, é algo a ser avaliado.

Antes de terminar, eu vou me aventurar a responder uma questão delicada: segurança cibernética. Esse é um assunto extremamente profundo, extremamente sério. Eu tive a oportunidade de instaurar o inquérito que investigou a interceptação dos dados da Presidente Dilma, das informações brasileiras, para investigar as denúncias feitas pelo Snowden. Presidi esse inquérito, compartilhei com o colega.

Essa é uma situação bastante delicada, porque nós tratamos de inteligência de Estado. E, quando tratamos de inteligência de Estado, não estamos tratando mais de crime organizado, nós estamos num nível extremamente mais elevado, que é o da segurança nacional, da segurança da própria existência do Estado.

Há uma disputa internacional muito grande — Estados Unidos, Europa, China, Rússia —, e é nesse contexto que nós entramos na espionagem de Estado. Ou seja, nós usamos equipamentos que não são nacionais, na sua grande maioria — são equipamentos americanos, chineses, russos ou europeus. E esses equipamentos, normalmente, têm um *backdoor*, ou seja, têm uma porta de saída que pode ser aberta. É o que se diz: pode ser aberta.

E a solução é deixar de usar esse equipamento, voltar à reserva de mercado de 1990, ou seja, ao atraso tecnológico? A solução é não usar? Ou a solução é tentar acordos internacionais, nos quais haja o compromisso de não se usar essa possibilidade? Mas esse compromisso vai ser realmente cumprido ou os Estados vão continuar acessando as informações? Essa é uma situação delicada.

Qual foi o recado? Houve até uma CPI — não sei se foi a CPI da Espionagem —, cuja Presidente, acho, foi a Vanessa Grazziotin, que discutiu esse tema, e o recado foi claro: protejam-se. Protejam as suas informações; protejam os seus dados; criem criptografia do Estado brasileiro — o Governo, por meio do Gabinete de Segurança Institucional — GSI, com o Exército, tem desenvolvido pesquisas nesse sentido —; desenvolvam técnicas para proteger os dados; criem os seus próprios antivírus.

Enfim, protejam as informações, porque o risco de uma interceptação ou de uma inteligência de Estado vai continuar existindo, mesmo porque as informações passam por satélites — os satélites normalmente não são nossos —, passam por

fibras, por cabos submarinos, que passam pelos Estados Unidos ou por algum outro país. Ou seja, o dado trafega.

Então, se nós não tivermos condições de proteger essas informações no meio, vamos começar a discutir propostas que não são viáveis nem interessantes sob o ponto de vista do desenvolvimento nacional. Portanto, esse assunto é bastante delicado.

E o que o Brasil está fazendo? Tentando se proteger. O Centro de Defesa Cibernética — CDCiber promoveu algumas jornadas para desenvolver a tecnologia nacional. Houve tentativas de acordos de cooperação ou de respeito mútuo da Presidência com o Presidente dos Estados Unidos. Enfim, realmente hoje o mundo está conectado, e nós consumimos tecnologia estrangeira. Então, pode acontecer, sim, de as nossas informações serem interceptadas.

Nós vamos deixar de usar essas tecnologias? Eu não me lembro de pessoas que deixaram de usar nem rede social, nem *e-mail*, nem outra tecnologia, depois da informação do Snowden. Nós continuamos usando. Eu uso o Facebook, uso o Twitter, uso o Telegram, uso o WhatsApp, uso *internet banking*.

O SR. DEPUTADO NELSON MARCHEZAN JUNIOR - Esse inquérito foi concluído?

O SR. CARLOS EDUARDO MIGUEL SOBRAL - Foi concluído. Não se conseguiu a materialidade da interceptação. Nós tivemos acesso àqueles arquivos de Power Point que foram disponibilizados, mas não houve conteúdo.

Nós também fizemos estudos, chamamos diversas instituições públicas e privadas para ajudar a estudar a estrutura da comunicação brasileira, e a conclusão foi esta: temos que nos proteger, porque os equipamentos e a estrutura de telecomunicação do País são também dependentes de tecnologia estrangeira. Essa foi uma decisão nossa no passado e talvez seja a mais interessante. Não sei. Isso é algo que o País tem que estudar.

Só para concluir, qual é a esperança, como brasileiro, em relação ao produto desta CPI? Como brasileiro, que resultado eu gostaria que a CPI tivesse? Primeiro, um estudo do problema. Nós temos que saber quais são os problemas envolvendo a tecnologia e o uso da Internet no País. É fraude? É segurança cibernética? É pornografia infantil? É estelionato? É propriedade intelectual?

Dado o diagnóstico do problema, é preciso identificar o que nós estamos fazendo para resolvê-lo, quais são as medidas que as instituições brasileiras estão adotando para resolvê-lo e, se não estiverem adotando alguma, como podem vir a adotar no médio, curto e longo prazo, para que realmente consigamos avançar e, daqui a alguns anos, passar a tratar outros problemas, e não os mesmos que estamos tratando já há um bom tempo.

Como os outros países avançaram? Com muita tecnologia, investimento e cooperação. É muito comum fora do Brasil a cooperação entre Estado, iniciativa privada e sociedade civil. Nós ainda temos um pouco de resistência a essa relação mais próxima entre instituições públicas e privadas.

Talvez tenhamos que quebrar algumas resistências e trabalhar de forma cooperada, todo mundo atuando junto, sem esquecer jamais educação, conscientização e prevenção — educação para que as pessoas saibam usar a tecnologia de uma forma mais segura, educação para que as pessoas não se sintam à vontade e motivadas a violentar outras pessoas através da tecnologia. Às vezes, você está na sua casa, alguém lhe agride, você resolve revidar, ou agredir através da rede, e isso se perpetua. As pessoas têm que ter consciência da lesão que isso pode causar.

Nós também temos que ter o entendimento de que todo o mecanismo de prevenção gera uma restrição ao usuário. Antigamente, falávamos: *"Olha, se você receber um e-mail não abra, se ele for de pessoa desconhecida".* Os criminosos passaram, então, a coletar a sua lista de contatos e a mandar um *e-mail* como uma pessoa conhecida. Aí, a orientação foi: *"Não abra e-mail nem se for de pessoa conhecida".* Eu falei: *"Então, como é que faz?" "Não, liga antes, para saber se ela mandou o e-mail".* Ou seja, quando tratamos de prevenção, às vezes, exageramos, no sentido de restringir a liberdade dos usuários. Isso também não dá certo.

Nós temos que ter tecnologias para conseguir prevenir, como o uso do antivírus, mas isso gera um custo para o usuário, que, às vezes, não quer assumir esse custo. Às vezes, é preciso trocar o equipamento, porque o antivírus teve que ser tão forte e tão pesado para conseguir conter as ameaças que não roda no equipamento. E é preciso trocar o equipamento. Troca-se o celular, depois, isso vai

ficando mais pesado, tem que trocar de novo. Ou seja, a prevenção também tem certo limite, ela não é um elixir, ela vai até certo ponto, mas ajuda.

Empresas e instituições participam na proteção. Hoje o Brasil investe muito. A FEBRABAN informa que são quase 10 bilhões de reais de proteção da informação em tecnologia, uma quantia alta, e as empresas investem muito.

As pessoas estão se conscientizando dos riscos, mas, no final, voltamos para aquela nossa fase inicial: precisamos melhorar a nossa estrutura. As instituições privadas avançaram, a proteção avançou, a educação avançou, há vários projetos e políticas públicas de educação e uso seguro da internet, mas infelizmente o nosso lado da investigação talvez tenha sido o último a receber o impulso que precisava para poder chegar ao mesmo nível.

Se conseguirmos, como produto desta CPI, que se faça o estudo desse problema e se proponham soluções para avançarmos, em médio e curto prazo, teremos alcançado o que esperamos desse trabalho.

Muito obrigado.

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

Gostaria de perguntar se todos foram contemplados com as respostas.

Agradeço ao Dr. Stênio, ao Dr. Elmer e ao Dr. Carlos, por terem vindo aqui responder e explicar um pouco a Operação IB2K. E o tema acabou sendo bem mais abrangente. Entramos em assuntos que dizem respeito às nossas sub-relatorias.

Para a nossa primeira audiência, acho que foi um grande passo para esta CPI. O Deputado Leo de Brito e outros colegas solicitaram que tivéssemos uma visão mais ampla sobre esse assunto. Acho que hoje conseguimos falar um pouco sobre cada assunto ligado a esses crimes cibernéticos. Então, agradeço-lhes.

Devido ao início da Ordem do Dia, vamos deixar as votações de requerimentos para a próxima terça-feira.

Nada mais havendo a tratar, declaro encerrada a presente reunião, antes convocando reunião deliberativa ordinária para a próxima terça-feira, 25 de agosto, às 14 horas, em local a ser informado na página da Comissão e encaminhado aos *e-mails* institucionais.

Está encerrada a presente reunião.