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: 1723/15	DATA: 15/09/2015	
LOCAL: Plenário 11 das Comissões	INÍCIO: 15h26min	TÉRMINO: 18h38min	PÁGINAS: 66

DEPOENTE/CONVIDADO - QUALIFICAÇÃO
ANDRÉ ABREU MAGALHÃES - Perito da Polícia Federal. LEONARDO BUENO DE MELO - Representante do Instituto Nacional de Criminalística — INC. EVANDRO MÁRIO LORENS - Representante do Instituto Nacional de Criminalística — INC. ALESSANDER FLORINDO DA SILVA - Representante do Instituto Nacional de Criminalística — INC. BRUNO TELES - Presidente da Associação Brasileira de Criminalística — ABC.

SUMÁRIO
Debate sobre a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade brasileira, tema objeto da CPI.

OBSERVAÇÕES
Houve exibição de vídeos. Houve exibição de imagens.

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

Declaro aberta a 12ª Reunião Ordinária de Audiência Pública da Comissão Parlamentar de Inquérito que investiga a prática de crimes cibernéticos.

Encontra-se à disposição dos senhores membros a cópia da ata da 11ª Reunião, realizada no dia 10 de setembro de 2015. Pergunto se há necessidade de leitura da ata.

O SR. DEPUTADO BRUNO COVAS - Sra. Presidente, peço dispensa da leitura da ata.

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

Em discussão a ata. *(Pausa.)*

Não havendo quem queira discutir, em votação a ata.

Todos que aprovam a ata permaneçam como estão. *(Pausa.)*

Aprovada.

Comunico o recebimento dos seguintes documentos:

Ofício nº 193, de 2015, do gabinete do Deputado João Arruda, que *"justifica a ausência do Deputado na reunião do dia 8 de setembro de 2015"*.

Oficio da Procuradoria Regional da República da 2ª Região, que "*encaminha os dados estatísticos dos grupos do Ministério Público Federal de combate aos crimes cibernéticos"*.

A reunião de hoje tem como objetivo audiência pública com a presença de peritos da Polícia Federal que atuam na apuração de crimes cibernéticos. A audiência dá consequência à aprovação do Requerimento nº 38, de 2015, de autoria do Deputado João Arruda, e do Requerimento nº 67, de 2015, de minha autoria.

Agradeço a presença dos convidados que se dispuseram a colaborar com a realização desta audiência. Desde já, convido para compor a mesa o Sr. André Abreu Magalhães, Perito da Polícia Federal que participou das Operações Proteja Brasil, Darknet e Gênesis *(pausa)*; o Sr. Leonardo Bueno de Melo, que representa o Instituto Nacional de Criminalística *(pausa)*; o Sr. Evandro Mário Lorens, que também representa o Instituto Nacional de Criminalística *(pausa)*; e o Sr. Bruno Telles, Presidente da Associação Brasileira de Criminalística. *(Pausa)*

Cada convidado disporá de 15 minutos para sua apresentação. Ao final das exposições, será passada a palavra ao Relator, aos Sub-Relatores e aos autores dos requerimentos. Os convidados responderão a esse bloco de indagações. Em seguida, pela ordem da lista de inscrições, os senhores membros poderão interpelar os convidados, por até 5 minutos. Os expositores responderão a mais esse bloco de indagações, podendo haver réplica. Por fim, haverá as considerações finais. *(Pausa.)*

Gostaria também de convidar o Sr. Alessander Florindo da Silva, representando o Instituto Nacional de Criminalística. *(Pausa.)*

Ao iniciar os nossos trabalhos, concedo a palavra ao perito da Polícia Federal, André Abreu Magalhães.

O SR. ANDRÉ ABREU MAGALHÃES - Primeiramente gostaria de agradecer a todos pela presença e agradecer o requerimento da Deputada Mariana Carvalho, em nome de quem cumprimento todos os demais presentes.

O tema que eu vou abordar é um crime cibernético que, infelizmente, é um dos líderes nas estatísticas em crimes cibernéticos: a exploração sexual infantil na Internet ou pornografia infantil na Internet.

Talvez uma definição clássica desse tema, do ponto de vista profissional de muitos, seria a posse ou divulgação de imagens contendo cenas de sexo explícito envolvendo menores de idade. Porém, durante a minha labuta, eu consigo estabelecer uma classificação um pouco mais profissional sobre esse tema, que seria: a divulgação de cenas de sexo explícito ou estupros praticados contra crianças e adolescentes através da Internet. Porque eu falo em estupro ou exploração sexual? Porque, se não houvesse a exploração física ou o abuso sexual dessas crianças, não existiriam imagens e, portanto, não haveria exploração sexual infantil e não haveria crime cibernético.

Quando se fala em pornografia infantil na Internet, para quem não está acostumado a lidar com esse tipo de crime, vêm-lhe à cabeça adolescentes. Mas infelizmente, esta não é a nossa realidade: quem lida com esse tipo de crime ou produz qualquer meio de prova a respeito, de pronto fica convencido de que se trata de imagens de estupros envolvendo, na sua grande parte, crianças e até mesmo bebês de colo.

Quem são essas pessoas que fomentam o mercado da pornografia infantil na Internet? Não existe um público específico e nem classe social: são pessoas maiores, pessoas menores, bastando apenas ter acesso a um dispositivo que se conecte à Internet.

Durante a minha *expertise* profissional, eu consegui estabelecer uma classificação para os tipos de consumidores de pornografia infantil na Internet, aquelas pessoas que visualizam, que gostam, que armazenam pornografia. E eu fiz uma classificação em três tipos — é uma classificação profissional minha: eu as classifiquei como iniciantes, amadoras e profissionais.

Quem seria o iniciante? Seria aquele que, de forma exaustiva, através dos próprios buscadores convencionais, procura imagens relacionadas a outros assuntos que o levem a ter contato com imagens de crianças exibindo seus órgãos genitais. Por exemplo, se eu utilizar um dos nossos buscadores convencionais e digitar *"doenças na vagina de crianças"*, eu vou ter como resposta alguma cena que porventura possa caracterizar uma cena de sexo explícito envolvendo uma criança ou um adolescente. Esses são os iniciantes.

Os iniciantes também são frequentadores dos fóruns de bate-papo. Existem vários fóruns na Internet em que pessoas procuram pornografia adulta. E nesses fóruns, outros ficam incentivando ou fazendo apologia, para que essas pessoas acessem uma pornografia ilícita, que seria a pornografia infantil. Essas pessoas, ao entrarem nesses fóruns, são chamadas para participar de algum grupo mais específico. E, daí, elas já têm outra classificação: passam a ser consumidoras com a classificação que eu digo de amador.

Então, o que seria os amadores? Seriam aqueles consumidores que, através da instalação de aplicativos de compartilhamento de arquivos pela Internet, realizam buscas através de termos específicos. Ou seja, durante a fase de iniciação, esse consumidor aprende que, se instalar alguns aplicativos de compartilhamento de arquivos — que são aplicativos amplamente divulgados, como eMule, Ares Galaxy, dentre outros, e de fácil obtenção na Internet — e se fizer pesquisas sobre alguns termos específicos, ele vai ter como resposta pornografia infantil.

Um exemplo dessas pesquisas que eles realizam é a procura pelo termo "pedofilia". Se você entrar em alguma dessas redes de compartilhamento de

arquivos e digitar a palavra “pedofilia”, consequentemente vai ter uma resposta, uma imagem ou um vídeo envolvendo a exploração sexual de crianças ou adolescentes.

No decorrer dessa busca, cada vez mais eles vão se especializando. Existem outros termos que encontramos bastante durante a atividade pericial e que seriam alguns dos mais apurados, como PTHC ou *hardcore*. Inevitavelmente, se você digitar um desses termos nessas redes de relacionamento, ele vai retornar a você algum tipo de pornografia, especificamente pornografia infantil por conta do termo. Por exemplo, PTHC significa *pre-teen hardcore*, que seria sexo com pré-adolescentes.

Existe até um estudo sobre esses termos feito por uma universidade estrangeira, que eu vou disponibilizar para vocês. Uma universidade estrangeira fez o seguinte estudo sobre esses termos nas redes ponto a ponto, que são as redes de compartilhamento: ao se digitar esses termos, qual percentual de pornografia infantil apareceria; em que a combinação desses termos melhoraria as consultas. Então, hoje é muito fácil obter pornografia infantil na Internet.

Elevando o nível e saindo dessas redes de compartilhamento, que seriam redes de compartilhamento abertas, o consumidor de pornografia infantil passa a querer algo mais. É aí que eu começo a classificá-lo como profissional.

O que seria o consumidor profissional? Seria aquele que participa de grupos restritos nas redes de compartilhamento de arquivos de forma criptografada, nas quais seus usuários precisam ser indicados e apresentar conteúdo pornográfico infantil para se manter dentro do fórum. Por exemplo, no estágio amador, o consumidor descobre que existem grupos fechados, em relação aos quais precisa de uma indicação de alguém lá presente para poder participar. Ou seja, eles querem ter a garantia do quê, por exemplo? De que aquele consumidor não seja um membro da Justiça que esteja investigando. Então, seria uma estrutura fechada e que, por conta da criptografia existente em alguns aplicativos de compartilhamento, pode dificultar o trabalho da Polícia Judiciária, do Ministério Público e dos órgãos de proteção.

Vou citar um caso que não aconteceu no Brasil, aconteceu nos Estados Unidos, em que determinada pessoa foi a um buscador disponível na Internet e pesquisou por alguns termos que sugeriam um ato terrorista, ou a montagem de

uma bomba, ou os insumos para se construir uma bomba. Em algumas horas, o FBI esteve presente na casa dessa pessoa e viu que não era aquilo que se pensava e que a pessoa havia pesquisado sobre mochila e mais algumas outras coisas. Isso foi amplamente divulgado pela mídia.

Talvez isto poderia ser feito no futuro: haver um controle para o caso de alguma pessoa digitar nesses navegadores os termos que foram definidas por essa universidade, como pedofilia, PTHC e *12-years-old* , que significa crianças com 12 anos, que são termos específicos para quem procura pornografia infantil na Internet. E quando eu falo de pornografia infantil na Internet, eu estou falando que é o registro de imagem de crianças que são estupradas.

No perfil profissional, eles buscam algumas redes de relacionamento que são protegidas por criptografia. Então, para explicar um pouquinho o que é criptografia, eu trouxe um vídeo didático para vocês, que vou pedir para ser exibido agora. Eu peço, por favor, a atenção de vocês para a questão da criptografia.

(Exibição de vídeo.)

O SR. ANDRÉ ABREU MAGALHÃES - Este é um vídeo bem didático, que define o que é criptografia. Então, por óbvio, a criptografia não foi concebida para ocultar atividades ilícitas. Ela dificulta o trabalho das instituições investigativas, porém, não inviabiliza esse trabalho, tanto que recentemente a Polícia Federal deflagrou uma operação totalmente em ambiente criptografado, a Operação Darknet.

Só para mostrar um exemplo de quão grave é a exploração sexual infantil na Internet, na última Conferência Internacional de Perícias em Crimes Cibernéticos, um dos delegados que trabalhou durante a Operação Darknet, citou algo que chamou muita atenção durante essa investigação. Quando falamos em pornografia infantil, sempre pensamos no exterior, mas isso acontece muito no nosso País. Uma pessoa aqui no Brasil fez o seguinte questionamento no fórum: a esposa dele estava grávida e ele queria saber qual era o melhor anestésico que poderia usar na criança que iria nascer, porque ele iria praticar um ato libidinoso e depois iria postar no fórum. Então, vejam o quão grave é isso. Por óbvio, houve uma medida contra esse usuário. Mas é só para registrar quão grave é esse assunto e a importância que ele tem perante o cenário dos crimes cibernéticos.

ONGs do mundo, como a National Center for Missing & Exploited Children — NCMEC, que é famosa nos Estados Unidos, e a SaferNet, aqui no Brasil, divulgam dados de que a pornografia infantil fomenta bilhões de reais ou bilhões de dólares. Ou seja, existem consumidores de pornografia infantil que pagam por ela. E elas são pagas devido ao fato de serem produzidas em ambiente familiar: quanto mais amadora, quanto menos divulgada, mais elevado é o seu valor.

Quando falamos em pagamento, não temos ideia de como ele seria feito. Seria um depósito ou alguma coisa do gênero? Algo que está se alastrando no Brasil, mas que já tem uma conotação muito grande em âmbito mundial, é uma moeda criada chamada *bitcoin*, que é uma moeda virtual.

Eu vou pedir para ser exibido outro vídeo, porque fica mais fácil entenderem o que ela faz e como age.

(Exibição de vídeo.)

O SR. ANDRÉ ABREU MAGALHÃES - Sobre *bitcoins*, nós temos um colega que é perito criminal federal, o Dr. Silvino Schlickmann Júnior, Diretor-Assistente de Pesquisa e Inovação do Complexo Global para Inovação da Interpol, em Singapura, que tem bastantes informações sobre como está sendo a repercussão dessa moeda no mundo, que está entrando no Brasil numa velocidade muito grande. O poder público precisa ter mais informações a respeito disso.

Este é um vídeo que o próprio Bitcoin divulga. E quando eles falam em anonimato, isso causa uma preocupação ainda maior a nós que trabalhamos com segurança pública e às pessoas também que trabalham com o mercado financeiro ou que trabalham na Receita e que precisam tarifar alguns produtos. Ou seja, é algo que está ainda num meio de que não se tem tanta informação disponível e de fácil acesso. Há um portal, o InfoMoney, que diz que o *bitcoin* seria um paraíso fiscal à disposição de todos. Então, só por essa frase, nós já podemos entender um pouquinho o que pode acontecer com isso.

Voltando ao tema, talvez o *bitcoin* seja o método de pagamento pela pornografia infantil. Eu digo "*talvez seja"* porque não posso ter certeza do mundo, por óbvio. Mas eu tenho, sim, certeza de que hoje existe um crime cibernético por meio do qual computadores estão sendo invadidos: os dados pessoais ou dados de empresas estão sendo criptografados; recebe-se uma ligação que pede um

pagamento pela devolução desses dados; e o pagamento é feito pela moeda *bitcoin*. Esse um crime que está acontecendo no Brasil inteiro, sobre o qual temos notícia de diversas ocorrências. Enfim, a ligação vem através de um VoIP lá do Leste Europeu. E o pagamento via *bitcoin*, como foi falado pelo próprio Bitcoin, pode ser um pagamento anônimo.

Talvez esse colega que esteja trabalhando na INTERPOL possa nos fornecer mais informações de como se está lidando com isso. Para terem uma ideia da importância de se saber mais sobre esse *bitcoin* — principalmente os Parlamentares que compõem esta Comissão —, até para casos de sequestro no exterior está sendo pedido o pagamento nessa moeda como resgate.

Voltando ao tema, eu classifico a pornografia infantil como um crime organizado. Por quê? Faturam-se bilhões; existe uma estrutura específica para fins ilícitos; vislumbra-se algum tipo de vantagem; pessoas são forçadas a ter algum tipo de relacionamento através de chantagem; e, principalmente, ela é gerida por criminosos. Então, quem compartilha, quem vende, quem tem qualquer vinculação, a não ser os órgãos de Justiça, com pornografia infantil é um criminoso. Então, caso se preencham esses requisitos, eu estou trabalhando com o crime organizado.

Como combater a exploração sexual infantil na Internet? A Polícia Federal tem feito um trabalho excelente nessa questão, principalmente pela divulgação, que é excelente. Nós deflagramos várias operações, mesmo em ambiente criptografado, e expomos esse problema, que é grave e não é de hoje que acontece. Enfim, é preciso ter uma política como a da Polícia Federal, com uma estrutura investigativa qualificada, uma estrutura com equipamentos específicos.

Principalmente na nossa área — eu sou perito criminal —, nós trabalhamos com o legado das operações. Ou seja, após a deflagração das operações é que começa grande parte do trabalho da perícia criminal. É nesse trabalho que acontecem diversos desdobramentos e conseguimos ter um contato bem direto com os diálogos que essas pessoas utilizam para aliciar menores, com o ambiente técnico-científico das aplicações utilizadas. Então, nós temos feito um bom trabalho.

Eu vou pedir para exibir um vídeo do que seria um ambiente para se trabalhar no legado não só de crimes de pornografia infantil, mas de outros crimes cibernéticos.

(Exibição de vídeo.)

O SR. ANDRÉ ABREU MAGALHÃES - Talvez esta seja a estrutura que a lei conhecida como Lei Azeredo dispõe no seu art. 4º, qual seja:

> *"Art. 4º Os órgãos da 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."*

Portanto, nós estamos preparados para eles.

Mas a pornografia infantil e a exploração sexual infantil na Internet não ocorrem só no Brasil, são crimes que atravessam fronteiras e que não dependem apenas de nós. Então, esse crime depende muito de organizações não governamentais, com as suas políticas, como a SaferNet faz através do seu portal *www.denunciar.org.br,* ou o Disque 100. Enfim, tudo que for para divulgar o comportamento ou a utilização de forma correta da Internet é válido para que os crimes cibernéticos não ocorram e para que a exploração sexual infantil na Internet pelo menos saia do *ranking* como um dos maiores crimes.

Aqui houve outras audiências públicas, especificamente uma em que estiveram presentes algumas procuradoras da República, que falaram sobre os termos de cooperação internacional. Eu vou citar o exemplo de um caso em que trabalhei de utilização desses termos de cooperação internacional, especificamente chamados de MLATs — Mutual Legal Assistance Treaties, que são acordos com o os Estados Unidos para fornecimento de informações e outras coisas relacionadas a crimes.

O caso era o seguinte: uma jovem, num ponto de ônibus na cidade de Porto Velho, Estado de Rondônia, foi alvejada com um tiro no rosto disparado pelo seu ex-namorado, por motivos passionais, e foi morta. E quando o pai dela chegou, ela ainda estava agonizando no ponto de ônibus. Foi um caso muito sério, um homicídio por motivo fútil. O juiz do caso recebeu do advogado um pedido de liberdade do réu por meio de *habeas corpus,* citando que a vítima havia feito ofensas ao réu através do Facebook e que, por motivo, ele foi levado a praticar o homicídio. O juiz, de pronto, fez ao Facebook um pedido para que fornecesse essas informações e pediu

apoio à Superintendência da Polícia Federal para utilização do acordo — o tribunal do júri, por exemplo, não tem tanta afinidade com isso. O Superintendente designou-me para trabalhar no caso. Eu estou falando do caso porque ele já foi julgado e está amplamente divulgado na mídia.

O que o juiz pediu? Estamos falando do juiz, uma autoridade do Poder Judiciário:

> *"DOS BACKUPS DO FACEBOOK. Defiro a diligência requerida, devendo ser oficiado o Facebook Brasil, para que encaminhe, a este juízo, em trinta dias, por meio de mídia digital, todo o conteúdo dos perfis da vítima (www.facebook.com/raissa.lopes.188) e do acusado (...), tais como álbuns, mensagens privadas, IP's de login, senhas, troca de senhas, atividade de registro e cadastro, postagens, comentários, a partir de 21 de maio de 2012 até 11 de setembro de 2012, inclusive se foi removida alguma mensagem dentro desse período ou posteriormente a esse período até 11 de novembro de 2012."*

Detalhe: é preciso ser redigida uma petição em português e uma petição em inglês. Essa é uma grande dificuldade que se tem, porque nem todo mundo fala inglês e não é exigido inglês nos concursos públicos, nem para o cargo de magistrado. A resposta já é em português.

Eu auxiliei tanto na redação das petições quanto no que pedi. A resposta vem através do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério da Justiça:

> *"Sr. Juiz, referimo-nos ao formulário MLAT, de 28 de fevereiro de 2013, recebido neste departamento em 5 de março de 2013, por intermédio do qual V.Exa. encaminhou solicitação de assistência jurídica em matéria penal extraída dos autos do Processo nº 001405769/2012-8220501, em trâmite perante este juízo, dirigida aos Estados Unidos da América.*

A esse respeito informamos que as autoridades estadunidenses não cumpriram a diligência cumprida, pois alegam que as evidências fornecidas não são suficientes fortes para que se conceda a quebra de sigilo telemático.

Isso posto, colocamo-nos à disposição para quaisquer esclarecimentos que se fizerem necessários."

Trata-se de crime de homicídio, o que dirá de outro tipo de crime.

Dando continuidade, eu formulei aqui — se os senhores me permitirem —, algumas sugestões que podemos fazer. Se me permitem a palavra, eu gostaria de fazer algumas sugestões. Nós precisamos de Termos de Cooperação Internacional mais céleres e que respeitem a legislação brasileira, principalmente. É preciso respeitar a legislação brasileira.

A plataforma *Law Enforcement*, que é o que o Facebook expôs aqui, é muito boa. Mas eles devem nos responder aquilo que o Brasil precisa. O que os Estados Unidos precisam é o que os Estados Unidos precisam, o que o Brasil precisa é o que o Brasil precisa. Então, se eu preciso de uma informação, eu tenho uma lei no Brasil que disciplina e uma representação dessa empresa aqui no País, e há uma lei que obriga.

Até se sugeriu um Termo de Ajuste de Conduta. Mas um Termo de Ajuste de Conduta para uma coisa que já existe? Nós já temos legislação suficiente para garantir isso. E, no crime de homicídio, no meu ponto de vista, é inadmissível!

Sugiro aos senhores, se possível, que se possa formar uma comitiva e que se faça uma diligência ao Facebook, seja no Brasil, seja nos Estados Unidos. Acredito que isso teria uma repercussão muito positiva, principalmente para eles nos fornecerem essas informações e também para que possam fornecer de forma melhor para as nossas autoridades informações de um aplicativo que eu acredito que todo mundo que está com o *smartphone* na mesa aqui tem e que se chama WhatsApp. E eu não vou entrar no mérito do WhatsApp.

A outra sugestão seria melhorar o apoio do setor responsável pela cooperação jurídica internacional em matéria penal no Ministério da Justiça, que funciona como intermediário da...

O SR. DEPUTADO FÁBIO SOUSA - Sra. Presidente, peço licença.

Dr. André, o senhor falou que não entraria no mérito do WhatsApp, mas se o senhor puder trazer algumas informações a respeito disso, seria muito interessante, porque a CPI está querendo tratar exatamente dessas áreas, inclusive as que se relacionam ao WhatsApp. Desculpe-me por dizer isso, mas...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Aproveito para dizer que há um requerimento do Deputado Alexandre Leite relacionado a este assunto. Ainda não o colocamos em votação, mas também é para discutir sobre esse assunto do WhatsApp.

O SR. ANDRÉ ABREU MAGALHÃES - Eu posso responder depois, em forma de perguntas especificamente? Está o.k.

Esse setor de cooperação de ativos em matéria penal no Ministério da Justiça poderia auxiliar na tradução, nessas petições em outros idiomas. Quando é inglês, é fácil encontrar, mas quando é outro idioma, fica um pouco difícil.

Eles fazem muita coisa, eles fazem algumas traduções, mas a petição inicial que temos que entregar tem que ser nos dois idiomas, tanto em português quanto no outro idioma. Então, se pudesse haver uma melhoria com relação a isso... O tratamento que eu tive quando telefonei foi excepcional. Porém, essa exigência de as próprias autoridades terem que fazer essa tradução... Às vezes é necessário traduzir uma decisão judicial. Uma vez me pediram para traduzir, e eu não traduzi, porque, para traduzir uma decisão judicial que defere um pedido de quebra de sigilo telemático, por exemplo, por mais que eu seja perito criminal e tenha afinidade com a língua, com o idioma, é preciso um perito nomeado pelo juiz, para fazer essa tradução. Se eu usar um termo diferente, ele pode ser interpretado de maneira diferente no outro país. Então, é uma dificuldade que se tem.

Conforme combinei com a Deputada Presidente, eu vou passar agora às sugestões. Talvez nós precisássemos da criação de uma agência reguladora de *software*. Assim como temos a ANATEL, precisaríamos de uma agência reguladora de *software*. Em que casos ela seria provocada? No jargão popular das pessoas que trabalham com computação, seria naqueles casos de aplicativos que “viralizam”. O WhatsApp, por exemplo, é um aplicativo que “viraliza”. O Uber, por exemplo, é um aplicativo que “viraliza”. Então, a partir do momento que eu tenho esses aplicativos,

eles vão ter uma consequência forense. E precisaríamos de uma agência reguladora para que ela dissesse*: "Esse aplicativo pode fazer isso, ele não pode fazer isso; isto aqui vai causar LID, isto aqui vai gerar problema".*

Dois aplicativos polêmicos são o Secret e o Uber. Cito o Secret porque ele dá a possibilidade de realizar postagens, em uma rede social, de forma anônima. Eu poderia escrever o que quisesse e estaria anônimo. Eu poderia ofender uma minoria, eu poderia ofender uma raça, eu poderia praticar crimes de forma anônima. Então, na Internet não pode haver o anonimato, isso é inadmissível nos tempos de hoje.

Talvez não seja necessária uma agência, poderia ser um grupo específico, dentro de uma agência reguladora, para a parte de *software*. Seria muito importante para o País. Eu acredito que não exista. Pode ser que exista, mas, se existe, eu nunca ouvi falar.

Bom, outra recomendação seria a seguinte: que fossem feitos ofícios, pelos senhores, através desta CPI, para os Estados, para que eles deem informações sobre o cumprimento do art. 4º, que eu li aqui, da Lei Azeredo, que diz:

> *"Art. 4º Os órgãos da 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."*

Isso para ver se eles se adequaram à legislação existente. Se eles não se adequaram, eu acredito que uma via seria, por exemplo, a apresentação de projetos à SENASP, que sempre está de portas abertas. Eu já apresentei, quando trabalhava no Estado, projetos à SENASP. Foram deferidos e o dinheiro, disponibilizado. Enfim, eu pude contribuir através desses projetos, e acredito que a SENASP está de portas abertas para qualquer projeto com essa finalidade.

As sugestões seriam essas. Enfim, quanto ao tema sobre o qual eu fui chamado para falar, é o que eu tinha a dizer.

Agradeço a atenção de todos e estou aberto a perguntas, se necessário.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada. E eu já gostaria de solicitar ao senhor, que, se puder, mande essas sugestões também para

o *e-mail* da CPI, e até depois, devido ao andamento desta Comissão, se vier a ter outras sugestões. Se puder contribuir, agradeceremos.

O SR. ANDRÉ ABREU MAGALHÃES - Permita-me usar da palavra novamente, pois me esqueci de duas sugestões. Como os senhores estão pedindo cópias de inquéritos, ou alguma coisa nesse sentido, e como eu falei em criptografia e em *bitcoins,* e em algumas outras coisas, duas operações de grande destaque, com repercussão nacional, em ambiente que envolve criptografia, que envolve alta tecnologia — se for possível o acesso, se a legislação permitir, se não estiver protegido por sigilo ou alguma coisa do gênero —, seriam Darknet e Infância Segura II. Com certeza, o conhecimento dessas operações por parte dos senhores melhoraria muito seu senso crítico com relação aos crimes cibernéticos.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Concedo a palavra ao Sr. Leonardo Bueno de Melo, representante do Instituto Nacional de Criminalística.

O SR. LEONARDO BUENO DE MELO - Boa tarde a todos. Primeiro, eu gostaria de agradecer o convite, a oportunidade de estar aqui para ajudar nos trabalhos da CPI, e cumprimentar a Mesa, na pessoa da Deputada Mariana Carvalho, e os demais presentes.

Bom, eu vou me apresentar. Eu sou o Chefe do Serviço de Perícias em Informática do Instituto Nacional de Criminalística. Estou lotado lá há 13 anos e, nos últimos 8 anos, envolvido com a Chefia, seja como chefe substituto, seja como titular. E nesse período eu pude acompanhar a evolução dos crimes cibernéticos e também das ações de combate.

Eu vou aproveitar esta oportunidade para apresentar a estrutura da perícia criminal da Polícia Federal na parte de informática, comentar sobre as dificuldades, algumas soluções que vemos para sanar, contornar essas dificuldades e expor alguns tópicos e algumas questões que os colegas, os peritos da Polícia consideram relevantes para serem discutidos.

A área de informática da perícia criminal já existe na Polícia Federal há 20 anos, quando foi nomeado o primeiro perito da área. Hoje nós temos 227 peritos da área de informática. Isso equivale mais ou menos a 20% do total de peritos da Polícia Federal, da ativa, e esses peritos estão distribuídos por 43 unidades da Polícia Federal, em todo o País. Nós temos um setor técnico-científico em cada

capital, em cada Superintendência, e unidades técnico-científicas e núcleos técnico-científicos em algumas Delegacias do interior também.

A presença da perícia em informática hoje é bastante forte na área de perícia como um todo. E em Brasília nós temos, dentro do Instituto Nacional de Criminalística, como eu comentei, o SEPINF — Serviço de Perícias em Informática, que é responsável por orientar, normatizar, acompanhar e também realizar os exames de perícia em informática, prestando apoio às unidades regionais, aprimorando técnicas e tecnologias, promovendo a capacitação dos peritos criminais federais e, de certa forma, tentando conduzir a evolução das atividades nesse campo.

Os peritos criminais federais, quando desenvolvem suas atividades dentro da Polícia Federal, têm dupla função. A primeira é aquela que todo mundo conhece, a de realizar exames periciais. Nós fazemos os exames e emitimos os laudos. A maior parte do nosso trabalho são exames em mídia de armazenamento computacional, que são os HDs, os *pen drives*, os DVDs. Muito forte também tem sido a carga de exames em celulares, em *smartphones*, mas também fazemos exames na Internet, em *e-mails*, *sites*. Fazemos interceptação telemática, interceptação de dados, exames em sistemas contábeis, em banco de dados e também, como o Dr. André falou, em dados criptografados.

Além dessa função, os peritos criminais da área de informática têm uma forte atuação também, dentro da Polícia Federal, como policiais especializados. Do corpo de policiais do DPF, nós somos a única categoria com a exigência de conhecimentos específicos de informática para ingresso no cargo. Com isso, muitas atividades que exigem uma capacitação técnica mais específica, mais avançada, ainda que não seja de natureza pericial, são desempenhadas pelos peritos.

Então, muitas vezes os peritos são chamados para prestar consultoria nas investigações policiais, prestam orientações técnicas nas fases de planejamento, de preparação dessas operações, e também atuam nas operações de busca e apreensão, identificando, selecionando material e os dados a serem apreendidos, assegurando, dessa forma, a cadeia de custódia dentro da Polícia.

Bom, considerando que o combate aos crimes cibernéticos não depende somente da capacidade de identificar e chegar até os criminosos, mas também da

capacidade de se conseguir a condenação criminal desses delinquentes, a importância da perícia assume dois aspectos.

Como eu falei, por meio dos conhecimentos técnicos que o perito detém e que não são exigidos ao juiz, ele consegue identificar, processar e interpretar os vestígios de interesse numa investigação de crimes cibernéticos. E toda investigação desse tipo acaba esbarrando em dificuldades para, por exemplo, localizar dados de interesse num volume muito grande de dados. Vemos que já há HDs aí de 6 *terabytes*. Em um HD apreendido, o número de arquivos e artefatos de dados passa facilmente de 1 milhão. E conseguir identificar o que interessa ali dentro não é uma tarefa trivial, exige correlacionamento de dados, categorização de dados, ranqueamento do que interessa, a partir de premissas, de informações que possam delimitar o escopo dessa busca.

As investigações de crimes cibernéticos, mais recentemente, com frequência, também têm esbarrado em dificuldades para acessar dados que são armazenados remotamente. Temos diversos serviços de Internet, como Google Drive, Dropbox, uma série de serviços em que os dados não ficam no dispositivo, e, sim, na nuvem. Os peritos muitas vezes são chamados para recuperar arquivos apagados, decifrar arquivos encriptados, quebrar senha de sistemas, como sistemas contábeis, sistemas corporativos, que são apreendidos numa busca e apreensão, remontar ambientes virtuais, analisar comportamento de vírus, de programas maliciosos, ou seja, analisar o código-fonte, o tipo de tráfego que ele gera, analisar fluxo de dados e lidar com mascaramento de conexões, *logs*. Há uma gama muito ampla de atuação.

O outro aspecto da importância da perícia no contexto dos crimes cibernéticos — acredito que o Dr. Bruno Telles também deve comentar a respeito — é garantir os princípios da segurança jurídica, da efetividade do processo e da verdade real. Ou seja, a perícia é fonte de prova material, é ela que fornece elementos idôneos e objetivos de prova que subsidiam o convencimento do juiz, estando livre da subjetividade dos outros tipos de prova, como as testemunhais, por exemplo. No âmbito dos crimes cibernéticos, isso ganha uma importância especial por causa da volatilidade inerente aos vestígios. Sabemos muito bem que um *site* que está no ar agora daqui a meia hora pode ter sido tirado do ar. Então, é importantíssima a

atuação da perícia para garantir a preservação desses elementos de prova, e as circunstâncias em que eles são coletados também são bastante transitórias.

Com isso, pode-se garantir uma cadeia de custódia para que essas provas coletadas, as evidências que tenham sido produzidas, as provas que tenham sido produzidas, sejam submetidas ao escrutínio posterior, tanto da acusação quanto da defesa. Dessa forma, conseguimos assegurar a aplicabilidade do princípio constitucional do contraditório e da ampla defesa. O próprio CPP reconhece a importância da perícia, exige o exame de corpo de delito nos casos em que houver vestígios, sob pena de nulidade do processo.

Voltando à situação da perícia na Polícia Federal, agora já com foco nas nossas dificuldades, para os senhores terem uma ideia, só este ano já foram emitidos 6.823 laudos de perícia de informática. Isso equivale a 20% de todos os laudos produzidos pela perícia da Polícia Federal este ano. Por ano, estima-se, de forma conservadora, que sejam processados cerca de 3 *petabytes* de dados. São aproximadamente 3 mil laudos de computadores e HDs, discos rígidos, e mais 6 mil laudos de celulares e outros tipos de mídias. Para efeito de comparação, na época em que estourou o escândalo do Snowden, a NSA, agência de inteligência americana, que foi acusada de espionagem governamental, declarou que eles processavam 10 *petabytes* por ano, ou seja, só um pouco mais de 3 vezes o que processamos hoje.

Então, é uma carga realmente altíssima de dados para serem processados e, a partir daí, se tentarem extrair as informações que possam interessar à investigação e à persecução penal, ao processo judicial. Isso logicamente gera uma sobrecarga na perícia, e eu falo isso não só me referindo à Polícia Federal. Vejo que nas polícias estaduais, nas perícias estaduais isso também é um problema sério. Com isso, nós temos hoje na Polícia Federal mais de 4 mil discos rígidos e SSDs aguardando perícia. Quase 3 mil celulares, 2.786, também estão esperando para ser periciados, e outros tantos materiais, como *tablets*, *pen drives* e DVDs.

O que assusta, particularmente, quanto a essas quantidades, é que há 1 ano verificou-se um aumento, no caso dos discos rígidos, de 38,5% e, no caso dos celulares, de 45%, em relação ao que estava pendente há 1 ano. Se não surgir nenhum novo pedido de perícia e todos os peritos de informática se dedicarem

exclusivamente a analisar esse material — o que não acontece, porque o perito de informática também está sujeito, como policial, a ser acionado durante um plantão ou, de sobreaviso, a fazer perícia preliminar de drogas, principalmente nos Estados —, seriam necessários quase 2 anos para que pudéssemos atender a todas essas pendências. Isso provoca claros prejuízos às investigações policiais, ao andamento dos processos judiciais. E o CPP prevê um prazo de 10 dias para a realização de uma perícia.

Entre as soluções que nós vislumbramos para contornar esse problema, para mitigar essas dificuldades, a primeira é o aumento de efetivo. Hoje, somente 10% dos policiais federais são peritos criminais — falo de todas as áreas, não estou falando só da área de informática —, por uma limitação de vagas disponíveis. Ou seja, é preciso que sejam criadas novas vagas para que possamos contratar mais peritos. Por essa razão, no próximo concurso, que está previsto, esperamos receber somente 67 novos peritos. E, quando isso acontecer, vai aumentar ainda mais a discrepância em relação ao efetivo dos nossos maiores demandantes, que são os delegados, porque, no caso deles, já existem as vagas criadas para preenchimento de 491 cargos. Então, essa relação entre perito e delegado vai aumentar 20%, ou seja, a tendência é que piore ainda mais a nossa capacidade de atendimento.

Outra solução é estudada na Polícia Federal. Existe uma linha muito tênue e uma diferenciação, que não é muito precisa, entre o que é perícia de informática e o que é investigação propriamente dita dos crimes cibernéticos, ou seja, entre o trabalho que é feito pelo perito e o trabalho que é feito pelo investigador, pelo agente, pelo delegado. Como eu comentei, pela capacidade técnica, pelo conhecimento que têm, os peritos acabam fazendo investigação. Uma das saídas que buscamos é diminuir, fazer com que alguns dos procedimentos possam ser feitos pelos agentes, pelos delegados, mas isso depende, como já foi falado aqui, em audiências anteriores, que eu pude acompanhar, de uma ação de capacitação realmente efetiva para os policiais.

Também consideramos de alta relevância o incentivo ao desenvolvimento e à pesquisa de ferramentas e soluções, para que possamos, com isso, otimizar os nossos métodos, rever os nossos procedimentos e tentar tornar mais eficiente e efetivo o nosso trabalho. A SENASP, em parceria com a Polícia Federal, está

construindo o Centro Nacional de Capacitação e Difusão de Ciências Forenses, onde hoje é o Instituto Nacional de Criminalística, e, com isso, esperamos uma atuação forte nessa parte de capacitação, de difusão de conhecimento.

Em junho — é um bom exemplo também —, foi realizada a Conferência Internacional de Perícias em Crimes Cibernéticos, conhecida como ICCyber, em conjunto com o ICMedia, que é a maior conferência da América Latina nesse campo. É uma ótima oportunidade para atualização de conhecimentos e estabelecimento de redes de contatos.

Entre as soluções que são desenvolvidas, apesar das dificuldades, nós temos o NuDetective, que é uma ferramenta desenvolvida pelos peritos criminais federais do Mato Grosso Sul que permite a detecção automatizada de pornografia, tanto em vídeos quanto em imagens. Nós temos ferramentas que são desenvolvidas para agilizar a atuação na busca e apreensão e projetos para tentar melhorar essa análise das mídias de armazenamento, como o SAD.

Para finalizar, eu gostaria simplesmente de citar alguns pontos que considero importantes a serem destacados em relação a esse contexto do combate aos crimes cibernéticos. Até hoje, ainda existe a crença, a impressão de que possa existir um crime virtual. Isso não é verdade. Os crimes são cometidos nos ambientes virtuais, mas as ações são concretas, eles deixam vestígios e por meio da perícia podem ter a materialidade, a autoria e o *modus operandi* determinados.

Outro aspecto importantíssimo é a questão da cadeia de custódia. As evidências digitais pela sua natureza não dependem do anteparo. Ou seja, não adianta eu tentar descrever um arquivo a partir do HD em que ele está dentro ou do *pen drive*, porque, se esse HD for copiado para outra mídia, vai ser exatamente o mesmo arquivo, ou ele pode ser substituído por um novo arquivo, e o anteparo não vai ter absolutamente nenhum impacto nisso. Então, a cadeia de custódia nesse contexto ganha uma importância, uma relevância realmente muito grande, para que possamos armazenar e garantir a integridade dos dados, seja durante a fase de investigação, seja depois, durante o processo judicial.

É importante também se estabelecerem regras e procedimentos a serem seguidos pelos grupos de resposta incidentes das empresas, das organizações, dos órgãos públicos, para permitir a elucidação dos crimes cibernéticos. Normalmente,

quando uma empresa, um órgão sofre um ataque, a primeira preocupação da equipe de TI é restabelecer o serviço o mais rápido possível. Eles não se importam muito em preservar as evidências. Eles não se importam se, para isso, vão ter que apagar alguns arquivos, comprometer a integridade de *logs*, o que gera prejuízos realmente graves depois, no momento em que se for tentar identificar a origem desse ataque, a autoria desse ataque.

Como propostas, a perícia tem, especificamente em relação a essa questão de custódia, as interceptações telemáticas. O colega Dr. Alessander pode explicar um pouco sobre um projeto para um carimbo de tempo com uma autenticação criptográfica das interceptações que são feitas durante a investigação policial, ou seja, para que se possa, sem margem a dúvidas a questionamentos, assegurar que o áudio que foi interceptado, os pacotes de dados que foram interceptados correspondem exatamente àquilo que foi trafegado nas linhas de comunicação do alvo.

Um tópico também de possível interesse é a difusão muito grande da interconectividade de objetos à Internet, ou seja, um momento chamado de Internet das coisas. Nós vemos geladeira ligada à Internet, carro se conectando à Internet. E isso abre uma brecha para uma série de falhas de segurança, de vazamentos de privacidade que precisam ser discutidos. Isso está diretamente ligado à adoção do IP versão 6, que foi discutido aqui na audiência passada. O Dr. Evandro Lorens deve comentar um pouco sobre esses aspectos.

Há também exames em grande volume de dados, a análise dos *smartphones,* que é para onde estão migrando os dados de interesse hoje nas investigações.

Eu encerro aqui. Basicamente era isso que eu gostaria de expor.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigado, Dr. Leonardo Bueno.

Com a palavra o Sr. Evandro Mário Lorens, representante do Instituto Nacional de Criminalística.

O SR. EVANDRO MÁRIO LORENS - Boa tarde a todos. Eu agradeço o convite. É uma honra para nós estarmos nesta Casa, trazendo um pouco da nossa experiência. Meu nome é Evandro Mário Lorens, sou perito criminal da Polícia Federal, mestre em Ciência da Informação pela Universidade de Brasília, graduado

em Ciência da Computação e especialista em telecomunicações pela Universidade Federal do Espírito Santo. Estou na Polícia Federal há 6 anos. Antes da Polícia Federal, trabalhei como servidor em quatro bancos, sendo incluídos aí o Banco Central e a Caixa Econômica Federal. Quando fui para a Polícia Federal, levei toda essa experiência bancária. Desses 6 anos que estou na Polícia Federal, há 2 anos estou trabalhando com o Dr. Leonardo, no Instituto Nacional de Criminalística. Recentemente, trabalhei como coordenador desse evento da ICCyber ICMidia, uma conferência integrada, quando trouxemos para o Brasil as discussões mais atuais relacionadas com os crimes cibernéticos: as perícias em crimes cibernéticos. Trouxemos convidados internacionais. Este ano, nós tivemos 14 palestrantes internacionais. Foi um evento muito rico. Inclusive, o Deputado Alessandro Molon foi um dos palestrantes desse nosso evento que aconteceu em junho.

O aspecto que vou abordar é um pouco mais genérico, um pouco mais focado em propostas, discussões sobre o que podemos oferecer, em termos de um apoio mais especializado, para a CPI.

De forma genérica, eu gostaria de lembrar que a perícia na área de informática, assim como toda perícia criminal federal, é voltada à realização da justiça pela ciência. O que é isso? Análise dos vestígios e, por meio desses vestígios, conseguir determinar a autoria ou a não autoria de determinados delitos. Da mesma forma acontece isso no mundo cibernético. Nós vemos que a Internet é um mundo dinâmico. Todos os dias nós temos novidades, boas e ruins. A perícia informática é uma disciplina totalmente dinâmica. Todos os dias temos que nos atualizarmos, voltando-nos para aquilo que é novo e tentando correr se não à frente, mas ao lado daqueles que estão usando a Internet, as redes e a informática para praticar delitos.

No caso, o Dr. Leonardo já abordou aqui o que é feito depois: a parte de análise dos vestígios. Mas há um aspecto importante, também, da perícia, que é o apoio que oferecemos às instituições governamentais no sentido da prevenção a eventuais problemas nos ambientes cibernéticos. Sempre que acionados por demanda, participamos de grupos temáticos relacionados com isso, oferecemos a experiência. Na questão da prevenção, dizemos: *"Olha, isso é temerário, é importante, isso é seguro, isso é seguro, isso não é*". É um trabalho de consultoria

mesmo, porque isso reflete lá na frente no nosso trabalho. Uma vez que o ambiente está mais seguro, mais protegido, em qualquer instituição governamental, o trabalho da Polícia Federal vai ser, vamos dizer assim, amortecido, pelo aspecto da prevenção que oferecemos como consultoria.

Outro aspecto importante — e aí já se trata da ocorrência de um crime cibernético — é a preservação. Nós trabalhamos orientando tanto os normativos do Gabinete de Segurança Institucional, quanto em qualquer ambiente de discussão relacionado com o tratamento de crimes cibernéticos, oferecemos nosso conhecimento no sentido de informar o que deve ser preservado. O Dr. Leonardo já abordou aqui uma questão, que é muito comum, quando um *site* de um órgão governamental ou de qualquer empresa é invadido, em geral, a primeira medida adotada é reinstalar o sistema em cima daquele que foi comprometido e voltar a funcionar o *site,* porque a imprensa está cobrando pelo *site* fora do ar.

O correto seria separar esse material, não tocar, desconectar da rede e deixar para que fosse analisado o que realmente aconteceu ali. Podendo analisar, a perícia consegue dizer: *"Olha, a entrada foi por aqui, o modo de operação foi esse e a origem foi essa"*, ou seja, todos os aspectos relacionados com o delito. Nós oferecemos também a preservação, o conhecimento que nós temos, de modo a facilitar o trabalho de rastreamento e de combate ao crime cibernético, que é a principal proposta de discussão desta CPI.

Eu coloquei um pouco mais cedo a questão da dinamicidade dos crimes cibernéticos, e aí já entrando nesse aspecto, que é uma discussão que eu gostaria de oferecer à CPI, sobre a Internet das coisas, como exemplo, caso real ocorrido recentemente nos Estados Unidos, de uma quadrilha especializada em tráfico de bebês. Essa quadrilha selecionava os bebês, que ela ia sequestrar para vender, por meio de babás eletrônicas conectadas em rede. Eles invadiam o equipamento dessas babás eletrônicas, que funcionam por meio de rede sem fio, aquelas babás que filmam o bebê durante a noite e que passam as imagens para os pais num monitor no quarto. De posse das imagens, eles mostravam as imagens e a pessoa escolhia o bebê, que era sequestrado e o vendiam. Isso não é ficção científica, isso é caso real. Aí nós entramos nesse aspecto da Internet das coisas, aspecto esse

que estamos à disposição da CPI para discutir nos termos que a CPI tiver interesse. Por quê? É a realidade. Se já fizermos uma lista, aqui no Brasil, do que já está conectado à Internet, nós vamos ter vários dispositivos. Nós já temos a tevê, o DVD, o *blu-ray*, os nossos telefones, os computadores, notebooks e, em breve, já existe — eu estou falando porque lá em casa não tem — a geladeira que vai me dizer o quê que eu tenho que comprar esta semana, já vai mandar a lista para o supermercado, tudo via rede, do que está faltando.

Esse aspecto de estar conectado em rede tem muitas variáveis e relaciona aí uma série de problemas que podem ocorrer relacionados com crimes cibernéticos, especialmente questões relacionadas com a privacidade. Esse exemplo que eu usei dos bebês é claro, ou seja, a babá eletrônica, que tem o objetivo único, simples, de apoiar o trabalho dos pais no cuidado com seus filhos, é usado como instrumento para execução de crimes, ou seja, um crime apoiado na cibernética para ser cometido. Então, a Internet das coisas, como o Dr. Leonardo colocou, está intimamente relacionada com a questão do IPv6, que é uma nova forma de endereçamento — nova é maneira de dizer —, mas é uma forma de endereçamento mais recente para os dispositivos, que permitem uma explosão gigantesca da capacidade de endereçamento que nós temos de dispositivos, hoje. Hoje nós temos o IPv4, a versão 4, que limita a quantidade de dispositivos, e hoje não temos mais endereços disponíveis. Então, o que é feito é o revezamento de endereços.

Acho que isso já foi falado para os senhores aqui recentemente, então não vou ficar falando mais sobre isso, mas a questão da Internet das coisas está intimamente ligada a isso, porque, à medida que algumas pessoas colocam IPv6 como solução — e ela realmente traz várias vantagens —, ela também traz consigo outros aspectos que demandam uma reflexão e também a ação nossa e de toda a sociedade com relação à forma de se comportar com essas novas tecnologias que estão chegando.

O SR. DEPUTADO JEAN WYLLYS - O senhor acha que não é a solução?

O SR. EVANDRO MÁRIO LORENS - Não entendi.

O SR. DEPUTADO JEAN WYLLYS - O senhor acha que não é a solução?

O SR. EVANDRO MÁRIO LORENS - Não é a solução. É uma solução importante, mas não é a solução. Eu poderia aqui falar somente de vantagens e

desvantagens durante uma hora e discutirmos o peso dessas vantagens e desvantagens, de forma até a refletir por que isso ainda não está, hoje, no nosso cotidiano, se é tão bom assim. Então, são questões práticas, filosóficas, de todos os lados, enfim, é uma discussão. Definitivamente, na minha opinião, lógico, não é a solução. É uma solução importante, mas não é a solução.

Então, como já foi falado para os senhores, traz muitas vantagens, mas traz consigo também o *overhead*, como dizemos, a carga de outras questões que nós teríamos que tratar, mas não é o momento agora. Nós nos colocamos à disposição dos senhores para tratar disso no nível que quiserem, pessoalmente, numa reunião, em outra apresentação, enfim, estamos à disposição. Quando falo nós, eu me refiro à perícia criminal federal.

Outro aspecto importante, que talvez seja o aspecto, hoje, mais crítico para a efetividade do trabalho da perícia criminal federal, é o exame de grandes volumes de dados. Todos nós aqui, que há 10 anos já tínhamos um PC em casa, não precisamos fazer muito esforço para lembrar qual era a quantidade de arquivos que tínhamos para copiar as músicas. Hoje em dia, eu faço um desafio para alguém me dizer quantos arquivos há dentro do HD do seu computador.

A explosão da quantidade de dados foi facilitada pela divulgação, a própria Internet, e pelo barateamento das mídias de armazenamento, ou seja, o armazenamento de um *byte,* hoje, é infinitamente mais barato do que era há 10, 20 anos.

Essa combinação de fatores, a explosão da sociedade da informação, a criação de dispositivos, a Internet e o barateamento dessas tecnologias, levou a uma explosão de dados. Enfim, antigamente, fazíamos conta do que se podia colocar no *pen drive*, do que não dava para colocar. Hoje em dia, vou à esquina, compro um *pen drive* por 50 reais, que cabe 3 vezes aquele último *pen drive* que eu tinha, e continua a vida, não quero nem saber quantos arquivos têm lá.

Esse grande volume de dados traz, olhando para o lado da perícia e até para o lado do controle e da Justiça, daquilo que nos propomos a fazer como justiça pela ciência, uma grande dor de cabeça. Esse volume exponencial crescente de dados faz com que o nosso trabalho seja ainda mais complexo, porque se antes eu analisava “x”, agora analiso cem “x” e tenho que entregar esses resultados com a

mesma celeridade, para que o processo não seja comprometido. Então, eu tenho que trabalhar em várias frentes ao mesmo tempo para que eu consiga dar conta dessa demanda.

Hoje, nós trabalhamos fortemente com a produção e a aquisição de equipamentos, com a criação de ferramentas internas para acelerar esses processos, e estamos trabalhando numa questão que é mais delicada, mas que exige muita reflexão, muito estudo, muito investimento, que é a análise integrada, ou seja, a propiciação de um ambiente de análise integrada pelos vários atores da polícia e até da persecução penal, para ter condições de dividir um pouco esse trabalho, ou seja, aquele trabalho que não necessita tanto da ação do perito e que possa ser feito por outro ator. Então, é isso que chamamos de análise integrada, ou seja, abrir certos ambientes, dar acesso a certos ambientes que hoje são exclusivos da perícia a outros atores do contexto policial, do contexto da investigação, da Justiça, para que esse processo possa ser também dividido.

Hoje em dia a economia é compartilhada, é uma realidade para nós. Nesse aspecto, temos trabalhado fortemente. No entanto, esbarramos em vários aspectos. Por isso, eu estou trazendo aqui para que a CPI, se houver interesse, possa discutir também como viabilizar isso através, talvez, de novos ajustes no Código de Processo Penal, através de novas legislações que podem ser discutidas conosco. Estamos à disposição também para esse tipo de coisa.

Por último, só para encerrar, eu tenho 21 segundos, mas vou tentar ser breve, é uma questão bastante importante para nós, que é a análise de *smartphones.* Já foi dito aqui, hoje, sobre a preocupação com os aplicativos, como WhatsApp, com a nossa exposição na medida em que tiramos *selfs* e mandamos pela rede, colocamos no Instagram, replica para o Facebook e assim por diante. Então, as análises de *smartphones* têm se tornado também um campeão. Acreditamos que, em um determinado momento, nós vamos ter a equivalência da quantidade de mídias tradicionais com a quantidade de *smartphones* para ser analisados. Isso é só uma crença. Nós não temos números concretos para dizer isso, mas, face o crescimento das plataformas de *smartphones* — e, quando falo *smartphones*, estou dizendo todos os tipos de dispositivos móveis que nós temos hoje —, o crescimento do acesso a esse tipo de tecnologia também, cresce para nós a análise, e também, do

mesmo modo, a quantidade de arquivos que estão armazenados, a quantidade de coisas que têm que ser analisadas dentro desses equipamentos.

As informações sensíveis dos usuários estão lá: nossa vida, nossos contatos, nossos diálogos, os diálogos íntimos que, às vezes, trocamos com pessoas do nosso círculo de interação. Então, esse tipo de questão coloca também o problema da privacidade, que já falamos aqui, em xeque, com relação ao crime cibernético, e também outras questões relacionadas com as transações bancárias que são feitas e outras coisas do gênero.

Para encerrar, outra questão também importante, do ponto de vista da perícia, é que, face a essa questão da privacidade, face a essa questão da necessidade de dar segurança aos usuários, os fabricantes têm investido fortemente em mecanismos de proteção. Com isso, são criadas formas de acesso, como uso de senhas mais fortes, criptografia, biometria, recursos de acesso que dificultam o acesso aos equipamentos. Isso, para o lado do usuário, tem um aspecto muito positivo, muito bom, mas, para o aspecto da perícia, traz mais dificuldades para que possamos fazer o acesso, quando esse acesso é necessário, do ponto de vista de análise pericial, ou seja, já dentro de um ambiente, num contexto policial e de Justiça.

Esses são desafios, também, que nós temos, desafios esses que precisamos vencer todos os dias, para que consigamos manter o nível de trabalho que a Polícia Federal, do ponto de vista da perícia, tem oferecido à sociedade brasileira.

Agradeço mais uma vez pela oportunidade e retorno a palavra.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada. E, até fazendo aqui uma consideração, quando o senhor fala da Internet das coisas, primeiro, já temos um *chip* em nós. Onde vamos levamos um celular que, com o serviço de localização, é possível saber o local onde estamos, e cada vez mais também a questão de usarmos os aplicativos de celulares, até mesmo com música, GPS, nos carros. Então conseguimos, o dia inteiro, estar monitorizados, tanto pelo carro, como pelo celular.

Acho que a Internet das coisas é um tema, Deputado Jean Wyllys, que temos que trazer para dentro desta CPI e discutir, os riscos que corremos ao ser monitorizados 24 horas.

O SR. DEPUTADO JEAN WYLLYS - Já estamos.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Há muito tempo.

Gostaria de passar a palavra ao Sr. Alessander Florindo da Silva, também representante do Instituto Nacional de Criminalística.

O SR. ALESSANDER FLORINDO DA SILVA - Eu gostaria de agradecer pelo convite à Deputada Mariana Carvalho, em nome de quem cumprimento todos os presentes.

Eu sou perito criminal federal, trabalho no Instituto Nacional de Criminalística. A minha formação é um pouquinho diferente da dos colegas aqui. Eles são da área de informática. Eu sou engenheiro eletricista e trabalho no serviço de perícias em audiovisual. Então, tudo quanto é arquivo de áudio, esses vídeos, acabam caindo em nossas mãos.

Eu gostaria de tratar, primeiro, da questão de cadeia de custódia, que o colega Leonardo citou um pouquinho antes. Na parte de interceptações de comunicações telefônicas ou telemáticas, nós precisamos garantir que, desde o momento da interceptação desse material, ele se mantenha íntegro até o fim da persecução penal.

O primeiro tema que eu trago seria, na verdade, um conjunto de sugestões para que possamos garantir essa cadeia de custódia.

Os sistemas têm melhorado ano a ano. Na Polícia Federal, os dois principais sistemas que utilizamos para a parte de interceptação telefônica, principalmente, são o Sombra e o Guardião. Dez anos atrás, o sistema era bem falho, tinha uma série de problemas, mas, com o passar do tempo, as empresas e as exigências que fazemos internamente fazem com que o sistema melhore.

Hoje, os sistemas são auditáveis. Então, eles são relativamente seguros. Eu digo relativamente, porque não existe segurança total. Isso é uma coisa que precisa estar claro para todo o mundo, e nós consideramos que é muito relevante trazer mais elementos de segurança para esse material.

A sugestão que eu trago hoje seria o quê? Fazer uso de tecnologias que estão disponíveis no mercado, como certificados digitais, uso de registros de resumos criptográficos e de uma Autoridade de Carimbo de Tempo, que já está homologada no Brasil pelo ITI, coisa de poucos anos atrás. Passou a ser

homologado o uso desse tipo de atividade, que seriam os cartórios digitais de tempo.

Na prática, a ideia seria a seguinte: você tem uma comunicação sendo interceptada. No momento em que essa comunicação se encerra, você vai salvar um arquivo digital com esse conteúdo, você calcula, usa um algoritmo matemático chamado h*ash*, que é o resumo criptográfico, eu gero uma série de dados de tamanho fixo que tem algumas propriedades. Uma propriedade deles é a seguinte: se eu modificar um *bit* que seja dentro de um arquivo original e tentar calcular de novo esse resumo criptográfico, vou encontrar um número totalmente diferente. Outra propriedade que ele tem é que a partir dele eu não sou capaz de recuperar a informação original. Então, eu posso trafegar essa informação livremente, e não é possível que a pessoa com conhecimento dessa informação descubra qual era a informação originalmente a que ele se refere.

Ele tem algumas outras vantagens que são do uso técnico e que não vêm ao caso trazer. Mas o que eu faço? A comunicação foi interceptada, eu pego esse resumo criptográfico, faço uma assinatura digital com um certificado digital da própria máquina da polícia que fez o procedimento de interceptação, mando esse conjunto para uma terceira parte contratada, que seria essa empresa chamada ACT, que é uma Autoridade de Carimbo do Tempo, já homologada pelo ITI, essa empresa pega esse conteúdo, acrescenta a informação de data e hora, buscada do Observatório Nacional, e usa o certificado digital dela e assina esse conjunto todo. De posse desse material, isso é levado e arquivado numa base de dados, e eu consigo, a partir desse procedimento todo, no futuro, 3, 4, 5 anos depois, quando essa gravação é levada à Justiça e a parte alega que houve uma edição desse material, é possível verificar que essa informação é a mesma, desde o momento em que ela foi assinada digitalmente pelo cartório de tempo. Com isso, a partir do momento em que eu faço a interceptação, questão de poucos segundos depois, eu já consigo esse Carimbo do Tempo. Você cria a situação de garantir que, a partir daquele momento, não houve modificação do conteúdo. Logo, não há tempo hábil para que alguém tenha conhecimento, faça medição no arquivo, insira dentro do sistema etc. Seria uma maneira muito prática de a gente conseguir ter a garantia de cadeia de custódia desse tipo de interceptação.

Essa sugestão, na prática, não necessita de uma legislação. Ela já foi levantada internamente e está sendo desenvolvida dentro de um novo sistema de interceptação de sinais da polícia. Eventualmente, se a questão temporal não for satisfatória, podemos conseguir por outros meios.

Um segundo elemento que eu gostaria de trazer à pauta é o seguinte: não adianta nada eu fazer uma interceptação de comunicação telefônica ou telemática, colocar na cadeia de custódia excelente, ter esse material todo armazenado e, na hora em que quero ouvir o que foi transmitido, não consigo, porque aquela comunicação está criptografada.

A efetividade de uma organização criminosa está diretamente ligada à capacidade de comunicação que seus membros têm. E hoje essa comunicação está migrando do telefone fixo, do celular, para os *smartphones* e para aplicações como o Skype, como o WhatsApp, como o Telegram, que é possível fazer uso de criptografia.

No videozinho, que o André apresentou aqui, apareceram lá algumas caixas. Na reportagem da *Globo*, apareceram ali alguns equipamentos que tinham como missão quebrar a criptografia de arquivos. Isso aí leva um tempo enorme, é superineficiente. Nós precisamos de outro caminho para fazer essa quebra. Se nós temos uma legislação vigente que diz que em determinados momentos é aceitável que a comunicação do indivíduo seja quebrada, que esse direito fundamental seja afastado, nós precisamos, sim, ter a capacidade de dizer à empresa que está provendo esse serviço de comunicação que ela tem a obrigação, ela tem o dever de nos passar a informação de como é que eu faço para quebrar essa comunicação.

Ela usou uma chave criptográfica para fazer essa comunicação. Ela tem que ter, então, portanto, a obrigação de manter salva essa informação na chave criptográfica e, na hipótese de haver a quebra ou afastamento do sigilo de comunicação do indivíduo, ela tem o dever de fornecer isso ao juízo.

Nós deveríamos receber isso das próprias empresas, não tentar ficar quebrando por força bruta. Esse é um tratamento que deveria ser dado de forma uniforme, e eu acho que a melhor maneira seria através de lei.

Um terceiro tema em relação ainda à parte de interceptação de comunicações telefônicas e telemáticas estaria mais afeta à ANATEL. O modelo atual não é muito

bom. Nós deveríamos seguir modelos mais modernos, como o proposto num consórcio europeu chamado ETSI, em que o desvio da comunicação telefônica interceptada ou telemática, a intercepção, de fato, ela é realizada dentro da rede de operadora de comunicação ou provedor de serviço a Internet, e esses dados interceptados devem ser encaminhados à Polícia idealmente por um canal de dados. A comunicação telefônica em VOIP, que é voz sobre IP, porque é assim que essa informação já circula dentro da rede das operadoras, e a comunicação de dados hoje já é entregue em dados, porque não haveria outra maneira de fazê-lo. Infelizmente, hoje, o modelo que nós temos é o modelo mais barato para as operadoras.

Então, elas fazem essa transmissão dessa informação para a polícia de uma maneira que não é das mais eficientes. Ela simplesmente gera uma nova ligação telefônica e ela junta as duas comunicações, o canal de transmissão do locutor A e do locutor B juntos, essas duas informações num canal só, faz um processo de mixagem, gera uma nova ligação telefônica para a polícia e faz essa transmissão. Essa ligação para a polícia tem um monte de problemas. Essa ligação pode cair. Então, mesmo que os indivíduos mantenham uma comunicação ao longo do tempo, a comunicação com a polícia pode ser interrompida a qualquer momento. Você insere mais ruídos nesse canal. Essa informação chega pra gente com a mixagem dos dois canais. Então, eu tenho dificuldade de entender falas sobrepostas. Eu poderia receber isso em canal estéreo. Eu poderia ser capaz de ouvir o locutor A isoladamente, depois ouvir o B. Isso me facilitaria também o uso para os sistemas de identificação automática de locutor.

Então, eu teria várias vantagens em receber esse dado diretamente como pacote de dados. Hoje, infelizmente, não é assim, porque foi a maneira, 10 anos atrás, que as operadoras encontraram, que era mais prático, mais barato para elas, de fazer essa implementação.

Então, existem melhorias ainda possíveis de serem aplicadas à parte de interceptação de comunicações. Do meu ponto de vista, eu acho que a ANATEL é que deveria ter um papel preponderante nisso aí e, em conjunto com as polícias, negociar o melhor modelo possível para fazer essas interceptações.

Era só isso o que eu tinha para trazer, e eu fico aberto a questionamentos.

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

Com a palavra o Dr. Bruno Teles, Presidente da Associação Brasileira de Criminalística.

O SR. BRUNO TELLES - Cara Deputada Mariana, eu gostaria de agradecer pelo convite de estar aqui. É difícil falar depois de todo mundo, quando quase tudo já foi dito. Eu vou fazer uma breve apresentação, não tão técnica, mas um pouco com a visão da criminologia, para tentar criar uma situação em que nós possamos enxergar o nosso cenário atual.

Meu nome é Bruno Telles. Sou Presidente da Associação Brasileira de Criminalística, que representa hoje os peritos oficiais de natureza criminal, que, em última instância, é quem irá receber esse material apreendido pelas autoridades policiais para prover a prova material em juízo. E eu queria falar antes um pouco sobre o background da Internet. Quando ela surgiu aqui no Brasil e passou a abertura do *backbone* para provedores comerciais, em 1995, eu pude acompanhar isso bem de perto. Eu era graduando na Universidade de São Paulo e pude acompanhar esse crescimento dos serviços de Internet.

Então, naquela época, o acesso era livre, muito mais livre do que a temos hoje, pouquíssimos bloqueios. Ainda estava começando a popularização do www. Para se ter uma ideia de como os bloqueios eram poucos, era possível você mandar um *e-mail* para qualquer pessoa e com o remetente que você quisesse, mesmo que ele não existisse. Então, você poderia mandar hoje um *e-mail* para qualquer Deputado aqui com o remetente de dilma@planalto.gov.br. Você iria responder e aquilo não iria retornar efetivamente para quem tinha enviado, mas você conseguia, de certa forma, mandar uma mensagem oculta para uma pessoa que você quisesse.

A grande sensação daquela época era invadir servidor, e eu tive a oportunidade de montar uns dois ou três servidores na USP, e você tinha que torcer para ninguém descobrir que você tinha montado um servidor lá dentro, porque a sensação na época era tentar invadir o servidor do colega de disciplina ali, justamente como uma forma de treino. Os servidores eram altamente desafiantes, tinham uma concentração de informações.

Então, eu me lembro muito dos meus colegas de engenharia de computação invadindo o servidor da USP para aumentar a taxa de *download*. Uma coisa simples, mas que você consegue, de atitudes às vezes inocentes, deslumbrar um cenário em que você poder fazer absolutamente qualquer coisa e ficar sem ser detectado. Mas aí o que aconteceu com os servidores?

(Segue-se exibição de imagens.)

Houve uma reação *server side*, as empresas começaram a contratar *hackers* para montar o seu sistema de *firewall*, seu sistema de defesa e invadir um servidor começou a ser uma tarefa hercúlea para a maioria dos especialistas da época. E também ele não dava nenhum retorno tão efetivo, até porque a criptografia começou a ser usada nesses servidores e você basicamente tinha acesso a um dado criptografado e que você ia ter que gastar ali horas e horas, e, quem sabe, até anos de computação para tentar quebrar aquele código na força bruta.

E foi aí que começaram os ataques *clients side.* Naquela época, os ataques *clients sides* eram muito mais requeridos, começaram a ser mais requeridos pelos criminosos da vida real, porque ele te dá uma margem menor. Às vezes, você invade um computador de qualquer um de nós aqui, não vai achar nada de interessante, nenhuma informação substancial, mas, ao mesmo tempo, eu tenho milhões de computadores que podem ser invadidos, e os computadores estão, na sua maior parte, desprotegidos, e eu posso trabalhar com alvo específico.

Então, naquela época, as maiores denúncias que se tinha desse tipo de ataque *client side* era da área empresarial, justamente para espionagem industrial. E a reação *client side* também aconteceu, em que os dispositivos de uso doméstico começaram a avançar, a ter níveis de criptografia maiores, contar com antivírus, proteção de Internet e proteção de dados individuais.

Eu cito aqui o caso da Blackberry. Foi uma empresa que todo mundo acha que ela vende celular, mas ela vende, na verdade, serviços. Ela é uma empresa que foi a primeira do ramo a identificar que as pessoas precisam se comunicar de forma segura e não deixar os seus dados, o seu tráfico de dados à disposição de qualquer um, seja por um ataque ou qualquer outra coisa.

Para quem assiste televisão, há um seriado chamado *House of Cards,* você vê todos os parlamentares americanos usando Blackberry. Eles não usam

Blackberry por acaso. Eles usam Blackberry pelo nível de criptografia que existe naquele telefone, só que hoje, do Iphone 4S para cá, aquele nível de criptografia está acessível para qualquer um de nós, Android também, dependendo da versão que você tiver e com uma versão certa de *softwares* para troca de mensagens ou para ligação utilizando VOIP. Toda aquela criptografia que surgiu durante a Guerra Fria está à disposição de qualquer um de nós.

Então, o que hoje temos no ambiente cibernético? Temos um cenário em que a possiblidade do anonimato é muito grande. Você tem um escala muito grande e uma agilidade absurda. Isso está disponível para qualquer um. Você pode ter uma ideia simples, como o criador do Uber teve de oferecer um serviço de transporte urbano, e a sua empresa valer bilhões de dólares em poucos anos, ou você pode criar a sua rede de pedofilia pelo Whatsapp.

Onde está o cerne da questão? O cerne da questão é que a interceptação de comunicação hoje deixou de ser uma decisão judicial; a interceptação da sua comunicação hoje é uma decisão sua. Se você comprar o celular certo e utilizar *softwares* adequados, somente você, fornecendo a sua senha, vai poder dar acesso para outra pessoa saber por onde você andou trafegando na Internet, por onde você navegou, quais são os seus contatos e as mensagens que você enviou.

O SR. DEPUTADO JEAN WYLLYS - Por exemplo, além do Blackberry.

O SR. BRUNO TELLES - Whatsapp.

O SR. DEPUTADO JEAN WYLLYS - Não, mas você falou em aparelho, em *hardware*, não só *software*.

O SR. BRUNO TELLES - Não, você tem que combinar o *hardware* com o *software*. Se você pegar um aparelho de celular ultrapassado, em que eu conheça as vulnerabilidades, eu consigo acessar as suas mensagens, porque o Whatsapp cria um banco de dados no seu aparelho. Então, você tem que juntar o *software* e o *hardware*.

Hoje, o Iphone 6s, eu duvido muito. Eu desconheço qualquer perito criminal que saiba a vulnerabilidade do Iphone 6s. E se você junta isso, por exemplo, ao Whatsapp... Eu tenho um colega que me disse que fez uma requisição de dados para o Whatsapp, e o Whatsapp falou assim "*Não posso te ajudar, pois os dados*

que trafegam pelo meu servidor são criptografados de ponta a ponta. Eu não sei o que passou por aqui, eu não consigo te dizer a mensagem que foi trocada".

O SR. DEPUTADO FÁBIO SOUSA - Desculpe-me a intromissão, só para eu entender. Quer dizer então que se a pessoa comete crime via Whatsapp, combina um crime, vocês não têm como investigar?

O SR. DEPUTADO JEAN WYLLYS - Só se adquirir o aparelho e tiver a senha de acesso ao conteúdo, aparente, que está armazenado.

O SR. BRUNO TELLES - Hoje existe uma grande gama de celulares e outros dispositivos que têm equipamentos que exploram justamente as vulnerabilidades. Elas estão cada vez mais difíceis. Mas eu posso lhe dizer que estamos chegando a um ponto em que realmente não vamos ter mais como investigar, e essa é uma das sugestões que eu fiz para vocês aqui.

O que levou a isso? Os ataques *client server-side* levaram as empresas a criptografar todos os dados. Elas têm um medo terrível de armazenar esses dados e alguém, de repente, invadir o servidor delas, subtrair todos esses dados, e elas terem que pagar milhões de dados em indenização. Já imaginou todas as suas mensagens do Whatsapp vazadas? O que ia ter de separação acontecendo por aí.

E o que eles fazem? Eles promovem um *software* que, quando instalado no seu aparelho — e vamos supor que o senhor vai mandar uma mensagem para o Deputado Jean —, a mensagem sai criptografada do seu celular, passa pelo servidor da empresa, criptografado a 128 *bits,* a 256 *bits*, e só o Deputado Jean, com a chave dele, vai conseguir abrir aquela mensagem. Se você fizer a interceptação, você vai interceptar um dado criptografado, e, hoje, com um dos melhores quebradores de senha, pode levar 100 anos para descobrir o que você mandou para ele. Hoje é o ambiente, e o ambiente leva ao anonimato, e anonimato em segurança pública só significa uma coisa: impunidade.

Eu era um grande defensor da Internet livre, adorava, lá na USP, o que a gente fazia. Hoje eu vejo que é um grande estratagema comercial. Qual é o estratagema comercial? Vamos manter a Internet livre sem regulamentações. Quando você tem um *lag* de regulamentação do Estado, você pode criar um serviço, vender esse serviço em outro país e, até que o Estado descubra que ele tem que tributar aquele serviço, ou que ele tem que regulamentar aquele serviço, podem se

passar alguns anos. E esses alguns anos te dão uma margem de lucro muito grande.

Eu considero, hoje, esse tema de Internet livre um estratagema. É a maior ferramenta para se cometer crimes e ficar no anonimato, hoje.

Vou falar um pouco dessa demanda, antes de concluir. Será que isso é resultado por acaso? Os espaços vazios tendem a ser ocupados. Se você tem um espaço onde a mão do Estado é menor e a capacidade de investigação do Estado é menor, é melhor atuar lá, se você é criminoso.

A demanda por interceptação telefônica na segurança pública hoje está diminuindo muito. Hoje somente os amadores falam de crimes em ligação normal. E está aumentando muito a demanda por perícias em computadores, dispositivos móveis, *tablets*, celulares, porque são formas mais seguras. A mesma ferramenta criada para manter comunicações entre Parlamentares, entre executivos de forma segura também é utilizada pelos criminosos.

Nós suspeitamos hoje que a maior rede de pedofilia esteja no aplicativo Whatsapp. Inclusive, é possível fazer transferência financeira pelo Whatsapp. Como o traficante hoje vende a droga, acerta o transporte da droga? Fazendo ligação telefônica? Não, ele manda uma mensagem via Whatsapp ou baixa qualquer outro aplicativo que criptografe as mensagens de ponta a ponta.

E aí nós chegamos justamente a essa necessidade de modernização. Não há nenhuma perspectiva — pelo menos considerando a minha experiência como Presidente da ABC — de que nós avancemos muito nesse cenário sem contar com a colaboração dos provedores de serviço. Não há como se entrar na Internet hoje sem passar por um ou dois ou quem sabe até mais provedores de serviço. Acesso de conteúdo, de navegação, de qualquer coisa.

O SR. DEPUTADO JEAN WYLLYS - Provedor de acesso e provedor de conteúdo... No caso, tanto as telefônicas quanto Facebook, Google...

O SR. BRUNO TELLES - Tem que ser integrado. Vamos supor que eu tenha mandado um *e-mail* lhe ameaçando. Aí você aciona a Polícia Federal e um perito da Polícia Federal pega aquele *e-mail*. Se tiver sido enviado pelo Gmail, vem sem cabeçalho. Já não dá para saber qual IP enviou aquele *e-mail*. É necessário oficiar o Google, por decisão judicial, e perguntar: *"Olha, qual IP enviou a mensagem tal para*

o destinatário tal?" Aí ele vai informar aquele IP. Quando aquele IP chega, descobre-se, na Internet, de quem é aquele IP. Vamos supor que seja da NET, aqui de Brasília. É necessária mais uma decisão judicial. O juiz tem que solicitar à NET a informação: *"Quem estava utilizando o IP tal, no momento tal, assim, assado, que acessou o serviço tal do Google?"* A NET vai responder.

De repente, pode-se chegar a um *cyber* café, a uma rede aqui da Câmara. Qualquer pessoa que visita um Parlamentar na Câmara pega uma senha e pode utilizar *wi-fi*. E, de repente, descobre-se que partiu de dentro da Câmara mesmo o *e-mail*, mas nunca se conseguirá apontar quem o enviou, pois foi um acesso anônimo.

O anonimato protege o consumidor de certos rastreamentos que o Facebook faz, mas também é a principal ferramenta utilizada pelos criminosos hoje. Sem a colaboração desses provedores de serviço, seja serviço de comunicação, seja serviço de postagem de fórum... Hoje há fóruns que permitem postagens sem identificação, aliás, grande parte deles é assim. O usuário tem acesso a algum tipo de *proxy* que disfarça a sua navegação, disfarça sua atuação na Internet.

Se nós não tivermos nenhum tipo de colaboração desses servidores e provedores de serviço, em breve vai ser impossível investigar qualquer tipo de crime cibernético. Nós vamos pegar sempre aquele pequenininho, o amador curioso, que está começando agora, mas o especialista, que é quem efetivamente mantém as redes de pedofilia, que é quem mantém as redes de interceptação de dados bancários, que é quem organiza efetivamente grandes operações para difundir o seu negócio, vai estar muito bem protegido por uma rede em que se defende supostamente a liberdade e em que basicamente o anonimato é o grande pagamento para quem utiliza a rede.

O segundo item que eu cito como necessário à melhoria do sistema é o fortalecimento da perícia criminal. As perícias estão ficando cada vez mais caras, cada vez mais complexas. Há uma necessidade grande de especialização da perícia criminal.

E nós temos um projeto na Casa justamente para constitucionalizar a perícia criminal e permitir que ela tenha uma atividade desvinculada da Polícia Civil e possa se especializar, na medida do possível. O que quer dizer, neste caso, "na medida do possível"? Significa que eu tenho que ter um perito para cada lançamento de celular,

se eu quiser efetivamente fazer perícia naquele dispositivo. Ele tem que investigar aquele celular e falar: *"Olha, estou aqui há 2 meses trabalhando e descobri essas vulnerabilidades. Nós conseguimos fazer perícia nesse celular através desse meio."* Para todo lançamento de *software*, tenho que ter alguém investigando as vulnerabilidades. É um tipo de agilidade que não conseguimos ter hoje inserida dentro das polícias civis.

Em suma, era isso o que eu tinha a falar para vocês.

O recado é que os espaços vazios vão ser preenchidos. A Internet foi mais um ambiente criado. Agora, nós temos os criminosos cibernéticos, e ela oferece a grande chance do crime perfeito justamente por essa capacidade enorme de se manter o anonimato. Se você souber efetivamente o que você está fazendo, você tem o seu anonimato garantido.

Muito obrigado.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Muito obrigado.

Encerradas as apresentações, passarei ao debate.

Por ordem de inscrição, concedo a palavra ao Deputado Fábio Sousa, para que faça suas intervenções, por 3 minutos.

O SR. DEPUTADO FÁBIO SOUSA - Sr. Presidente, não vou usar todo o meu tempo, até porque é muito curto. Cumprimento V.Exa. e todos que estão à mesa.

Tenho três perguntas. Eu imaginei que o Dr. André ia falar sobre o Whatsapp, e o Dr. Bruno também falou de forma muito clara. É uma preocupação que não só esta Comissão Parlamentar de Inquérito tem, mas que também esta Casa precisa ter urgentemente, porque nós estamos sendo informados hoje de que há uma certa facilidade. Até quem não sabia mexer em celular ou na Internet aprendeu a mexer no Whatsapp. Então, hoje há uma facilidade muito grande de se cometer crimes. Nós precisamos evidentemente armar o sistema de segurança do Brasil para combater os crimes.

Farei três perguntas preparadas pela assessoria do partido. A primeira pergunta é sobre a Convenção de Budapeste. Os senhores têm conhecimento? Parece que o Brasil não aderiu a esta Convenção. Trata-se de uma Convenção que troca informações, via crimes cibernéticos, no mundo todo. Por que o Brasil não é

um Estado-membro? Na visão dos senhores, seria importante que o Brasil fizesse parte disso?

Segunda pergunta. Nós aprovamos recentemente o PL 1.404, de 2011, nesta Casa, que voltou ao Senado — e, com toda sinceridade, não sei como anda no Senado Federal —, que vai permitir que as próprias polícias, tanto a Polícia Federal quanto a Polícia Civil, possam usar o que os Estados Unidos, a Inglaterra e Portugal já usam, que são os chamados espiões. É assim que eles falam, que são os policiais à paisana na Internet que se disfarçam de pedófilo, de crianças, para ir atrás de pessoas que cometem esse tipo de crime. Até pouco tempo atrás nós não podíamos ter isso por falta de legislação no Brasil, mas com essa aprovação, parece-me que vamos ter condições.

Pergunto aos senhores se a polícia estará preparada para isso, haja vista, Sr. Presidente, Deputado Rodrigo Martins, que isso tem sido usado até por uma ONG italiana, que tem feito um trabalho extraordinário no mundo todo caçando esse tipo de pedófilo. Uma recente reportagem do programa *Fantástico* mostrou que havia dois ou três agindo no Brasil dessa forma, e eles não podiam fazer nada. Essa ONG passava informações à autoridade policial local, mas ela não podia fazer nada, devido a não aprovação dessa lei, mas agora ela está aprovada.

Por fim, pergunto aos senhores, em especial, ao pessoal da Polícia Federal, se hoje a polícia dispõe de recursos financeiros necessários para tomar as medidas preventivas necessárias, e também medidas repressivas, para combater pedófilos, *hackers*, gente que comete esse tipo de crime, que, se hoje ainda não é o principal crime cometido, com certeza, será no futuro, haja vista sermos todos escravos da modernidade. Não adianta, podemos até tentar fugir hoje, mas logo, logo seremos abraçados por ela.

Era isso, Sr. Relator e Sr. Presidente.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Passo a palavra à Mesa para alguém que queira se manifestar.

O SR. DEPUTADO JEAN WYLLYS - Não é melhor fazer as perguntas em bloco?

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Só temos mais dois inscritos, Deputado Jean, mas se for consensual...

O SR. DEPUTADO FÁBIO SOUSA - Elimina as três perguntas e depois eles respondem.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Então, se é consensual, passaremos ao bloco.

O Deputado Jean Wyllys é o segundo inscrito.

O SR. DEPUTADO JEAN WYLLYS - Obrigado, Sr. Presidente.

Quero agradecer a todos pelas falas, pelas contribuições, e agradecer em especial ao André pelas sugestões que deu. Eu não sou Relator da CPI nem Relator das Subcomissões, mas registro todas as sugestões dadas por todas as pessoas que vieram às audiências públicas.

Eu tenho duas perguntas específicas para fazer. André, você usou o conceito de crime organizado para dizer que o crime organizado opera no nível da violência sexual contra criança e adolescente, motivado ou não por pedofilia. Tem gente que comete crime de exploração e violência sexual contra criança não necessariamente movida por desejo, mas por dinheiro, e há aqueles que consomem e que são movidos por desejo.

Eu pergunto se essa noção também pode ser aplicada ao crime de ódio e às difamações, porque no Brasil há uma série de *sites* constituídos legalmente que operam como uma rede de difamação, destruição de reputações e de incentivo a crimes de ódio.

Vou dar um exemplo. Em 2012, foram presos dois rapazes, um de Brasília e outro de Curitiba, que tocavam aquela página chamada Silvio Koerich, que incitava o ódio contra minorias e defendia a pedofilia apenas para meninas, o que era uma coisa bem curiosa. Quer dizer, a pedofilia estava autorizada, desde que praticada contra meninas, porque a pedofilia praticada contra meninos, na cabeça deles, estava associada à homossexualidade, algo que eles tinham de erradicar. É o tipo de doente que produz esse conteúdo.

Eu pergunto se a gente pode estender essa noção também para esse tipo de crime, se a polícia pode operar com essa noção de crime organizado.

Você também falou — posso chamar de você, não posso? — que falta infraestrutura tecnológica para a polícia, a partir da qual ela deve operar. O que falta mesmo? Como é a infraestrutura da polícia para fazer o trabalho de prevenção e

repressão a esses crimes? O que falta nessa estrutura para a polícia empreender melhor esse trabalho?

Evandro, você falou do caso do sequestro dos bebês, que não era ficção, era realidade, mas isso foi parar na ficção. *CSI: Cyber* tratou exatamente deste caso do acesso às babás eletrônicas e do sequestro de bebês.

Eu pergunto: a polícia daqui registrou algum caso utilizando as câmeras de segurança que também podem ser acessadas pelo celular? Quer dizer, as pessoas instalam câmeras de segurança em suas casas e as acessam do trabalho. Há algum caso de invasão dessas câmeras para praticar roubos, assaltos e sequestros?

Por fim, eu pergunto ao Bruno, na verdade não é uma pergunta, mas um comentário: eu sei que você defende arduamente o fim do anonimato, só que o anonimato é algo bastante ambivalente. A gente não pode esquecer que, graças ao anonimato, algumas liberdades individuais são garantidas, e a liberdade é um valor. Então, o anonimato está sempre nessa economia entre algo importante para defender as liberdades e entre algo usado pelos criminosos para promover seus crimes. Assim, a gente fica em uma postura ambígua de defender ou não o anonimato.

Há um caminho para se incidir contra o anonimato apenas e tão somente no caso dos crimes? Em que medida os agentes públicos estão preparados para lidar com essa triagem?

Vou dar um exemplo: no Rio de Janeiro, o Ministério Público empreendeu toda uma investigação junto à polícia em relação aos movimentos sociais de esquerda anti-Cabral que questionavam os gastos da Copa. Essas pessoas foram indiciadas por causa dessa investigação, e essa investigação tinha mais a ver com a ideologia dos agentes públicos do que com crimes praticados pelas pessoas. Para se ter uma ideia, até Bakunin, um filósofo do século XIX, foi citado em um processo como alguém a ser indiciado. Então, em que medida os agentes públicos também estão preparados para agir...

O SR. DEPUTADO ESPERIDIÃO AMIN - Mas ele foi registrado pelos comunistas.

O SR. DEPUTADO JEAN WYLLYS - *(Risos.)* Foi, ele estava lá participando.

O SR. DEPUTADO ESPERIDIÃO AMIN - Ele era anarquista, e os comunistas que o perseguiram.

O SR. DEPUTADO JEAN WYLLYS - Sim, Deputado Amin, mas ele não tem que ser indiciado em um processo de quem jogou coquetel molotov contra banco. Faltou informação aos agentes públicos para saber que ele existiu no século XIX e produziu no século XIX e não no século XXI.

Então, esse tipo de postura está no agente público, e o agente público tem posição, ele não é uma figura neutra, por mais que ele se queira colocar assim.

Vou dar um exemplo dos crimes motivados por homofobia ou por homolesbotransfobia. A grande maioria deles, até hoje, resultou em nada, quer dizer, ficaram impunes os crimes, porque simplesmente os delegados não reconhecem a motivação homofóbica daquele crime. Por não reconhecer a motivação homofóbica, eles dão outra linha de investigação, que nunca chega ao assassino, embora os movimentos sociais e os amigos estejam dizendo que, sim, há uma motivação homofóbica que poderia resultar em um crime. Então, esse tipo de postura por parte dos agentes públicos ameaça, por exemplo, as liberdades individuais.

Queria, então, que você explicasse melhor de que maneira a gente pode discernir as duas coisas: defender o anonimato para preservar as nossas liberdades e combater o anonimato, quando se trata de crimes, mas aí todos os crimes e não seletivamente, o que eu reconheço como crime e o que eu não reconheço como crime.

São essas três questões.

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

Com a palavra o Deputado Silas Freire.

O SR. DEPUTADO SILAS FREIRE - Sra. Presidente, Deputada Mariana Carvalho, cumprimentando V.Exa., eu cumprimento a todos da Mesa.

Queria dizer que nós tivemos uma tarde hoje muito importante. Estiveram aqui aqueles que têm acesso... Por isso, eu defendi, em uma PEC que votamos ainda há pouco no plenário, que eles não perdessem a autonomia e não se diferenciassem dos delegados, para que tivessem o seu poder de demonstrar, em todo o País, o seu trabalho.

Da mesma forma, senhores, eu digo que estou assustado, pois os senhores acabaram de nos informar que o ambiente cibernético é completamente “seguro” e totalmente “inseguro”. Se nós usamos um lado para proteger o cidadão que adentra a grande rede, nós não o protegemos por total, mas protegemos o bandido quase na sua totalidade, pelo menos foi o que eu entendi da narrativa dos senhores aqui.

Só para citar a minha compreensão de toda a fala dos senhores, eu tenho algumas perguntas que, claro, já foram até por vocês narradas, mas por mim precisam ser detalhadamente entendidas.

Qual é o grau, de zero a dez, por exemplo, que os senhores têm das dificuldades de investigação para descobrir um crime cibernético como um todo? Qual o grau, de zero a dez? Isso vocês vão poder relatar. E depois nos falem dos limites. São vocês que investigam, são vocês que dominam hoje a técnica da investigação. O limite do anonimato é importante? Nós não podemos fugir disso, esta Casa não pode fugir disso. Vai dizer que é liberdade? É liberdade. Mas, se o anonimato for para propagar e dar novas dimensões ao crime, nós não podemos defendê-lo, nós temos de estudar uma forma. É um limite? É uma linha de limite? Os senhores também poderão nos orientar.

Pelo que eu entendi desta Comissão Parlamentar de Inquérito, pois já cheguei com o andar da carruagem, ela é muito mais propositiva do que investigativa. É o que eu vejo nas suas audiências públicas e nas suas proposições.

Então, essa é a nossa linha de busca de compreensão. De zero a dez, qual é o grau da perícia brasileira hoje de elucidação total de crimes cibernéticos, sejam eles em aplicativos que dificultam a leitura, que não guardam nos seus *softwares*? Qual é o grau? Esse é o entendimento que nós gostaríamos de ter e saber se esse limite do anonimato poderia ajudar na elucidação dos fatos por parte dos senhores e da perícia criminal como um todo.

Muito obrigado.

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

Com a palavra o Deputado Nelson Marchezan Junior.

O SR. DEPUTADO NELSON MARCHEZAN JUNIOR - Obrigado, Presidente Deputada Mariana.

Quero pedir desculpas aos palestrantes, pois, além desta CPI, hoje, ocorrem outras três, e de uma delas eu faço parte. Também faço parte da Comissão de Constituição e Justiça e da Comissão Especial que analisa o projeto de registro único de certidão de identificação, e ambas têm reuniões ocorrendo paralelamente. Então, eu cheguei atrasado, Deputado, e não tive a oportunidade de ver as manifestações dos senhores ao vivo, apenas as daqueles que apresentaram algum material eu poderei ler.

Eu teria só duas questões que foram colocadas quando estiveram aqui os representantes do Google, do Facebook e do Twitter. Discordando um pouquinho do Deputado Jean, o art. 5º, inciso IV, da Constituição, garante a liberdade de expressão, sim, mas ele veda o anonimato. Portanto, o anonimato está vedado pela nossa Constituição.

A minha pergunta é: como os senhores enfrentam, em suas ações, a questão da absoluta possibilidade do anonimato, em virtude das facilidades do Google, do Facebook, etc. de não exigir nenhuma identificação dos seus clientes, em que eles podem efetivamente navegar livremente, buscar informações, comprar produtos, levar informações falsas, verídicas? Enfim, em pleno anonimato. Há alguma ação no que se refere a isso? Existiria alguma forma de nós tentarmos organizar isso de modo mais transparente, em que pudéssemos acessar, de forma mais rápida, criminosos, por exemplo? Essa é a primeira questão.

Segunda questão. Eu não conheço, não tenho dados técnicos nem elementos para falar da *deep web*, mas o que sabemos é que, em reunião com o Google, com o Facebook, etc., os colegas entraram pelo aparelho da Câmara normalmente na *deep web* e viram tudo o que sabemos que tem lá. Foi mostrado ali que era possível qualquer cidadão entrar, inclusive de um computador público e de forma anônima.

Seria proveitoso que nós buscássemos formas de criminalizar o Google ou o Yahoo, que dão acesso de forma tão fácil a esses *links*, ou isso dificultaria de alguma forma a captura ou a localização de pessoas que cometem crimes através da *deep web*?

Eu gostaria que pudessem explicar um pouquinho melhor essa facilidade que se tem na *web* e como coibi-la. Para mim, que sou leigo no assunto, isso seria extremamente importante.

Era isso.

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

Com a palavra o Deputado Delegado Éder Mauro.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Sra. Presidente, senhores convidados, nós agradecemos pela fala de vocês, que só fazem somar nesta CPI.

Nas últimas reuniões, nós contamos com a presença de policiais federais e de representantes de algumas operadoras, ou ligados às operadoras. Vimos, nesse conteúdo todo, a dificuldade que existe hoje para a apuração de crimes cibernéticos, com um pequeno número de policiais federais e civis, não só pelo quantitativo, mas muitas vezes também até pelo qualitativo. Os criminosos cibernéticos estão 24 horas trabalhando nessa área e se adiantam cada vez mais, à frente até dos policiais. Então, nós vimos que essa dificuldade é muito grande.

Pelo que nos foi dado, salvo engano, são pouco mais de 20 policiais federais especializados em todo o Brasil nessa área de apuração de crimes cibernéticos. Sabemos que a quantidade de crimes, principalmente de pedofilia e outros tipos de crimes sexológicos que saem pela rede cibernética, inclusive os de estelionatos e os golpes, avança cada vez mais, e a polícia está cada vez menos na apuração. Eu gostaria de saber se essa questão é devido à falta de investimento dos Governos Federal e Estaduais nesse tipo de crime, principalmente na questão do aparelhamento dos policiais e da própria polícia.

Com relação às operadoras, para que se possa descobrir crimes e até preveni-los, nós precisamos, como foi dito aqui, inclusive por mim, que as informações sejam precisas e rápidas, a fim de que se tenham elementos suficientes, e isso não acontece por parte das operadoras. Algumas, inclusive, têm a cultura, se é que se pode dizer assim, de achar que as informações de dentro dela só podem sair com ordem judicial, quando muitas informações, pela própria legislação, não precisam disso, como, por exemplo, dados de pessoas, conteúdos de endereços, que não necessitam de uma ordem judicial, com exceção da quebra de sigilo telefônico.

Então, eu gostaria de saber, nesse ponto, se a Polícia Federal, principalmente, já que nós temos um perito direto aqui, que é o André, se ele pode

nos dizer se eles realmente também encontram essa dificuldade, porque nós estamos, através de requerimento, e a Presidente está sabendo disso — inclusive, fizemos uma pequena modificação, Sra. Presidente —, solicitando a presença de todos os representantes das operadoras e, inclusive, do representante da ANATEL, do Presidente, para que nós possamos fazer a regulamentação para que isso acabe, para que as polícias que estão em cima disso possam trabalhar de uma forma mais efetiva. Então, esse é um ponto.

E, por último, eu gostaria de saber do André, principalmente, sobre a questão das ordens judiciais de informações da quebra de sigilo. No que diz respeito aos SMSs, sabe-se que eles já passam decifrados para a polícia; na questão do áudio, ele passa decifrado para a polícia; na questão dos *e-mails*, passam decifrados para a polícia; de localização, através de ERB, de Azimute, tudo é passado tranquilamente para a polícia. E o WhatsApp, ele é passado decifrado? Porque o que nos foi colocado aqui pelas operadoras é que não o é. Então, nós gostaríamos de saber se a polícia recebe o WhatsApp, se ele é decifrado ou é indecifrável, se passam assim, para que a polícia possa fazer isso, o que eu acho uma inconveniência muito grande para que a polícia possa avançar.

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

Antes de passar às respostas, eu gostaria de fazer alguns questionamentos também. Fiz algumas anotações aqui durante as apresentações. Eu, até mesmo falando aqui e contemplando a pergunta do Deputado Nelson Marchezan Junior, gostaria de saber se existe alguma metodologia usada pela polícia, de investigação, e de que forma ela é feita, para investigar esse submundo, *dark net*, *deep web*, e também como é que vocês trabalham essa metodologia, até por termos conhecimento de que, quando falamos sobre esse assunto, muitas pessoas nunca ouviram falar sobre isso e não têm o conhecimento da gravidade do que ocorre nesse submundo.

Então, eu gostaria de saber até mesmo de uma forma para a CPI poder trabalhar. É como se fosse um *iceberg*, e nós só conseguimos mesmo ver a ponta do *iceberg*, e o que acontece nesse fundo nós precisamos trabalhar, porque é aí que

muitas vezes acontece mesmo a gravidade do uso dessas redes sem uma legislação prevista para esse assunto.

Eu gostaria também de saber como é que vocês fazem para caracterizar. Qual o critério que vocês usam para uma imagem ser considerada um caso de pornografia infantil ou ter ali algum crime, naquela imagem, se vocês têm algum critério para isso e quais são eles.

E também gostaria de saber de todos aqui, que já devem ter trabalhado — como foi dito até mesmo aqui pelo perito André, que trabalhou em algumas operações —, quais as operações mais chamaram a atenção nesses casos, que mexem mesmo com a sociedade, para termos noção. Quando falamos nessa condição de discutirmos sobre como a rede pode funcionar, muitas vezes as pessoas podem achar que nós estamos querendo acabar com essa permissão, de que forma utilizar as redes sociais. Até mesmo quando veio o Marco Civil da Internet, não havia nenhuma legislação que discutia esse assunto, e às vezes nós estamos causando uma censura em relação a isso. Mas temos que mostrar que existe, muitas vezes, esse caso grave, e uma parcela da sociedade ainda não tem conhecimento do quão grave pode ser isso que está acontecendo nas redes.

E eu também gostaria de saber como é que vocês enxergam essa questão do registro de conexão, essas conexões previstas no marco civil com relação ao compartilhamento dos IPs. Estiveram aqui presentes as Procuradoras, falando um pouco sobre esse assunto. E eu gostaria de ouvir a opinião de vocês. De que forma esta Casa Legislativa pode contribuir cada vez mais, com as sugestões, algumas eu anotei, para vocês encaminharem também a esta CPI. Nós sentimos, e é até preocupante, o Deputado Silas Freire foi bem feliz aqui com essa fala, que há uma preocupação de todos os Deputados em relação a isso, até por vermos que não existe um corpo, quando se coloca ali uma sala, como você mostrou que vocês têm, eu gostaria até de saber quantas salas vocês têm, e se nessa sala que foi mostrada vocês têm capacidade de trabalhar e de reconhecer todos esses casos de crimes cibernéticos.

Então, eram essas minhas perguntas. Eu vou passar a palavra para o Dr. André, perito da Polícia Federal, para começar a dar as respostas.

Muito obrigado.

O SR. ANDRÉ ABREU MAGALHÃES - Bom, vamos por ordem aqui. São várias perguntas. Vamos às perguntas formuladas pelo Deputado Fábio Sousa. Sobre a Convenção de Budapeste, eu não saberia dizer. O senhor me disse que o Brasil não é signatário, mas eu entendo que nós devemos participar de qualquer convenção que nos traga informações, e seria, assim, um contrassenso não querer uma informação de um país que nos possa auxiliar no combate ao crime organizado. Então, essa é a minha resposta em relação a isso. E, salvo engano, as Procuradoras falaram aqui também nessa convenção.

Quanto aos espiões, agentes, robôs, infiltrados na Internet, na última conferência internacional de combate aos crimes cibernéticos, que foi aqui em Brasília, e eu estive presente nas últimas quatro também, foi apresentado o protótipo de um robô e foi feita uma simulação na Internet. Eu não me recordo quem apresentou, mas foi alguém da área acadêmica, e, enfim, o resultado foi muito bom. Eles conseguiram coletar diversos IPs, esse robô conseguiu estabelecer um diálogo com os — vou usar o termo que os americanos usam — predadores, porque eles são verdadeiros predadores, de fato. Então, eles conseguiram reunir muitos IPs, só que, pela legislação brasileira, você estabelece um diálogo com um robô, e um robô não é um cidadão.

O SR. DEPUTADO FÁBIO SOUSA - Dr. André, eu não enfatizei a questão só do robô, mas também de policiais à paisana, de entrarem na Internet disfarçados de crianças ou disfarçados de pedófilos, para entrarem nessa *dark net* aí e descobrirem quem são essas pessoas.

O SR. ANDRÉ ABREU MAGALHÃES - Deputado, essa resposta é assim... O senhor está se referindo a infiltrados. Então, a lei de combate ao crime organizado prevê essa possibilidade. Isso existe, de fato. Então, eu sugeri que fossem feitas cópias de duas operações, para melhorar o senso crítico de vocês. E talvez alguma reposta que eu dê aqui... Em outras palavras, o crime organizado, esse que eu citei, ele está de olho nesta CPI. Então, se eu falar algumas coisas aqui, eu posso estar ajudando o crime organizado. Então, vocês vão poder ter acesso às cópias desses materiais, vocês aqui, entre vocês, e, aí, vocês vão ter acesso às metodologias. Por isso que eu... Perfeito?

O SR. DEPUTADO FÁBIO SOUSA - Estou satisfeito.

O SR. ANDRÉ ABREU MAGALHÃES - Com relação aos recursos financeiros necessários, eu não trabalho diretamente com essa parte. Mas o que eu posso dizer é que nós temos uma infraestrutura não em todos os Estados, como aquela que eu mostrei ali, das salas secretas, mas nós temos uma estrutura suficiente para lidar com os crimes. O que acontece é que o volume de crimes é muito grande. Então, eu tenho um fator aí, que é o tempo. Eu tenho prazo para o Código de Processo Penal, eu tenho prazo de prescrição. Às vezes, eu posso ficar 3 meses em uma perícia. Então, com relação aos recursos, em si, eu não sei. Eu sei o que eu tenho hoje para trabalhar. E o que eu tenho hoje para trabalhar eu posso dizer que são equipamentos de ponta e que são utilizados no mundo inteiro.

Bom, eu vou responder a todas as perguntas aqui e depois... O Deputado Jean Wyllys perguntou sobre a modalidade de investigação de crimes cibernéticos, se ela pode ser estendida a outros tipos de crime, como os crimes de ódio ou os crimes praticados contra as minorias. Quando eu mostrei as salas secretas, não sei se vocês prestaram atenção, ele falou de crimes cibernéticos no geral. Então, assim, a metodologia utilizada para investigar um crime de pornografia infantil na Internet é a mesma metodologia que eu vou usar para investigar um crime de ódio; a estrutura é a mesma. Então, às vezes nós recebemos um pedido de apoio, por exemplo, das polícias civis, e eu já fui indagado várias vezes por alguns delegados ou alguns membros do Ministério Público, algumas ligações telefônicas, e, assim, nós ajudamos na medida do possível e de acordo com a autorização que temos para ajudar.

Para investigar hoje um crime cibernético, na fase da investigação, se nós melhorássemos os nossos tratados internacionais, e se nós conseguíssemos fazer com que a legislação brasileira fosse aplicada, eu precisaria apenas de papel e caneta. Por quê? Porque são pedidos. Então, a pessoa, quando chega à delegacia, ela já chega com o impresso da ofensa que lhe foi feita no Facebook, ela chega com o aliciamento que foi feito ao seu filho, através do Facebook, através dos diálogos. Então, para isso, eu não preciso de equipamento. Para isso, eu preciso do quê? Capacitação de quem está recebendo essa noticia de crime. Então, às vezes, não é muito fácil... Para nós, entender essas tecnologias, entender esses termos é tranquilo, mas é difícil para o operador do Direito. Eu ainda não me formei em

Direito, mas estou na faculdade e faltam algumas matérias. Na faculdade de Direito, você tem medicina legal, você não tem cibernética, você não tem outras coisas. Então, é difícil para a pessoa que acaba de passar no concurso público, que assume como promotor, que assume como delegado, que assume como juiz, ir para ao interior e ter que resolver. Então, é difícil. Ou seja, tem que se cobrar o art. 4º da Lei Azeredo para que seja cumprida; a capacitação de todas as autoridades policiais, se possível; e a criação dos centros de combate unificado seria uma boa estratégia. Então, com relação a isso, eu respondi à pergunta?

V.Exa. perguntou o que falta de infraestrutura. O que falta de infraestrutura é o seguinte: aquela infraestrutura que mostrei poderia ser convertida, pelo local onde ela está, em um projeto e ser submetida ao SENASP – Secretaria Nacional de Segurança Pública – para avaliação, se é possível reaplicar para os Estados. Aquilo ali já está montado. Então, a partir de um modelo montado, é tranquilo montar um projeto e submeter para apoio.

Uma grande dificuldade que vou colocar para V.Exas. é a seguinte: quanto a esses equipamentos, para nós conseguirmos montar uma estrutura daquela, é difícil eu ter um certame licitatório. Eu deveria ter outra via para comprar aquele tipo de equipamento, por exemplo. Há um equipamento, por exemplo, que é o melhor usado no mundo, é feito em Israel, onde se trabalha com terrorismo, só que na hora que vou licitar, não posso direcionar. Então eu faço uma especificação e, talvez, aquele equipamento que ganhe a licitação não me atenda. Então, nós precisamos melhorar nessa questão para conseguir fazer uma aquisição direta.

Eu respondi à pergunta?

Agora, as perguntas do Deputado Silas Freire. A criptografia não veio para garantir o anonimato e, sim, para a confidencialidade e a integralidade, enfim, assim como a pólvora também não veio para ser um insumo de uma arma de fogo para disparar contra um cidadão de bem.

O anonimato na Internet pode ser resolvido, e aqui, nesta Comissão, V.Exas. vão ter condições de nos ajudar, para que isso não ocorra mais. Como V.Exas. podem ajudar? Podem ajudar forçando que os tratados sejam cumpridos, celebrando outros tratados, elaborando projetos de lei que preencham as lacunas.

Se não houver colaboração dos provedores de conteúdo, dos provedores de conexão, se eles não atenderem à nossa legislação, que sejam punidos. Nós temos legislação. Eu digo a V.Exas. que temos uma legislação, com relação ao Marco Civil, excelente. A finalidade à qual ela se destina é muito clara e objetiva. O que falta é que haja punições para quem não a cumpre.

Então, a partir do momento em que posso punir alguém que não cumpre uma regra no Brasil, por exemplo, alguém se abstenha de responder uma ordem judicial, que se bloqueie o serviço. Bloqueia-se o serviço e o suspende. Quanto essas empresas faturam aqui, no País? Elas faturam bilhões. É um dinheiro que fica no Brasil? Esse dinheiro não fica no Brasil. Eles vêm aqui, exploram o nosso dinheiro e não são capazes de nos fornecer informações? Informações que são de crime organizado, que tratam de exploração sexual infantil, que tratam de outros crimes relacionados, crimes de ódio.

Até manifesto no meu tom de indignação, porque fico revoltado com isso, porque sou brasileiro e eles têm que respeitar. Quando nós vamos ao exterior — eu fiz viagem até lá —, se você não se adequar à legislação deles, você vai sofrer uma punição automática.

Com relação a essa questão do WhatsApp, vocês imaginem num cenário nos Estados Unidos, onde dois terroristas possam se falar pelo WhatsApp sem serem interceptados. Alguém pensa nessa possibilidade? Isso existe? Talvez V.Exas. possam montar uma comitiva e diretamente eles possam falar isso para vocês.

Agora, a polícia, dizer assim que a polícia não tem condições de fazer alguma coisa, talvez falar que não tem é um termo muito forte, porque o tempo todo nós estamos tentando trabalhar nas brechas, trabalhar com outras técnicas. Não existe só investigação via WhatsApp. Essas pessoas falam pelo WhatsApp, mas elas têm condutas fora do telefone, fora do computador.

Então, não é só uma metodologia de investigação. As outras metodologias podem suprir, até porque a Lei nº 9.296 prevê que você tenha uma série de requisitos anteriores a fazer uma interceptação. O WhatsApp pode servir como um meio de comunicação, mas a conduta de fato deve ocorrer. Agora, para pornografia infantil fica difícil, porque o objeto pode ser trafegado pelo WhatsApp do começo ao fim. E se o provedor, o caso de detentor de direitos autorais, o Facebook, não

colaborar, fica muito mais difícil para nós, não impossível, mas muito mais difícil de driblarmos essa forma com que ele conduz.

Com relação ao anonimato, nós temos diversas técnicas para se trabalhar com anonimato. Então, vou dar a mesma resposta que eu dei para o Deputado Fábio Sousa. Essas duas operações que eu citei, para que V.Exas. possam estar pedindo um técnico, trabalham justamente com serviços que, em tese, seriam anônimos. Então, ali se pode ver um *modus operandi,* uma expertise da Polícia Federal, em driblar esse anonimato e chegar a esses delinquentes.

Bom, as perguntas do Deputado Nelson Marchezan Junior, que fala que na Constituição é vedado o anonimato, se existem documentos cadastrados. Não existem documentos a serem enviados para você ter um cadastro. Não existe mesmo. Isso é fato, todo mundo que usa, sabe. Para você criar uma conta no Facebook você não precisa mandar nenhum documento seu, nem uma cópia nem nada. Enfim, a resposta é, já estou sendo repetitivo: os acordos internacionais têm que ser cumpridos, temos que celebrar mais acordos onde não há, temos que ter uma instituição no meio que possa intermediar.

Eu não posso ter apenas a Polícia Federal como referência, por quê? Modéstia a parte, a Polícia Federal tem um nível alto com relação à investigação e tecnologias, mas, às vezes, existem outras instituições. O crime que seja mais investigado, talvez seja o crime de homicídio. Então, quando vou registrar uma ocorrência na delegacia de um crime que foi cometido no espaço cibernético, eu não sei qual é o grau de relevância que ele tem. Se eu não consigo investigar, por exemplo, um crime de homicídio que, acredito, seja o mais grave, como vou dar uma conotação maior a um crime cometido no espaço cibernético, quando se trata de estelionato na Internet*,* uma pornografia infantil que não seja entre brasileiros, alguma coisa assim e não vou dar atenção a esse crime? Acredito que seja nessa linha.

Então, para resolver isso, eu preciso de efetivo e capacitação.

Com relação à *deep web*, ela é uma Internet dentro da Internet. Qual a finalidade? Assim como a criptografia, a *deep web* não foi feita para fins ilícitos. Ela foi feita para quê? Para evitar censura. Existem países onde se tem censura na Internet. Então, através da *deep web*, eu consigo acessar como se eu estivesse em

outro país, e eu consigo ter acesso às informações. Ela foi concebida com essa finalidade. Ela é criptografada e você, entre aspas, "estaria anônimo". Esses dados dos quais eu falo dessas duas operações, nas nossas publicidades — a Polícia Federal dá as publicidades —, falam-se sobre essas operações. Por isso sei que a *darknet* foi feita na *deep web*.

Então, utilizou-se uma metodologia para se investigar dentro da *deep web*. Eu não vou falar dessa metodologia, porque, se não, eu vou ensinar para os próximos e, se conseguirem ter acesso, ou através de outro canal fechado, nós podemos conversar sobre isso, mas o anonimato não é garantido em plataforma nenhuma. Então, essa é a minha opinião e a minha visão.

Com relação às perguntas do Deputado Delegado Éder Mauro, que há apenas 20 policiais capacitados, se existe falta de investimento, de aparelhamento, as operadoras.

Vou falar sobre as operadoras aqui, porque as outras, acho que já respondi, que é cultural, em relação a uma ordem judicial. Acredito que o Deputado Delegado Éder Mauro estaria fazendo referência à Lei nº 12.830, que dá prerrogativa à autoridade policial de requisitar, sem uma autorização judicial, algum tipo de informação.

Bom,, talvez essa pergunta possa ser melhor respondida por uma autoridade policial, mas, enfim, eu acredito que hoje o operador de conexão está respondendo bem. Ele talvez tenha aquela dificuldade com relação ao que foi levantado aqui pelas procuradoras, com relação ao NAT, mas, enfim, esse NAT, que significa Network Address Translation, que seria um jeitinho para haver mais IPs no Brasil — pela falta de IPs —, pode ser contornado através... Eu estou fazendo uma investigação: eu tenho um número de IP, que é compartilhado com algumas pessoas. Dependendo do número de pessoas, eu consigo fazer diligências e sanar essa dificuldade. Agora, difícil se faz quando ocorre, por exemplo — como o Dr. Bruno citou —, quando um acesso é feito aqui, por dentro da Câmara, onde um IP é compartilhado com muitas pessoas. Essa dificuldade que existe no NAT já existe há muito tempo com relação a esse tipo de provedor.

E nós temos provedores a rádio. Por exemplo: na minha casa, o provedor é a rádio, porque eu não consigo uma porta de DSL na cidade onde eu moro. Então, o

IP que existe na minha casa é um IP que não é real, como a gente chama; não é um IP que está disponível para ser acessado diretamente da Internet.

Então, a gente já lida, no nosso cotidiano, com essa dificuldade, e, enfim, existem métodos para que a gente possa sanar essa dificuldade. A operadora, de acordo com o Marco Civil, não fala em... Eu não vi, em nenhum momento, ela falar em IP. Ela fala em registro das comunicações. Acho que eu tenho até o artigo aqui, porque eu já esperava que fosse perguntado isso. Seria o seguinte:

> *"O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos, deverá manter os respectivos registros de acesso a aplicações da internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento."*

Em nenhum momento aqui foi falado em IP, em porta de origem. Ou seja, a operadora tem que cumprir o que está na lei, entendeu? A lei foi concebida para identificar o usuário; a lei não foi concebida para armazenar o IP. Se é através do IP mais a porta de origem, ela tem que dar o jeito dela de individualizar essa comunicação; foi para isso que a lei foi criada.

Já pensaram se a gente tivesse que criar uma lei para cada tipo de delito especializado? Por exemplo: crime de dano. Eu venho aqui e quebro esta mesa: eu cometi um dano. Imagine se tivesse que haver dano à mesa, dano ao copo, dano ao computador! Então, é uma coisa que foge à minha inteligência o fato de que esse artigo seja interpretado de outra maneira.

Bom, passando aqui à outra pergunta do Deputado. Ele falou sobre estelionato. Estelionato é um dos líderes... Acho que talvez seja o líder entre os crimes cibernéticos. Enfim, os estelionatos ocorrem com as páginas geralmente oferecendo produtos ilícitos ou você fazendo uma compra através de um *site* e, na hora em que o produto chega, não era aquilo que lhe era oferecido. Então, enfim, é o estelionato. Ele deve ser tratado como é o estelionato convencional, só que a única diferença é que ele ocorre no espaço cibernético.

Ou seja, se existe quem está comprando... Eu tenho todos os atores: eu tenho quem está vendendo, quem está comprando. A investigação seria a mesma; a diferença seria que talvez eu tivesse que fazer alguns pedidos de quebra de sigilo ou dos dados cadastrais de quem está vendendo, e eu vou estar com a minha apuração em andamento.

Bom, com relação às ordens judiciais, se o WhatsApp entrega decifrado ou não decifrado, disso eu falei. O Facebook, o detentor de direitos, tem a obrigação de atender às nossas normas. Se ele entrega cifrado ou não entrega cifrado — as procuradoras aqui já falaram, entendeu? — Eu vou repetir as palavras dele: *"Eles querem entregar cifrados"*.

Agora, o conceito de interceptação, o conceito que a Lei nº 9.296... Você imagine se a lei fosse prevista para eu entregar uma coisa que não seja possível visualizar! Seria como interceptar um telefone e ter essas conversas criptografadas e enviar para você: *"Ó, pegue aí e veja o que você consegue fazer"*. Então, é isso que estão fazendo com a gente. Isso dificulta o nosso processo? Dificulta.

A Polícia Federal tem várias metodologias que contornam algumas criptografias, alguns tipos — não vou revelar aqui os métodos que ela utiliza. Mas, enfim, a legislação brasileira deve ser cumprida. O WhatsApp, o Facebook, todas as redes sociais devem responder de acordo com a nossa legislação. Se eles não estão cumprindo — os senhores aqui já têm ciência, não são só palavras minhas, são palavras de outros palestrantes que já passaram por aqui, inclusive membros do Ministério Público —, então, vocês têm que fazer valer. Eu acho que os senhores têm prerrogativa para isso e têm força para isso.

Bom, com relação às perguntas da Deputada Mariana: investigar a Deep Web e a Dark Web, eu acho que eu já respondi — pedir aquela cópia daquelas operações, o *modus operandi* vai estar lá, existem as técnicas e, daí, entre os senhores, o senso crítico vai ficar um pouco mais aguçado.

Com relação ao critério das imagens sobre a pornografia infantil, isso aí... Enfim, por mais que a gente queira colocar uma técnica numa foto, fica complicado. Mas, assim, há imagens... A gente classifica imagens que são categóricas. Exemplo: uma criança entre zero e cinco anos, entendeu? Eu vou responder a essa pergunta... Como a Deputada propôs aqui um caso que chamou a atenção — o que

chamou atenção, coisa aqui que você... Não tem como você não se lembrar de algo que acontece em ambiente familiar. Ainda bem que isso aí não aconteceu no Brasil. Não foi no Brasil, mas foi num dos legados das nossas operações. Eu pude avaliar um vídeo em que se falava em espanhol — eu sou fluente no idioma; então, eu sei muito bem o que estava sendo falado — em que, numa piscina, estavam tio, tia, filho... Tio, tia, pai e mãe dentro de uma piscina. Eu lembro até o nome do arquivo, para vocês terem ideia — e esse fato foi em 2009, para vocês terem uma ideia de como marcou —, o nome do arquivo se chamava Niños de Venezuela. Então, era um arquivo em que havia crianças de 3 a 5 anos, no máximo, dentro de uma piscina, onde elas praticavam sexo oral em todo mundo, e a menina que estava presente era estuprada por todos.

Então, enfim, são coisas que não são legais de ver, causam um transtorno, causam revolta. E quando eu vejo uma operadora ou um serviço de conteúdo negar uma informação que nos vai levar a prender um criminoso como esse, causa-me uma tremenda de uma sensação não só de insegurança, mas também de impotência, de total impotência.

Bom, com relação aos registros do NAT, eu já respondi. E quanto às salas secretas que foram exibidas, aquela sala secreta ali, existe na Superintendência Regional de Curitiba, e, aqui, no nosso Instituto Nacional de Criminalística, o Dr. Leonardo pode falar melhor sobre a infraestrutura. A infraestrutura da Superintendência Regional onde eu trabalho, em Rondônia, não tem aquela sala, mas tem um conjunto de equipamentos um pouco mais modesto, mas que alcança a finalidade das nossas demandas, o que não alcança, assim, a quantidade de pendências que a gente tem. Então, o fator tempo, para a gente, é preponderante.

Enfim, as respostas para a Deputada são essas. Eu acho que havia uma classificação aqui que eu pulei, que seria de zero a dez, que seria do Deputado Silas Freire. Essa classificação de zero a dez tem muitas variáveis que a gente tem que colocar para poder dar um dado preciso, que seja tempo. Por exemplo: se eu tiver 1 ano para trabalhar numa investigação, talvez ela suba para 10. Se eu tiver 1 dia, talvez ela seja zero. Talvez, se eu tiver 6 meses, ela suba para 9. Então, o fator tempo é extremamente preponderante para eu poder fazer uma resposta quanto a esse quesito.

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

Com a palavra o Dr. Leonardo Bueno de Melo, representando o INC.

O SR. LEONARDO BUENO DE MELO - Bom, eu vou tentar complementar, rapidamente, as respostas do Dr. André.

Em relação à Convenção de Budapeste, eu não tenho acompanhado a evolução do debate sobre essa convenção. Eu lembro que, no início, houve um esforço muito grande do Conselho da Europa para que fosse difundido pelos outros países. Num primeiro momento, a resistência do Brasil, que eu me lembre, foi por motivos diplomáticos. O MRE — Ministério das Relações Exteriores — alegou que não havia sido chamado para discutir os termos dessa convenção, e, desde então, eu lembro que houve algumas controvérsias sobre as adequações que o País deveria fazer ou se comprometer a fazer para poder aderir.

A minha opinião pessoal é a de que ela era extremamente benéfica na medida em que padroniza e estabelece algumas condições comuns entre os países de forma que a cooperação internacional, que é o fator chave na investigação dos crimes cibernéticos, seja otimizada com essa convenção.

A questão do uso de espiões disfarçados. A perícia, via de regra, não atua diretamente nesse tipo de atividade mesmo. Já existe a figura da infiltração, mas o que eu sei é que, nos Estados Unidos, nos treinamentos que tivemos, isso era uma tática bastante efetiva, pelo menos o que foi relatado, para a questão da pedofilia, no combate à pedofilia.

Eu sei que eles têm algumas restrições. Lá a prostituição é crime; então, eles têm também... usam técnicas semelhantes para combater a questão da prostituição, mas eles não podem abordar o cliente, eles têm que esperar o cliente ser abordado.

É mais ou menos da forma como eles fazem lá também; eles criam *nicknames* nesses fóruns, nesses *sites* de troca de material de pedofilia, sugestivos, dando a indicar que é uma menina de 5 anos, que é um garoto de 12 anos, e ficam aguardando que os pedófilos entrem em contato, que os abordem e proponham o envio de fotos ou um encontro presencial. E os relatos são de que são técnicas bastante efetivas.

Sobre o questionamento do Deputado Silas Freire, o grau de dificuldade para a investigação e elucidação completa de um crime cibernético varia muito. Existem

crimes que são cometidos por amadores, digamos assim, não tomam cuidados mínimos para tentar ocultar a origem das suas conexões, e são relativamente simples de serem obtidos, mas, no geral, eu considero que há um grau de dificuldade bastante alto pelos motivos que basicamente já discutimos aqui. A necessidade de cooperação internacional, que é inerente à maioria das investigações cibernéticas, porque muitos provedores do tráfico de dados passam por fora do País; a questão da volatilidade das provas, a necessidade de coleta e preservação rápida dessas provas, que se perdem rapidamente; o uso difundido de criptografia e pouca efetividade de métodos tradicionais de investigação. Há uma necessidade do uso, do desenvolvimento de novos métodos aos quais boa parte da polícia ainda não está completamente capacitada para fazer.

A questão da possibilidade de anonimato é uma discussão realmente bastante controversa. A nossa posição, eu falo a minha posição como policial, como perito criminal, tende a atrapalhar mais do que ajudar, mas reconhecemos a importância de mecanismos que garantam esse anonimato em situações de regimes de exceção para tráfico de informação, de informantes e jornalistas. São situações bastante específicas, mas que têm uma relevância muito grande, e é realmente difícil sabermos ponderar se vale a pena abrir uma exceção ou se é o caso de realmente vedar.

Foi perguntado se existem recursos necessários na Polícia Federal para o desenvolvimento das atividades. A resposta é sim e não. Isso em relação aos recursos financeiros. A Polícia Federal hoje, eu a considero bem equipada; nós temos equipamentos razoáveis; nós temos as ferramentas necessárias para atender à maior parte dos exames que precisamos fazer, mas, ao mesmo tempo, em vários campos da nossa atuação, em termos de recursos financeiros, o céu é o limite. Nós ficamos assustados quando vemos as cifras das agências policiais americanas.

Por exemplo, no caso de quebra de senhas, no Instituto Nacional de Criminalística existe um equipamento, um *cluster* que é utilizado para quebra de senhas. Dependendo do algoritmo, ele consegue realizar 300 mil tentativas por segundo. Se eu gastar mais 10 milhões, consigo um equipamento que vai multiplicar essa capacidade por mil. Isso não vai me dar nenhuma garantia de que vou conseguir quebrar a senha, mas, dentro dos procedimentos que a perícia utiliza para

fazer a quebra de senhas, pode nos fazer ganhar bastante tempo numa tentativa, porque o que fazemos basicamente é usar os recursos para a montagem e dicionário de dados e estabelecer um período de tentativa, porque, dependendo do algoritmo, vamos ficar milhares, milhões de anos, sem garantia de que vamos conseguir quebrar determinada senha. Recebemos as demandas e estabelecemos um prazo para quebrar aquela senha. Não conseguindo, abandonamos, simplesmente desistimos ou aguardamos, tentamos identificar uma vulnerabilidade que tenha surgido, alguma outra forma de acessar aqueles dados e partimos para o próximo. Então, a questão dos recursos financeiros é sempre importante.

Como eu comentei, eu participo, acompanho de perto a gestão de criminalística e posso dizer que nosso grande entrave hoje para a aquisição de equipamentos, de recursos é a burocracia do serviço público. Nós temos a Lei das Licitações, que estabelece uma série de mecanismos em parte justificáveis, pela necessidade de evitar desvios de recursos, mas que ao mesmo tempo cria uma quantidade inimaginável de peças processuais, certidões, documentos que precisamos providenciar. E no nosso caso de atuação — atuamos com tecnologia de ponta, temos que validar as ferramentas que surgem a cada dia, *softwares* que são lançados a que precisamos ter acesso rápido até para saber se funciona, muitas vezes é um *software* barato, um equipamento que não custa muito, mas só é vendido no exterior, não há nenhum representante no Brasil —, temos que iniciar um procedimento de compra internacional, e muitas vezes, até conseguir comprar esse equipamento, já saiu um modelo mais novo, já existe um concorrente que lançou um equipamento que faz coisa melhor. Então, nesse ponto, há um atraso muito grande na nossa capacidade de dispor dos recursos desejados para poder acompanhar a linha de frente do desenvolvimento.

E, nos crimes cibernéticos, mais do que em geral, eu acredito, essa questão é sempre uma briga de gato e rato. O Dr. Bruno comentou do iPhone 6s, que ninguém consegue quebrar. Foi lançado na semana passada. Ainda não recebemos nenhum iPhone 6s para periciar. Ele tem mecanismos bastante robustos de proteção, mas, ao mesmo tempo, nós temos as polícias do mundo inteiro interessadas em quebrar esses mecanismos, em acessar os dados que são protegidos pelo iPhone 6s. Nós temos empresas multimilionárias, com orçamentos multimilionários, com equipes de

desenvolvimento dedicadas a achar, encontrar e desenvolver métodos de burlar esses mecanismos para poder acessar os dados.

Então, fatalmente, daqui a algum tempo vai haver uma situação específica, algum modelo de versão do sistema operacional, alguma circunstância em que foi utilizado que vai permitir acessarmos. É sempre uma corrida muito grande. Os *hackers*, os criminosos tentam achar falhas, tentam achar brechas de segurança, e a Polícia corre atrás para tentar identificar, detectar e combater essas ações.

Com relação à questão da cessão de *logs* de acesso pelas operadoras, nossa visão é um pouco alinhada com a dos demais participantes das outras audiências aqui. São dados administrativos. Hoje todo policial tem acesso aos dados cadastrais, aos dados de um proprietário de carro. Isso não depende de autorização do DETRAN, muito menos de determinação judicial, e ele simplesmente... No caso dos registros de conexão, que acho o grande foco do debate, nada mais é do que dizer quem estava usando a Internet com aquele IP, naquele determinado horário. Não é, na minha opinião pelo menos, uma questão de invasão de privacidade.

Complementando a questão da caracterização de imagem de pornografia infantil, a perícia, por excelência, trabalha com critérios científicos. Nós trabalhamos com padrões, com referências a partir das quais possamos balizar nosso trabalho. Existem muito poucos critérios para se determinar a idade de uma pessoa numa foto, critérios científicos. Nós temos, dentro da Polícia Federal, uma quantidade extremamente reduzida. Mas nas Polícias Civis há um efetivo razoável de médicos legistas que estudam dimensões do rosto da pessoa, características de proporções do corpo da pessoa, para tentar estimar uma faixa de idade a partir daquilo ali. Fora disso, qualquer avaliação é subjetiva, por mais óbvio que seja ver uma criancinha na foto — *"Não isso, é uma criança, não tem 18 anos. Não tem como!"*. É uma avaliação que se constata ali: olha e vê que não há necessidade nenhuma de um perito para dizer isso.

Ou seja, a minha posição é que, em última instância, a não ser nesses casos restritos em que, por meio da determinação dos pontos de proporção da face ou do corpo seja possível determinar cientificamente se é uma criança ou não, essa análise vai caber ao investigador, ao agente, ao delegado que estava lá, ao promotor que vai oferecer a denúncia e, em última instância, ao juiz que vai olhar

aquilo ali e avaliar se é caso de criança, se não é. A perícia pode, obviamente, auxiliar se houver suspeita de que seja montagem, arquivo digital que tenha sido alterado, ou as circunstâncias em que aquela imagem foi transmitida, divulgada, publicada. Nós sabemos que existe essa diferenciação no Estatuto da Criança e do Adolescente.

Basicamente, era isso que eu gostaria de expor.

Obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigado, Dr. Leonardo de Melo.

Concedo a palavra ao Dr. Evandro Mário Lorens.

O SR. DEPUTADO JEAN WYLLYS - Sra. Presidenta, começou a Ordem do Dia e estão solicitando minha presença no plenário. Então, vou escutar a resposta do Dr. Evandro e sair.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Até mesmo para aproveitar que o Deputado Jean Wyllys ainda se encontra aqui, todos devem ter ido ao plenário devido ao início da Ordem do Dia, peço que sejam mais breves.

Teremos a resposta do Dr. Evandro e depois do Dr. Bruno Telles.

O SR. EVANDRO MÁRIO LORENS - Vou começar pela pergunta do Deputado Jean Wyllys sobre as câmeras instaladas. Na Polícia Federal nós basicamente tratamos de crimes contra entes federais. Então, a casuística de câmeras que não sejam ligadas a serviços federais para nós é zero. Só num caso de muita repercussão.

O SR. DEPUTADO JEAN WYLLYS - Não, mas eu perguntei a natureza, se os senhores tinham registro de crimes dessa natureza, inclusive sobre os entes federais, ou seja, invadir as câmeras para praticar outro ilícito, roubo de documentos, fórmulas.

O SR. EVANDRO MÁRIO LORENS - Isso. Eu vou chegar lá. Do ponto de vista de registro nosso formal, nós não temos; conhecimento de que houve, sempre ouvimos falar. Agora, registro formal que eu possa apresentar e dizer que formalmente aconteceu, pericialmente provado, eu não tenho. O que sabemos — é científico — é que é totalmente possível ser feito, isso de histórias de fora do País também, a questão dos bebês. Praticamente todos os enredos do *CSI: Cyber* são

baseados em fatos verídicos. Inclusive, essa era uma premissa do diretor, da equipe, para que os casos não caíssem numa situação fantasiosa e até de chacota do pessoal da área, dos especialistas. Então, eles se baseiam em casos reais. Inclusive, alguns dias antes daquele episódio, eu estava lendo sobre isso, apresentaram várias marcas de babás eletrônicas que eram vulneráveis a algum tipo de ataque. Em algumas semanas, logo no início do seriado nos Estados Unidos, eles lançaram esse episódio, eu fui procurar saber e realmente é um caso verídico. Mas não temos um registro de casuística formal que eu possa apresentar.

Uma questão interessante, em relação aos crimes de ódio eventualmente serem ligados a crime organizado...

O SR. DEPUTADO JEAN WYLLYS - De serem praticados organizadamente.

O SR. EVANDRO MÁRIO LORENS - Organizadamente. Tem que haver diferença. É exatamente o ponto que eu ia tocar. Na verdade, normalmente os crimes são realizados por interesse pessoal ou econômico. Não dá para dizer o que é mais pesado, mas sabemos que o crime organizado é muito mais ligado ao interesse econômico. Não é nem muito mais, é praticamente só ligado ao interesse econômico. Não tem razão um crime organizado tratar de questões pessoais e ideológicas, entidade de crime organizado do ponto de vista que a Polícia trata. Agora, a possibilidade de que exista uma organização social, vamos dizer assim, para praticar crime de ódio não pode ser descartada. Mas aí, volto: crime organizado do ponto de vista que tratamos está ligado geralmente a interesse econômico. Eu queria só deixar isso. É uma opinião pessoal também.

O SR. DEPUTADO JEAN WYLLYS - Uma boa opinião e um bom critério para discernir uma coisa da outra. Inclusive ajuda muito na resposta que eu queria, porque o interesse econômico pode estar difuso, não tão claro.

O SR. EVANDRO MÁRIO LORENS - Exatamente pode está envolvido com...

O SR. DEPUTADO JEAN WYLLYS - É. Ele pode estar difuso, na prática. Pode estar por trás do crime de ódio, muito subjacente, o interesse econômico.

O SR. EVANDRO MÁRIO LORENS - E isso, só uma observação, é muito difícil tratar do ponto de vista pericial, investigativo, mas não é impossível. Sempre costumamos dizer isso.

Com relação a anonimato, temos duas forças muito conflitantes: o anonimato como direito do cidadão e proteção aos direitos individuais e, do outro lado, o uso disso para acobertamento de crimes. Então, são dois lados que puxam. Do meu lado, como policial, a ponderação que faço é que o excesso de anonimato e liberdade vai gerar o paraíso para o exercício do crime. O controle excessivo gera efeitos colaterais terríveis, nossa história registra e nós sabemos muito bem do que se trata. Entretanto, como policial, do lado da segurança pública, olhando as questões de segurança — e não descarto outros pontos de vista, ângulos de visão diferentes, opiniões sociais —, minha opinião pessoal é que o anonimato deve estar debaixo da necessidade de segurança e que os efeitos colaterais, o mau uso das questões que são importante para a segurança, sejam tratados exatamente como mau uso, como desvio e como crime.

Então, o abuso cometido por uma autoridade... Usando um exemplo prático, em outros países, quando um policial está fazendo investigação, ele vai ao provedor e diz: *"Eu preciso dos dados de conexão dessa pessoa"* — aquele registro de conexão sobre o qual vai se falar daqui a pouco —, e o provedor é obrigado a entregar. Se o investigador está fazendo uso pessoal daquilo — *"eu quero saber o que a minha noiva está fazendo ou quero saber o que o meu rival ou meu vizinho chato está fazendo"* —, ele vai responder por isso, pelo desvio de conduta.

O SR. DEPUTADO JEAN WYLLYS - Em tese.

O SR. EVANDRO MÁRIO LORENS - Não. É o que vai acontecer se ele fizer o mau uso e isso ficar comprovado. Levantar a questão — e eu nem posso fazer isso — de que, por exemplo, as forças poderiam acobertar esse tipo de coisa... Não posso tratar nesse nível. Então, formalmente, ele vai responder por isso. É o ponto de vista que defendo, como profissional de segurança pública. Então, em respeito também à questão do *"em tese"*, de *"ah, não é bem assim".*

O SR. DEPUTADO JEAN WYLLYS - Não, é só para nós podermos complexificar a questão, sair do mundo ideal, porque as provas plantadas, as drogas colocadas no carro de pessoas inocentes...

O SR. EVANDRO MÁRIO LORENS - Sim.

O SR. DEPUTADO JEAN WYLLYS - ...não são abstrações. Elas existem.

O SR. EVANDRO MÁRIO LORENS - Existem. E é por isso que eu digo que desvio de conduta tem que ser tratado como desvio de conduta.

O SR. DEPUTADO JEAN WYLLYS - Claro.

O SR. EVANDRO MÁRIO LORENS - E nós só conseguimos resolver isso fortalecendo as instituições que têm que resolver isso: Justiça, órgãos da segurança pública e a própria sociedade, com uma coisa que eu vou colocar daqui a pouco, em razão de uma pergunta muito propícia que foi feita, porque eu acho que educação é fundamental. Essa questão sobre como eu vou resolver algumas questões eu vou colocar daqui a pouco. Então, como profissional de segurança pública, eu espero que V.Exa. entenda. É isso.

Voltando às perguntas iniciais do Deputado Fábio Sousa, quanto à Convenção de Budapeste eu corroboro o que foi dito aqui pelo Dr. Leonardo sobre o contexto em que essa Convenção foi concebida, quando alguns países interessados da Europa, depois de desenvolverem o texto, chamaram os países para aderir a ele. O Brasil se ressentiu muito de não ter participado dos debates e, principalmente, do fato de alguns pontos dessa Convenção conflitarem diretamente até com legislações internas. Mas o País não se mostrou disposto a trabalhar para mudar essas legislações, do ponto de vista técnico, por questões sociais internas, soberania interna. E, por outro lado, houve a questão diplomática também, pelo fato de o País não ter sido chamado. Então esse é o posicionamento, idêntico ao que o Dr. Leonardo tem.

E com esse gancho falo sobre uma das sugestões que eu tenho para a CPI: que ela estimule ou indique ao poder público responsável — no caso, o Governo Federal — que trabalhe na elaboração de acordos internacionais que atendam às nossas necessidades, porque só dizer que a Convenção de Budapeste é ruim, por isso não quer saber de acordo, é muito pouco.

O que atende ao Brasil? Foi colocada por vários colegas aqui a questão das empresas de outros países que têm má vontade em atender às nossas demandas. Então, vamos trabalhar em acordos, vamos sugerir ao poder público que faça isso. *"Ah, mas quem é que pode trabalhar nisso?"* Em nome da perícia federal, nós estamos à disposição para ajudar a construir esse texto, ajudar a construir ideias relacionadas a isso, porque nós somos os maiores atingidos. Quando a gente

recebe uma demanda, como a daquele assassinato que o Dr. André citou, e a resposta vem: *"Ah, não há elementos suficientes para te mandar um material"*, a gente tem que ter... A gente sabe exatamente onde dói. Então a gente está à disposição para trabalhar em conjunto. Em nome da perícia, eu nos coloco à disposição para que nós trabalhemos. Nós temos feito isso em várias legislações.

Eu sei que o tempo está curto, então, deixe-me acelerar.

Sobre a questão dos recursos, o Dr. Leonardo já falou.

Quanto à questão do zero a dez, a resposta é: depende. Depende, por exemplo, das condições de preservação dos vestígios. Se um Ministério é invadido, alguém vai lá e formata um servidor, a preservação é zero. O que sobrou para nós trabalharmos? Quase nada, não é? Se os vestígios são preservados, as condições de trabalho para analisar aquilo são boas, então as chances aumentam muito.

Com relação às perguntas do Deputado Nelson Marchezan Junior, sobre como se faz para nós tratarmos dessas questões de serviços que não exigem identificação, que não tratam disso aí, a minha opinião é que nós temos não só que olhar a parte técnica, mas olhar principalmente a nossa sociedade. Nós temos que trabalhar com educação digital.

O Reino Unido tem um programa hoje que atua praticamente em todos os níveis da sociedade para educação em segurança cibernética. Ele aplica programas de educação para toda a população. Estão acessíveis a toda a população programas de educação. O cidadão que faz aquele programa e vai demonstrando aptidão vai ganhando níveis de educação mais profundos, de forma que, nessa peneira, vai haver pessoas comuns que vão ter um nível de educação, vai haver pessoas com um pouco mais de conhecimento, que podem trabalhar como formadores de opinião, idealistas, e, lá no fim dessa cadeia, vão aparecer aquelas pessoas que têm talento para trabalhar no combate ao crime cibernético. Então, eles têm feito programas de educação muito sérios voltados para isso, com objetivos muito definidos.

A criminalização da *deep web* eu acho inviável — é opinião pessoal —, porque seria tentar legislar para um ambiente que não é controlado. E legislar para ambiente não controlado é inócuo, na minha opinião.

Quanto às perguntas da Deputada Mariana Carvalho sobre os métodos para investigar o submundo, nós usamos tudo que a tecnologia põe à disposição e todos os métodos sociais também — engenharia social, ferramentas, infiltração. Ou seja, tudo aquilo que estiver a mão para ser usado vai ser usado, óbvio, dentro da legalidade.

Critérios de imagem já foram considerados preciosamente aqui pelo Leonardo.

Operações de mais impacto. As mais recentes são as mais difíceis, porque são tratadas em níveis mais complexos. Então, a recomendação do Dr. André eu a refaço, para que se tenha acesso ao material.

A questão das salas também já foi respondida.

Se eu não respondi a alguma das perguntas, eu peço, por favor, que os senhores se manifestem para que eu possa responder. Devido ao adiantado da hora, vou passar para o próximo palestrante.

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

Com a palavra o Dr. Alessander Florindo.

O SR. ALESSANDER FLORINDO DA SILVA - Eu acredito que as perguntas já foram respondidas extensamente. Eu não tenho nada a acrescentar às respostas.

Eu gostaria apenas de fazer mais uma observação em relação ao fato de a gente estar em um momento interessante dentro da INTERPOL. Um colega perito criminal federal, atualmente, é Diretor Assistente de Pesquisa e Inovação do Complexo Global para Inovação da INTERPOL, localizado em Cingapura. Esse complexo é responsável justamente pelo combate a crimes cibernéticos e busca a troca de informações entre governos, via acordos internacionais. Então, eu deixo a sugestão, se houver interesse da Casa, de formar uma comissão, fazer uma visita, conhecer as instalações desse Complexo em Cingapura e ver o trabalho deles lá. Seria enriquecedor, eu acho, para os trabalhos desta CPI.

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

Com a palavra o Dr. Bruno Telles.

O SR. BRUNO TELLES - Cara Deputada, para encerrar — eu queria que o Deputado Jean estivesse aqui —, quero dizer que nós não estamos escolhendo

entre anonimato ou não. A pergunta essencial não é essa. A pergunta é: pode uma empresa oferecer um serviço não comercial aqui no Brasil, através da Internet, e se negar a cumprir ordens judiciais da nossa Justiça, quando um juiz já decidiu que aquele anonimato tem que ser quebrado?

Outra pergunta: pode uma empresa, situada em qualquer local do mundo, prestar um serviço comercial no Brasil e, além de não recolher os impostos aqui, como as empresas nacionais estão sujeitas a recolher, não se sujeitar a atender a uma decisão da Justiça brasileira? Será que isso é cabível? É o que acontece hoje. Eles respondem se quiserem e como bem entenderem. Eu duvido muito que eles respondam para a Justiça americana da mesma forma como respondem para nós. Lá, eles seriam presos bem rápido. O FBI está conseguindo controlar muito bem a navegação nos Estados Unidos e identificar a rede social ligada a essa parte, porque há uma colaboração muito forte com o Facebook e com o WhatsApp. Eles alegam que, como não estão sediados aqui no Brasil, não estão sujeitos à nossa legislação.

Então, a pergunta não é se nós vamos discutir o anonimato ou não. A pergunta é: podem essas empresas atuar em território nacional — e, se estão atuando pela Internet, estão chegando ao território nacional — e oferecer serviços sem se submeter à nossa legislação? Caso negativo, temos que bloquear o serviço, e o grande embate, quando se bloqueia um serviço, é que vem alguém lá do fundo e diz: *"Poxa, isso é censura!"*

Então, mais uma vez, não estamos dizendo que é censura nem que não é; é algo estritamente relativo à submissão à legislação brasileira. A pergunta é se ela pode atuar aqui sem se sujeitar às nossas leis, simplesmente isso.

Muito obrigado.

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

Quero agradecer, mais uma vez, a presença e a participação de todos: Dr. Evandro, Dr. Leonardo, Dr. Alessander, Dr. André, Dr. Bruno. Foi de extrema importância a participação de vocês aqui, até porque vocês conhecem, na prática, como funciona, já que participam de várias investigações.

Fiz a anotação das sugestões dadas pelos senhores e, sem dúvida alguma, vamos apresentar requerimentos relativos a elas nesta CPI.

Reitero o pedido de que mandem sugestões à nossa CPI. Fizemos até requerimento de solicitação ao próprio Instituto Nacional de Criminalística para ter acompanhamento de vocês aqui mais de perto. Isso é importante para o andamento dos trabalhos e o bom resultado desta CPI.

Como disse o Deputado Silas Freire, neste primeiro momento, estamos convidando instituições e órgãos relacionados ao tema para explicarem um pouco melhor como se dá o crime cibernético, o que acontece, e qual a realidade disso no Brasil.

Agradeço, mais uma vez, a participação de cada um de vocês, que foi de extrema importância.

Nada mais havendo a tratar, vou encerrar a presente reunião, antes convocando reunião ordinária para a próxima quinta-feira, dia 17 de setembro, às 9h30min, com pauta a ser publicada na página da Comissão e encaminhada aos *e-mails* institucionais dos gabinetes e Lideranças.

Está encerrada a presente reunião.