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: 2489/15**	**DATA: 19/11/2015**	
LOCAL: Plenário 4 das Comissões	**INÍCIO: 10h56min**	**TÉRMINO: 13h08min**	**PÁGINAS: 51**

DEPOENTE/CONVIDADO - QUALIFICAÇÃO
FERNANDO MERCÊS - Pesquisador de ameaças da empresa Trend Micro Incorporated. **FABRÍCIO RABELO PATURY - Promotor de Justiça e Coordenador do Núcleo de Combate aos Crimes Cibernéticos — NUCCIBER do Ministério Público do Estado da Bahia.** **MAYANA REZENDE - Delegada da Polícia Civil e Chefe do Grupo de Repressão a Estelionato e Outras Fraudes da Delegacia Estadual de Investigações Criminais — DEIC de Goiânia, Estado de Goiás.** **SÍLVIO KIST HUPPES - Delegado Titular da Delegacia de Policiamento do Interior — DPI do Município de Encantado, Estado do Rio Grande do Sul.**

SUMÁRIO
Debate acerca de reportagem exibida no Programa *Profissão Repórter*, da Rede Globo, sobre crimes cometidos pela Internet.

OBSERVAÇÕES
Há expressão ininteligível. **Houve exibição de imagens.** **Houve exibição de vídeo.**

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

Declaro aberta a 32ª Reunião Ordinária da Comissão Parlamentar de Inquérito que investiga a prática de crimes cibernéticos.

Comunico que a Comissão recebeu as seguintes correspondências: Ofício nº 1.507, de 2015, do Procurador-Geral da República, Rodrigo Janot Monteiro de Barros, informando não ser possível atender à solicitação da CPI para compartilhamento das informações referentes à apuração sobre a publicidade digital promovida pelo Governo Federal nos últimos 10 anos, cujo pedido decorreu da aprovação do Requerimento nº 87, de 2015; mensagem de *e-mail* na qual o Sr. Jeferson Monteiro encaminha respostas às indagações feitas em reunião pelo ilustre Deputado Sandro Alex, relacionadas ao convite da Presidente da República para comparecer à posse da Presidenta Dilma Rousseff; declaração da atriz Taís Bianca Gama de Araújo, comunicando a impossibilidade de colaborar com a CPI em razão de compromissos profissionais.

Quero lamentar a ausência de mais um artista, uma pessoa pública muito querida e admirada, que possui grande influência junto ao público e que poderia mostrar a sua indignação contra essa prática de se publicar *posts* e comentários difamatórios na Internet de forma impensada e irresponsável.

A CPI se colocou à disposição da atriz Taís Araújo. Nós estamos na Semana da Consciência Negra. O dia será comemorado amanhã, dia 20 de novembro, e seria mais uma oportunidade para se combater o racismo existente em nosso País.

A CPI também recebeu ofício do Bloco/PP/PTB/PSC/PHS, subscrito pelo nobre Líder Eduardo da Fonte, indicando o Sr. Deputado Paulo Henrique Lustosa para integrar a Comissão na condição de suplente.

Os documentos encontram-se disponíveis na Secretaria.

Ordem do Dia.

Audiência pública.

A reunião de hoje prevê a realização de audiência pública com os entrevistados no programa *Profissão Repórter*, da Rede Globo, que relatou casos de crimes cibernéticos que estão sendo praticados no País.

O Requerimento nº 94, de 2015, é de autoria do Deputado Rodrigo Martins, Sub-Relator da área de segurança na rede.

O programa *Profissão Repórter* foi exibido no último dia 29 de setembro e relatou a apuração de crimes virtuais cometidos nos Estados da Bahia, Goiás e Rio Grande do Sul. Na Bahia, o tema foi a respeito de *posts* difamatórios e de intolerância e ódio.

Convido para compor a Mesa o Sr. Fabrício Rabelo Patury, Promotor de Justiça do Núcleo de Crimes Cibernéticos — NUCCIBER do Ministério Público do Estado da Bahia.

O SR. DEPUTADO SILAS FREIRE - Sra. Presidenta, enquanto o convidado se posiciona...

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

O SR. DEPUTADO SILAS FREIRE - Primeiro, eu quero pedir a V.Exa... Sei que não será deliberado hoje...

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Devido ao início da Ordem do Dia.

O SR. DEPUTADO SILAS FREIRE - o requerimento... Eu fiz dois requerimentos em relação a preconceitos praticados contra o meu Estado. Um, pedindo providências à Polícia Federal para identificar quem cometeu o crime de preconceito contra o Estado do Piauí, para que possamos tomar as providências judiciais; e o outro, ao Portal G1, solicitando que nos explicasse por que a permanência de tamanhas ofensas por bom tempo. O Portal G1 já nos procurou, oferecendo-nos todas as informações. Isso nos deu por convencidos. Então, eu queria retirar o requerimento que pede ao Portal G1 explicações, mas permanecendo o requerimento pedindo providências à Polícia Federal, até porque o Portal G1 vai colaborar na identificação dos culpados.

Para complementar a informação, eu devo dar entrada nesta CPI em requerimento de nossa autoria, para que seja submetido à deliberação da Comissão Parlamentar pedido de realização de um fórum de debates, de apenas 2 dias — é importante para a nossa CPI, é um trabalho da minha assessoria e da assessoria do Partido da República —, que irá tratar da defesa da segurança nacional. Como estamos passando — e depois eu vou detalhar — por ameaças terroristas no mundo inteiro, nós precisamos, nesta CPI, ter certeza de que o nosso País tem algum tipo de segurança cibernética.

Eu acredito que no momento correto V.Exa. colocará esse requerimento para deliberação.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Sem dúvida. Fica o registro. Na semana que vem estará na pauta da Ordem do Dia também esse requerimento.

Convido também a Sra. Mayana Rezende, Delegada do Grupo de Repressão a Estelionato da Delegacia Estadual de Investigações Criminais, de Goiânia.

Gostaria de convidar para tomar assento à mesa o Sr. Silvio Kist Huppes, Delegado de Polícia, Titular da Delegacia de Policiamento do Interior — DPI 19ª RP, na cidade de Encantado, Rio Grande do Sul, e também o Sr. Fernando Mercês, analista em segurança da informação.

Estipulamos a cada um dos nossos convidados o prazo de 20 minutos para a sua apresentação, tempo que acreditamos ser o necessário.

Primeiro, concedo a palavra ao Sr. Fernando Mercês.

O SR. FERNANDO MERCÊS - Bom dia a todos.

Meu nome é Fernando Mercês. Eu fui convidado — estou muito honrado por estar aqui nesta CPI — por conta de um trabalho que fazemos de investigação de *cybercrimes* em uma empresa privada, mas temos colaboração de agências de polícia em todo o mundo.

Hoje, gostaria de explicar, aqui, para V.Exas. o que fazemos, como fazemos e como podemos trazer isso para o Brasil. Eu digo trazer porque já iniciamos esse trabalho, mas ainda não tivemos oportunidade de colher frutos, de ver isso funcionando aqui, por conta de uma série de motivos. Talvez consigamos nesta CPI desmistificar alguns desses motivos.

(Segue-se exibição de imagens.)

O departamento de pesquisa da nossa companhia tem três missões, sendo que uma delas é interessante para esta CPI, que é a investigação de *cybercrimes*. Enquanto empresa privada e fornecedora de *softwares* de segurança, enfim, e de uma série de coisas que não vêm ao caso, nós temos acesso a uma série de ataques que acontecem em todos os países onde temos clientes. E o Brasil não é diferente.

Nós temos uma facilidade razoável — não vou dizer que é muito fácil — de identificar ataques quando eles estão começando e, em muitos casos, chegar às pessoas que estão por trás desse ataque. É uma possibilidade de colaboração bem interessante.

É importante deixar claro que nada disso é vendido. E há uma colaboração da polícia em todos os países onde atuamos. Enfim, é por cidadania mesmo, nada disso envolve dinheiro.

Nós monitoramos o que chamamos de *underground,* ou seja, o submundo. Estamos inseridos nos meios de comunicação possíveis de que os *cybercriminosos* se utilizam para se comunicar uns com os outros, de modo que podemos estudar como funcionam e como eles se organizam. Publicamos inclusive relatórios anuais sobre como eles estão planejando e executando seus ataques.

Então, é uma coleta de inteligência que, sem dúvida, faz bastante sentido. Quando ocorre um *cybercrime*, por exemplo, a polícia ou quem estiver investigando, um ministério ou qualquer agência da lei, tem acesso a um *e-mail*, a um nome, a um IP, a um endereço que identifica alguém na rede. Com isso, nós conseguimos ajudá-los, justamente por conta de toda essa monitoração. Nós mantemos isso tudo. É um histórico muito poderoso. É um histórico que pode dizer, por exemplo, que um *e-mail* já foi visto numa atuação suspeita.

Nós não investigamos somente crime, mas qualquer tipo de ameaça, se a lei a definiu como crime ou não, se a vítima reclamou ou não e se isso chegou aos ouvidos da lei. Às vezes a vítima nem sabe que foi infectada, que sofreu algum dano de imediato, então ela nem chega a levar isso a um caso criminal; ou sofreu uma tentativa de ataque e de fato o dano não ocorreu ainda. Mas nós sabemos. Então, nós temos como correlacionar esses dados, em busca de entender os ataques, se estão partindo daqui, se estão partindo de outro país, se é de atuação nossa.

Há várias contribuições para que essa inteligência exista. Uma das principais coisas é que nós trabalhamos de forma dividida no mundo. Temos pesquisadores — é como nos intitulamos —, os que fazemos as pesquisas em ameaças, em praticamente todos os continentes. Essa inteligência é compartilhada.

Por que isso é interessante, se estamos falando de crime brasileiro? A Internet é muito diferente do ambiente físico tradicional na questão de se cometer o

crime — e talvez em todas as outras. Para lesar uma vítima aqui no Brasil, um indivíduo pode utilizar-se de uma infraestrutura que envolve dois ou três países a mais, o que dificulta muito o trabalho das polícias para obter colaboração de todo o mundo, às vezes de países que não estão dispostos a colaborar.

A existência de pesquisadores, de pessoas envolvidas fazendo a mesma pesquisa no *underground*, no submundo, monitorando as ações dos cybercriminosos, no maior número de pontos possíveis, colabora conosco, é muito útil para nós na hora de entendermos um ataque que está acontecendo aqui, mesmo que seja um ataque de uma capital brasileira a outra ou de uma cidade periférica a outra. É muito comum que, justamente para dificultar as ações da lei, cybercriminosos aluguem, trabalhem com infraestrutura fora do País. Isso dificulta bastante, se não trabalhamos assim.

Ainda na questão de *cybercrime*, nós temos colaborações de sucesso com Interpol, Europol, FBI, Polícia Montada Real do Canadá. Já efetuamos investigações em conjunto que resultaram em condenações, em prisões, principalmente com Interpol e FBI. Estamos aqui para fornecer dados, para que isso possa acontecer no Brasil também. Temos tentado há algum tempo, mas até agora não conseguimos com sucesso essa entrega, por uma série de problemas, como a legislação, talvez, mais branda que em outros países.

Há também certa resistência na questão do entendimento desses tipos de crimes. Crimes que são feitos fora da Internet com o mesmo intuito muitas vezes têm uma pena muito maior do que quando são cometidos na Internet. Isso acaba fazendo com que os recursos depositados para esse tipo de investigação do *cybercrime*, que é muito sério, não sejam suficientes e nós acabemos não tendo sucesso nessas investigações. Nós chegamos às pessoas que os fizeram, e essas pessoas continuam soltas e cometendo esses crimes.

No momento em que estou falando aos senhores, eu tenho certeza de que há uma série de pessoas pensando em novos métodos de como burlar o sistema de segurança que nós temos hoje. Existem fóruns, só para dar um exemplo, com mais de 100 mil usuários ativos, todos interessados em *cybercrime* São fóruns na Internet especializados somente em *cybercrime*, com mais de 100 mil usuários brasileiros e alguns estrangeiros. Então, não existe outro motivo para a pessoa estar cadastrada

naquele fórum, a não ser para cometer crime. Então, muita gente está pensando e praticando esse tipo de crime, mesmo que nem todos os casos cheguem ao nosso conhecimento.

Ainda com relação a investigações, eu vou falar basicamente sobre uma, a primeira das quatro que eu coloquei aqui. Ela aconteceu no Brasil e foi sobre o primeiro vírus criado para computador que infectava terminais de pontos de venda de lojas, como cafeterias ou qualquer tipo de loja onde o cliente pudesse passar um cartão de crédito naquela maquineta que é conectada a um computador.

O grupo que estava por trás desse crime criou um vírus de computador que só infectava esses computadores no Brasil, somente esses. Para quê? Para coletar os números de cartões de crédito dos clientes e enviar-lhe tais números e todos os dados, como a data de nascimento do cliente, o código de verificação do cartão, enfim, tudo o que é possível encontrar num cartão de crédito, seja com *chip* ou com tarja. Era um tipo de vírus muito sofisticado e com uma especialização muito grande, que, honestamente, ainda não tínhamos visto no Brasil.

Isso aconteceu em abril deste ano. Esse grupo desenvolveu o vírus e infectou mais de cem terminais em todo o País. Os senhores imaginem quantas transações de cartão de crédito acontecem em cada computador de um terminal de ponto de venda por dia. E esse crime durou meses. Pelo nosso cálculo, que publicamos no *site*, em apenas 1 mês de operação ou talvez um pouco mais, esse grupo obteve 20 mil números de cartões de crédito válidos, novos, recentes, com saldo e tudo.

Eu comento esse caso só para que se tenha uma ideia do potencial de dano desse crime, do dano que pode gerar esse tipo de crime, que é praticado sem que os criminosos saiam de casa ou da cadeira, apenas utilizando um computador. E 80%, da infraestrutura que eles empregam está fora do País, enquanto que as vítimas estão aqui.

Portanto, é um desafio real. Não é fácil nem para nós, nem para a polícia, nem para os envolvidos investigar isso, porque é um cenário novo, um cenário onde o sujeito não se exibe, está atrás de um nome ou de um apelido e consegue um poder de fogo muito grande, como o deste caso e de outros que eu poderia mostrar aqui. Nós vemos isso todos os dias, com prejuízos de milhares e milhões de reais a

empresas. Alguns casos são privados, não vêm a público por conta da empresa. Enfim, é um contexto muito amplo.

Como eu disse, nós temos interesse em colaboração. Justamente por isso, muita coisa que publicamos e desenvolvemos, nós colocamos numa comunidade. Há uma comunidade de segurança, há uma série, eu diria, dos chamados *hackers* do bem — com o perdão do termo —, há uma série de pessoas. Cada empresa privada tem um grupo de pessoas que trabalham para protegê-la, e essas pessoas trocam informações numa comunidade.

Existem eventos de segurança onde estão presentes governo, exército, polícia, comunidades de segurança, pessoas interessadas em proteger sua infraestrutura, bancos, que são muito atacados. E nós estamos presentes nisso.

Deixo aqui um convite aos senhores e a todos os interessados em entender como isso funciona, porque o *cybercrime* hoje está organizado. Nesses fóruns brasileiros, há pessoas estrangeiras, assim como já encontramos *posts*, ou seja, mensagens de brasileiros em fóruns russos de *cybercrime*. Um desses brasileiros não falava russo, comunicava-se muito mal até, mas, utilizando um tradutor, conseguia fazer negócios, conseguia trocar informação com *cyber*-criminosos na Rússia. Ou seja, de novo, sem sair de casa, ele conseguiu uma colaboração, talvez, inédita.

Hoje na América Latina, também há uma colaboração muito grande até pela facilidade do idioma. Mas, enquanto eles se organizam juntos, nós muitas vezes caminhamos para o individualismo, com uma investigação aqui e outra ali; *"Alguém atacou a minha empresa aqui, então, eu vou cuidar desse caso aqui isoladamente".* E o poder de quem está trabalhando junto é muito, muito maior.

Por isso, eu diria que hoje nós estamos atrás na luta contra o *cybercrime*. Eles começaram mais cedo e, como as nossas leis ainda estão um pouco brandas, têm uma certa motivação, uma certa segurança de impunidade. Tanto é que, em países onde o *cybercrime* é tradição, como China e Rússia, existe uma série de *softwares* que eles utilizam para se comunicar e evitar os olhos da lei.

No Brasil, eu diria que pelo menos 60% da comunicação *cyber*-criminosa é feita por redes sociais tradicionais, inclusive com fotos do que eles conseguem e tudo o mais. A mensagem que fica é de que eles não estão temendo a lei

justamente por uma série de falhas que têm encontrado, que utilizam para cometer seus crimes.

Mas nós estamos dispostos a mudar isso. Faço aqui o convite para conversas futuras, para que possamos ajudar a de fato reduzir esse índice que, infelizmente, só tende a crescer caso nós não nos preocupemos com ele.

Agora eu posso abrir para as perguntas?

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Na verdade, Sr. Fernando, nós vamos ouvir todos e depois abriremos para as perguntas.

O SR. FERNANDO MERCÊS - Tudo bem. Obrigado.

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

Eu concedo a palavra ao Sr. Fabrício Rabelo Patury, Promotor do Núcleo de Combate aos Crimes Cibernéticos — NUCCIBER, do Estado da Bahia.

O SR. FABRÍCIO RABELO PATURY - Primeiramente eu queria cumprimentar todos da Mesa na pessoa da Deputada Mariana Carvalho, os nobres Deputados aqui presentes e demais participantes.

Eu queria, antes de mais nada, apresentar-me: eu sou Fabrício Patury, Coordenador do Núcleo Especializado de Combate aos Crimes Cibernéticos do Estado da Bahia.

(Segue-se exibição de imagens.)

O Núcleo nasceu em 2011, a partir da visualização do então Procurador-Geral da necessidade de um combate mais próximo a esse tipo de crime. Porém, nesses 4 anos de nossa existência, nós mudamos um pouco — já são três atos — até pelo aprendizado. E nesse intervalo de aprendizado de crimes cibernéticos, nós nos dividimos em duas frentes. A primeira, na qual nós nos encontramos sempre por necessidade, de apoiamento ao colega final.

Estamos evitando a concentração num núcleo só. Na verdade, nós combatemos os grandes crimes cibernéticos, enquanto os crimes tradicionais, chamados crimes cibernéticos impróprios, ficam na mão dos promotores naturais, até porque, hoje, homicídios e estupros são cometidos pela Internet. Então, nós verificamos que seria impossível concentrar esses crimes comuns em um único núcleo, para efetuar esse combate.

Inclusive, hoje até lutamos com as delegacias especializadas, para que não concentrem tais crimes, já que a tendência a curto e médio prazo é de que praticamente todos os crimes, de alguma forma, no seu *iter criminis,* tenham um ato executório com viés cibernético. Inclusive os tráficos de drogas e homicídios são regulados e até mesmo tratados através de redes sociais ou mensageiros eletrônicos. Então, nós fizemos essa divisão. E hoje estamos apostando em outra seara, no NUCCIBER, que nós consideramos como prevenção. Nosso *site* está aí. Nós fazemos não só o apoiamento como recebemos as denúncias e investimos muito na parte da prevenção. A nossa experiência nos alertou que os crimes cibernéticos, uma vez preparadas as vítimas, uma vez preparadas as pessoas, é o único crime em que a capacitação consegue praticamente zerar a possibilidade de a pessoa ser uma vítima pelo menos dos crimes de opção, dos crimes de *phishing*, de estelionato, ou qualquer outro. Se as vítimas estivessem preparadas, se elas soubessem se capacitar, evitariam postagens indevidas, evitariam a exposição indevida, podendo ser menos vítimas.

Nós, atualmente, estamos investindo muito na capacitação em escolas de ensino médio e de ensino fundamental, pegando uma nova geração, que trata das ferramentas, mas, equivocadamente, estamos escutando que essa geração sabe muito de Internet. Ela sabe muito do uso da ferramenta, mas ainda não tem — como qualquer criança de 9 anos, 10 anos, 11 anos — o discernimento necessário para se portar em qualquer caminho. Isso nunca mudará. Não há como se considerar, como dizem, *smartphones*, *tablets*, *smartwatches* na mão de crianças e adolescentes, que ainda não têm o devido preparo para esse mundo. Serão vítimas em potencial.

Estamos também sempre preparados para atuar nos crimes contra a honra, contra o *sexting*. Estamos investindo muito.

Aqui há exemplos de várias escolas às quais estamos levando a preparação e a capacitação. Aqui também estamos levando nossa capacitação às mulheres, vítimas preferenciais dos crimes contra a honra. Os crimes de feminicídio estão aflorando. Já temos feminicídios e homicídios provenientes de tratativas em Internet, através de uma revanche pornô.

Então, como vítimas preferenciais estão os idosos, as mulheres e as próprias faculdades em *cyberbullyings.* Esse está sendo o nosso segundo foco. Somos um

núcleo tanto de repressão e de capacitação dos colegas para fazer repressão, como também, prioristicamente, acreditamos na prevenção, na capacitação e na orientação. É um crime em que a prevenção é a chave. Quem estiver capacitado, consegue se livrar desses crimes.

Aqui também mostramos a nossa capacitação a promotores, a juízes, a defensores, investindo no conhecimento. Temos aqui entidades e governos, como o da Bahia, que temos orientado. Há também outros governos que orientamos e pessoas de fora. Acreditamos que este norte não pode nunca ser sobrelevado, precisamos levar as capacitações.

Aqui, por exemplo, foi uma forma de mídia que levamos às ruas de Salvador, em que colocamos um carro de vidro, mostrando atores encenando seu dia a dia e dizendo: "Vocês estão agindo assim na Internet!" A mídia chocou bastante. Houve repercussão, e as pessoas passaram a entender que essas postagens do tipo *Eu estou bem*, meu *Checklist*, o *Check-in*, *onde eu estou*, *hoje eu estou sorrindo*, *hoje eu estou alegre*, na verdade, se todos lessem os termos de uso do *Facebook* saberiam que nós estamos sendo usados como cobaias e todos esses dados são repassados e vendidos. Ou seja, o que você externa vira regra, vira negócio, vira bilhões, para quem usa, e nós pouco sabemos e pouco utilizamos esse dado. Esperamos que avance a legislação de proteção de dados no Brasil. Isto está nas mãos dos senhores.

Aqui, algumas ferramentas que nós usamos, o *face cards*. Tentamos falar a linguagem da atualidade e colocar pelas redes o seguinte: WhatsApp, Telegram, ICQ, Facebook, passando algumas gotas de conhecimento para tentar dar uma publicidade massiva à preparação e à prevenção.

Aqui são cartilhas que rodaram nos ônibus de Salvador. Nós colocamos a seguinte chamada: “Vendo, tratar com Paulo, casado com Ana, trabalho na Hotline, pai de Antônio, só me ligue às 21h porque à noite chego cansado.” As pessoas estão agindo assim na Internet. Vários casos de sequestro foram obtidos com dados obtidos em *Facebook*. Até a questão de Ilhota, que chamou a atenção há pouco tempo, baseou-se nesses dados. Insisto: é preciso levar, sim, como ponto crucial a prevenção. Capacitação e prevenção são importantíssimas.

Aqui, alguns estudos com a Universidade Federal da Bahia, em que, após as palestras de prevenção, houve uma queda significativa nas escolas. Depois, tende a voltar a subir. Mas sempre quando volta, volta no mínimo 30 a 40% a menos os crimes que acontecem no dia a dia. Isso significa que até nas escolas que visitamos duas vezes obtivemos resultado. Então, a prevenção é, sim, fator de enxugamento dos crimes posteriores. Esse investimento, cada vez mais, tem que ser maciçamente feito.

Por que nós acreditamos nisso, senhores? Porque nós vivemos em outra sociedade. Agora, neste momento, nós todos, quando podemos, estamos mandando *e-mails,* WhatsApp*,* mensagens. Por quê? Porque esta é a nossa sociedade. Não vamos voltar atrás. Pelo contrário, vamos aprofundar.

Esta imagem é bastante elucidativa e mostra o seguinte: em 2005, a posse do Papa Bento XVI foi assim. Em 2013, em menos de 8 anos, foi assim. As pessoas não olham mais pelos seus olhos. As pessoas olham nas telas. Esta é a nossa sociedade. Esta foto apareceu recentemente como viral. Todos acompanhavam aqui o que estava sendo passado pelas ruas, somente aquela senhora via pelos seus próprios olhos, porque ela veio de uma geração que ainda acreditava que ver pelos olhos era melhor.

Eu gostaria muito de voltar atrás porque também acho que ver pelos olhos é melhor, mas, infelizmente, hoje não temos como voltar atrás em uma sociedade que mudou. Sua cultura mudou. Como a própria cultura mudou, hoje até mesmo nos currículos se coloca isso: nós pegamos esse currículo em que a pessoa afirma que administra 23 grupos de WhatsApp. Eu achei estranho e perguntei ao pessoal do RH: *"Mas isto é realmente relevante?"* Eles me disseram: *"Se você pensar bem, significa que é uma pessoa articulada, que tem condições..."* Eu pensei: "Rapaz, para mim era um vaga...", mas deixa para lá. Enfim, fale e está contando, porque a nossa sociedade mudou. Nós precisamos acompanhar isso.

Mas a pergunta que sempre nos chega é: será que toda sociedade realmente está sendo incluída? Será que toda sociedade, Deputados, é como a que nós estamos vendo aqui? Falando em WhatsApp, resolvendo uma situação?

Fui Promotor no interior durante 11 anos. Como estadual todos sabem que nossa carreira começa nas pequenas comarcas até irmos crescendo de entrância até chegarmos às finais.

Aqui eu coloquei um videozinho, feito no interior, que bem repercute o que é, no interior, o conhecimento de Internet. O que me preocupa antes de passar este vídeo? Quando eu estava no interior, o projeto de levar Internet barata, da Intelbrás, a 15 reais, estava colocando as pessoas massivamente na Internet, fazendo a inclusão digital sem educação digital. Isso significa que nós estamos colocando uma massa enorme de vítimas potenciais para serem manipuladas. Está aqui o exemplo claro, acho que os senhores vão entender o recado.

(Exibição de vídeo.)

O SR. FABRÍCIO RABELO PATURY - Pois é, senhores, Twitter virou droga, dança, maconha, tudo.

Mas essas pessoas estão usando a Internet e são vítimas em potencial de golpes simples, de golpes de estelionato, mas, se estivessem um pouco preparadas, elas estariam evitando que isso acontecesse. Por isso insistimos que a prevenção é a chave.

Saindo da parte da prevenção, eu evitaria até falar de crime cibernético. Não trouxe esse item, Excelência, porque a CPI já está trabalhando há bastante tempo. Todos já sabem aqui que o crime cibernético é próprio e impróprio. Os crimes cibernéticos impróprios seriam os crimes comuns, já previstos em legislação penal e legislação penal extravagante, em que, no *iter criminis*, em um dos atos executórios está o viés cibernético. Os crimes próprios são aqueles que atuam contra a máquina, contra os sistemas informáticos e assim por diante.

Pela nossa experiência, e é o que nos atinge efetivamente, para que haja uma atuação nos crimes cibernéticos é necessário um tripé: nós precisamos de prevenção, de normatização adequada e de procedimento célere. A pergunta que fazemos é: temos normatização adequada? Aí está a questão.

Por exemplo, hoje todos sabem que de cada 100 reais furtados de banco, 95 reais foram pela Internet. Vejam: os crimes de roubo a banco ou com explosão de caixas eletrônicos, mazelas em nossos interiores, ou aqueles cometidos com mão armada respondem por 5%. Por que os bancos não estão nem aí para o interior e

para as mazelas sociais, se acontecem as explosões? Porque 95% do prejuízo deles não está lá. O prejuízo está na Internet. Só que há um detalhe: eles investem, nos ajudam, colaboram, mas, vejam só, quando nós tentamos colocar o crime contra roubo, o crime de furto bancário como furto pelo menos qualificado por destreza, que seria uma das qualificadoras do tipo penal, todos os tribunais derrubam nossa tese e consideram furto simples. Enquanto o furto "punga", ou seja, a simples retirada de uma carteira sem a pessoa sentir, é considerado destreza — nós estamos dizendo que furtar uma carteira sem que a pessoa sinta — e a pena é de 2 a 8 anos, o furto simples pela Internet, crime extremamente pernicioso, que força os bancos a não investirem, a pena é de 1 a 4 anos, e nós não conseguimos reverter isso no Judiciário. Da mesma forma, o crime de estelionato simples, o bom e velho crime do golpe de loteria, que praticamente mais ninguém cai, mas muitos já caíram, tem a mesma pena do crime de *site* falso, aquele que pega indivíduos de boa-fé, que pouco conhecem a Internet e levam o golpe. Legislativamente, há um descompasso. O princípio da proporcionalidade dos valores contrastantes não está sendo respeitado. E isso incentiva quem usa, porque o custo benefício é de quem comete o crime — da mesma forma a pornografia de revanche.

Sei que aqui está sendo discutida a legislação, mas a pornografia de revanche virou um problema sério, porque, como consequência, já houve vários suicídios. Tratar a pornografia de revanche como uma injúria simples, tratar a pornografia de revanche com, no máximo, a Lei Maria da Penha como suporte não é suficiente, porque as repercussões são infinitamente superiores ao que o ilícito prevê. Trouxe aqui dois casos de suicídio. Um deles é o caso de uma garota que se matou na faculdade.

Isso até mesmo permite que cantores sertanejos, a dupla sertaneja Max e Mariano, façam uma letra como esta: *"E sem que você percebesse eu gravei de nós dois um vídeo de amor. Eu vou jogar na Internet nem que você me processe".* Essa música está circulando por aí, no Youtube, *etc*., tamanho o grau de impunidade que há. Chegaram ao ponto de fazer uma música dessas e publicizar. A pornografia de revanche é cantada em verso e prosa porque não temos, realmente, uma legislação que ataque efetivamente um caso como esse.

A mesma coisa o Tio Astolfo, que foi repassado. Até hoje ainda não conseguimos identificá-lo, porque esse *site* está inoculado nas Ilhas Faroé. Estamos tentando batalhar nessas Ilhas.

O que nós temos de resultado? Cresceram os casos de estupro cometidos contra mulheres que acessam, não só estupros reais como estupros virtuais. Não sei se os senhores têm conhecimento, mas é possível cometer um estupro pela Internet, já que nosso tipo penal de estupro hoje permite o constrangimento sem a conjunção carnal. Como é que nós estamos pegando esses casos? As mulheres estão trocando vídeos íntimos com seus namorados e, quando terminam o relacionamento, os namorados insistem que elas continuem mantendo esses vídeos íntimos. Elas dizem que não vão manter, e eles ameaçam pegar essas fotos e postá-las na rede. Constrangem ilegalmente a mulher a cometer um ato libidinoso diverso da conjunção carnal. Então, até esse estupro está acontecendo diariamente por causa da pornografia de revanche, que não é punida na sua origem.

A mesma coisa foram os casos que nós vimos envolvendo Majú e, agora, Taís. Isto aqui é uma injúria preconceituosa. É um crime de injúria, não é um crime de racismo. Um ataque direcionado individualmente a uma pessoa não pode ser considerado racismo legislativamente falando, embora as penas se equipararam. Porém, ao não coibir os ataques individuais, havendo um crime contra a honra individual, propaga-se o quê? Um efetivo crime de racismo, porque nós não conseguimos atacar na origem, pois que não havia legislação.

A mesma coisa aqui. O que mais chama a atenção são os ataques que acontecem. Eu fui professor e promotor eleitoral durante 10 anos, e estamos preparados para o caos em 2016. Vou explicar o porquê.

Peço mais 5 minutos. Na parte da atuação, de procedimentos, nós estaremos fadados ao caos com as eleições de 45 dias em vez de 90 dias. E vou explicar aqui, detalhadamente, por que, com a experiência de cinco eleições municipais e três estaduais. Enfim, isto aqui é regra geral. Os ataques são maciços, quando não há legislação. A legislação posta na minirreforma de 2013 não é suficiente. Fica típico quando o ataque não é de contratação. Então, já houve várias quedas. Quando isso aqui não atua, o que acontece? Lá na Bahia houve a destruição pública de um

candidato com ataques cibernéticos, e não havia ferramentas para simplesmente evitar.

Tudo isso, senhores, implica em dizer que está faltando legislação, sim. Estão faltando tipos penais, tipos cíveis e tipos administrativos competentes para servir de ferramenta a todos nós no trabalho. Inclusive, eu não quis pôr nomes, coloquei apenas porque tenho a obrigação de referência, mas há várias iniciativas que vêm responder a isso. Existe o PL da pornografia de revanche, existe o PL da Lei Maria da Penha virtual, existe o PL sobre os crimes contra a honra, todos tramitando e criando excelentes tipos penais com excelentes ferramentas. Coloquei alguns, mas, até para evitar direcionar, encaminhar a um Deputado ou a outro, eu passo rapidamente. Peço desculpas, mas não é minha intenção desmerecer ou merecer, é apenas algo exemplificativo. Então, tramita, sim. V.Exas. já estão fazendo. E nós estamos aqui orando para que as coisas fluam e, com esta CPI, se consolidem e se encaminhem.

Naquele tripé ainda há o procedimento célere. Temos procedimento célere no Brasil? Não temos. Por que não temos? Todos sabem, não vou repetir, que os nossos mecanismos são os *logs* e os registros, os IPs, para buscar alguma pessoa na Internet.

Nossa dificuldade é ter que localizar o autor, ter que localizar o computador, desconsiderando os limites geográficos, e tentar coligar o autor ao dispositivo informático. Ou seja, não basta só chegar ao dispositivo informático. É preciso continuar a investigação e chegar até a pessoa que efetivamente cometeu. Agora, vamos dizer: a pessoa que está na Itália usa o computador dos Estados Unidos, afeta 250 computadores em 35 países e usa sete servidores para bloquear o seu IP.

Quando nós conseguirmos não passar por essa situação que praticamente inviabiliza nossa vida de investigação, quando não é cometido o crime pela *deep web*, provavelmente mais pela *dark web*, que também, praticamente, está inviabilizando todos os delegados e promotores estaduais. Só a Polícia Federal e o SESB Cyber têm ferramentas suficientes para atuar na *deep web* com cooperação internacional. É muito difícil para nós atuar. Quando não é pago via Bitcoin, o que inviabiliza toda a nossa atuação, porque a Bitcoin é irrastreável, é um escambo virtual. Quando não temos agora no Brasil essa aberração chamada NAT IPv4, que

transforma os nossos IPs em 132 IPs possíveis. Ainda por cima, os provedores nos negam a porta alegando que não está previsto no Marco Civil. O Marco Civil diz apenas IP, hora, minutos, segundo e GMT. Todos sabem que nós, Ministério Público, temos a obrigação de produzir a prova acusatória. Não podemos produzir uma prova genérica. Eu não posso dizer que 132 pessoas são acusadas. Eu tenho que dizer qual pessoa é acusada. Resultado: em muitas investigações, eu estou simplesmente abortando ou largando de mão, porque não consigo chegar e não sou irresponsável de culpar alguém sem provas. Quando tudo isso passa, ainda vêm os *wi-fi* públicos. Nós não temos a mínima regulamentação dos *wi-fi* públicos, não sabemos de onde esse IP vem, nem para onde vai. Ao chegarmos aos interiores, que hoje estão dando gratuitamente os *wi-fi,* os provedores dizem que o Prefeito nem mandou analisar quem era. Ficamos: *"Meu amigo, não tem o mínimo..." "Não temos ferramenta aqui para saber quem pegou o IP."* Várias pessoas transitam pela cidade, pegam o IP e vão embora. Não conseguimos investigar mais nada.

Quando conseguimos passar por tudo isso, temos que providenciar o protocolo de atuação. Quando chegamos ao protocolo de atuação, o que nos sobra? Os *logs* e os registros. Nesse caso, o Marco Civil nos colocou a imposição, antes não existente, de que, em todos os casos, até mesmo no de provedores de aplicação, tem que se pedir a quebra judicial, sob a alegação do princípio da liberdade de expressão, *etc*., com o qual eu concordo. Agora, convenhamos: vou passar à vida prática e, depois, deixo a discussão para os senhores. Na vida real, eu vou dar um exemplo prático de investigação em Facebook de página *fake*.

Chega à delegacia essa representação, a colega é obrigada a compor, faz o seu termo circunstanciado, chega à página, essa senhora não é ela, essa foto foi retirada do Google, o motor de busca que faz questão de botar a foto de todo o mundo, pega essa foto, cria uma página *fake* e começa a se passar pela pessoa. Até que a vítima teve a sorte de identificar que sua foto estava sendo utilizada por terceiros e levou o caso à delegacia.

Como se fazia no ano passado, antes do Marco Civil, que é uma excepcional lei, mas que, nesse ponto, não entendeu a realidade brasileira? Nós, via Law Enforcement, conseguíamos diretamente o IP, que não diz nada — IP, GMT, hora e

data —, para, só depois, fazer o pedido de quebra ao provedor de conexão e conseguir os dados cadastrais.

A lei de lavagem de dinheiro, a lei de lavagem de capitais, todas elas permitem que tenhamos acesso aos dados cadastrais, menos a Lei dos Crimes Cibernéticos. O que vou ter que fazer? Eu entro com o primeiro pedido de quebra. Esse pedido de quebra vai ser analisado, no mínimo de 5 a 7 dias, por um juiz. Não há varas especializadas em crimes cibernéticos. Eu demoro 7 dias para ter esse dado, para o juiz me dar o deferimento. O Facebook ou outras empresas até conseguem, com algum grau de celeridade, mas nunca em 24 horas, como o STJ exigia. Quando chega para nós, já se passaram 10 dias, 15 dias. Chegou o primeiro IP. Vamos pegar esse IP, analisar quem é o provedor de conexão e, com esse provedor de conexão, pedir uma segunda quebra, para agora procurarmos saber do provedor de conexão a quem atribuiu esse IP. Quando recebemos essa informação, de novo o juiz vai ter que apreciar, de novo vai ter que dar uma decisão, para chegar até nós o dado cadastral. Resolvemos o problema? Não. Chegamos até o dispositivo informático. Isso não significa que a pessoa que usou o dispositivo informático seja o acusado. Precisamos agora, junto com a delegacia, fazer a investigação tradicional: quem usou, busca e apreensão da máquina, oitivas de testemunhas, *e-mail*, *make* da máquina.

Aqui, por exemplo, foi um caso de erro. Chegou-se à máquina do Mução, ele foi preso, mas não cometeu o crime. Quem cometeu o crime foi o irmão. O cara ficou preso por 24 horas, até que o irmão assumisse a culpa, o que é um erro. Não se pode chegar ao dispositivo de informática e pressupor que a pessoa seja a culpada, tem que se prosseguir com as investigações.

O que acontece? Nós estamos levando, em média, de 15 a 120 dias para descortinar um dispositivo informático. O tempo médio, na melhor das hipóteses, é de 30 a 45 dias, quando todo o mundo está concentrado só nisso.

Aqui é o suicídio da garota que estava sofrendo *cyberbullying*. Quarenta e cinco dias para ela é uma vida. Ela morreu, ela não suportou a pressão. E não havia condições de chegar até lá, porque todos esses passos precisam ser tomados.

Eu vou dar o exemplo dos senhores. Eleições 2016. Acho que os senhores estão todos aqui. Como nós levamos o tempo? Nós precisávamos, antes, em 90

dias, do cadastro de registro de candidatura, da impugnação dos registros de candidatura. Depois de impugnados, começam a separar os comitês, dias e datas dos comitês, local de comitê. Começam as propagandas partidárias, impugnação de propaganda partidária, age de um lado, age de outro, todo o prazo em horas. Vejam: quantas vezes o registro de candidatura não chegava a ficar pronto antes de 90 dias. Agora, com 45 dias, nós vamos conseguir realizar o que já havia de dificuldade para fazer? É quase impossível. E quem vai ter tempo para analisar crime cibernético dessa forma, como tem que ser feito, em dois passos, com pedido judicial, com deferimento judicial?

A verdade é que, se a média é de 30 a 45 dias, e em 45 dias termina, basta que se contratem 100 pessoas e comecem a ofender o candidato, que vai ser praticamente inviável perseguir e apurar quem foi. Essas vão ser as eleições de 2016. Estamos enxergando claramente, da forma como fomos fechados. Nós temos dois pedidos, o juiz não dá conta, e nós não vamos dar conta. *"Mas a Polícia Federal tem know-how."* A Polícia Federal não investiga em eleição. Quem investiga em eleição é a Polícia Estadual. E o promotor de atuação em eleição é o promotor estadual. A área federal não atua nas eleições, só quando as eleições são estaduais ou federais. As eleições municipais, todas elas são passadas para nós, promotores estaduais.

Então, é só para passar aos senhores quão difícil é a nossa atuação, com a ferramenta que nos é dada. Há, por exemplo, um PL que tramita nesta Casa, que visa justamente a corrigir isso. É o PL 1.589, que permitiria que nós tivéssemos acesso direto, tal como na prisão em flagrante, e que respondêssemos por crime de 2 a 4 anos, se efetivamente fosse utilizado indevidamente um IP sequestrado.

Nós vivemos um Estado, nós somos Estado, por que não sermos responsabilizados? Sim, mas dificultar, também, vai levar-nos todos ao caos.

Vou tratar agora, só para tentar fechar aqui, das dificuldades de intercepção telemática. WhatsApp, Telegram e ICQ são ininterceptáveis no Brasil. De tudo que é falado, nada se consegue pegar. O WhatsApp se nega a oferecer *QR Code* para nós pegarmos via WhatsApp e *web*.

A criptografia ponto a ponto praticamente inviabiliza a análise, porque é feita em camadas de sete pontos. Ou seja, eu, promotor em execução penal, quando chego aos presídios, vejo 7 *wi-fi* dentro do presídio, chegando facilmente.

O que fazem os presos? Falam mais por telefone? Não. Meu sombra e meu guardião estão lá, praticamente inutilizados, porque os presos falam tudo pelo Voz sobre IP (VoIP), que, no Brasil, hoje, é ininterceptável. E, porque não temos regulação, simplesmente aceitamos a imposição feita pelo mundo. Nos Estados Unidos e na Europa é interceptável, para nós é ininterceptável, porque o WhatsApp se nega a dizer.

Inclusive, nós temos um problema de notificação do WhatsApp. Ele se recusa a ser notificado, porque ele diz que está sendo agregado. É uma agregação que nunca acaba, há 1 ano e meio, essa agregação com o Facebook. Então, ele se recusa a receber a intimação, e o Facebook se recusa a receber a intimação, os crimes estão acontecendo e simplesmente acabam por aí, e nós não conseguimos chegar a lugar nenhum.

Aqui, os crimes cibernéticos próprios — já tentando finalizar — também se servem do mesmo tripé. O tripé da prevenção está no clicador feliz, porque os usuários, em regra, quando recebem seus *spams* e estão naquele dia mais feliz do mundo só fazem apertar "O.K." Eles não são orientados, não são capacitados, e vão inoculando seus *malware*, seus *worms*, seus *Trojans*, e vão colocando... Todos os ataques DOS e Botnet se dão a partir dessas infecções, e o nosso colega já falou ali como rastrear.

A normatização é adequada? Não, pelo contrário. A Lei Carolina Dieckmann — eu não gosto de citar a lei pela vítima, mas assim é conhecida a Lei nº 12.737 —, de longe, tem uma tipicidade penal complicadíssima. Tem tipos objetivos inaceitáveis. A gente não consegue interpretá-los, eles estão caindo em todos os tribunais porque ninguém consegue compreender o que é uma violação indevida de mecanismo. É físico? É ausência? Ou seja, a bisbilhotagem não está inclusa aqui.

Se você for ao banheiro e esquecer o seu telefone aberto, e alguém fizer o que fizer, não está inoculado aqui. Se alguém pegar o seu *e-mail* aberto, também não está inoculado aqui. São tantas elementares do tipo objetivo, que não conseguimos nunca incorporar pegando a primeira parte. Eu só uso a segunda: a

vulnerabilidade para obter vantagem ilícita — e ainda não foi caracterizada que vantagem ilícita é essa. É econômica, é geral, como nos outros crimes que consideram como vantagem ilícita?

Eu sei que está muito difícil, eu sempre caio nos tribunais quando eu tento levar.... E o crime? De 3 meses a 1 ano. E vejam: Juizado Especial Criminal. Então, esta é a nossa dificuldade.

Não há uma legislação para ativistas que possa nos ajudar — *deface*, nada disso. É considerado um crime de dano comum, então não nos ajuda em nada. O crime de *cyberterrorismo* simplesmente é tratado ao largo. O nobre Deputado falou sobre essa preocupação, que é nossa também. É tratado ao largo.

O Brasil é um terreno fértil, não somente para o *cyberterrorismo*, mas para ataques a infraestruturas. Nós não temos nenhum tipo de *certs* no Brasil, fora os *certs* nacionais. É um país com dimensões continentais, sem nenhum tipo de defesa.

E aí eu digo: quanto custa uma guerra convencional, quanto custa uma guerra cibernética? Tenho certeza de que a gente não teria condições de despender 2 bilhões. Nenhum dos nossos "inimigos" gastariam tudo isso com bombardeiro Stealth, com caça *Stealth*, mas, para fazer uma *cyberarma* com 300 reais você começa bem. Basta ter um computador e alguns sisteminhas simples, para começar a trabalhar.

E como se localiza uma fábrica de crimes cibernéticos? Localizar uma fábrica de bombas nucleares é fácil: coloca no Google Earth e consegue buscar. E onde está aqui uma fábrica de crimes cibernéticos, de *cyberarmas*? Não conseguimos localizá-la. Aliás, pode haver até alguém aqui conosco, construindo uma *cyberarma* neste momento, em um local completamente insuspeito.

Aqui, por exemplo, são dois ataques que aconteceram. Parece bobo — já encerrando, Excelência, porque queremos ter sempre a oportunidade de falar tudo o que nos angustia e passar para os senhores.

Foi um ataque a uma infraestrutura. Esse hotel — vamos dizer assim — foi construído com autorização e foi bom para o Município, mas atacou moradores que eram contra esse hotel. Havia *hackers* nesse hotel. O que eles fizeram? Atacaram o sistema de esgotamento que ficava ao lado e conseguiram, a partir desse ataque,

desmoronar toda a parte de controle de bombeamento das estações. Jogaram 7 milhões de litros de esgoto cru em cima do *resort*, destruindo não só o empreendimento, mas toda a área ambiental ali existente, com um simples ataque cibernético.

A mesma coisa foi o ataque Stuxnet, de que todos já ouviram falar. Foi um dos melhores códigos já construídos, mas que atrasou o programa nuclear iraniano em 3 anos; sem uma bomba, sem nada, atacaram toda a infraestrutura crítica do Irã, a partir de... *(ininteligível)*.

Lá na Bahia nós temos o Polo Petroquímico de Camaçari, que, no ano passado, sofreu 32 ataques, e a Braskem sofreu 27. Nós estamos trabalhando com a criação de um *certs*, um centro de respostas imediatas a ataques, porque, se, por exemplo, alguém entrar na Braskem e trocar apenas um componente químico de 0.1 para 1, ele explode a área e contamina toda região de Camaçari, Salvador e adjacências. Basta trocar uma variável da plataforma. Hoje, nenhum lugar do Brasil, um país de dimensões continentais, tem uma *certs*, fora a área federal. Nós não tratamos seriamente os ataques e estamos altamente vulneráveis se eles acontecerem.

Aqui há o exemplo de todas as camadas que podemos ter.

Senhores, isso era o que eu tinha para falar de crimes cibernéticos.

Eu tinha uma apresentação projetada para 35 minutos, mas eu soube que seria apenas 20, e não vou poder concluir, até porque vários colegas ainda vão falar aqui.

Outra questão, por exemplo, são os dados pessoais. Hoje, os dados pessoais que não estou sendo protegidos adequadamente são causa direta de vários crimes cibernéticos, como, por exemplo, o site Tudo sobre Todos. Eu vou parar, porque eu não tenho mais tempo, Excelência.

O SR. DEPUTADO RODRIGO MARTINS - Sra. Presidente, eu só queria só solicitar ao Dr. Fabrício que ele disponibilizasse a apresentação aos Deputados e às assessorias, para que pudéssemos...

O SR. FABRÍCIO RABELO PATURY - Excelência, fica a critério de V.Exas. Eu levaria mais 5 ou 10 minutos para fechar aqui a apresentação, só que eu acho

que seria ruim, seria um desrespeito aos colegas. Eu disponibilizo, claro, sem problemas.

Quero apenas dar um panorama aos senhores sobre o que nós usamos hoje e o que é usado contra nós. Os nossos dados são vendidos. Fontes de dados, o site Tudo sobre Todos e tantos mais que são usados contra todos nós são praticamente sementes de vários crimes cibernéticos.

Só a título de exemplo, existe um site de rede social chamado Sexlog, quase 7,5 milhões de brasileiros o utilizam. É um site brasileiro, no qual os termos de uso concedem licenças vitalícias e sub-reptícias que autorizam a edição. A este site se mandam fotos sexuais suas e de seu cônjuge e relações sexuais sua e de seu cônjuge, que são vendidas a um estabelecimento de voyeurismo, a uma *ménage à trois*, mas, na verdade, é uma autorização de venda ao Xvideos e para outros casos. Então, várias pessoas dizem que seus vídeos foram parar no Google. Mas você leu o termo de condições? No termo de condições, você autorizou. Ao Instagram, que os senhores usam, são doadas as suas fotos. O Facebook as doa, e os senhores não têm direito a nada, os senhores autorizaram a licença. O Facebook cria *cookies* que autoriza mais 420 outros modos e outros sites a utilizar os *cookies*. Por isso que os senhores, quando acessam qualquer consulta, têm 300 mil perguntas na sua tela de computador, e eles não param de atacar até que os senhores ou formatem aquele computador ou joguem ele no lixo, porque serão atacados o tempo todo.

Por fim, se é para fechar, que lutemos pela proibição de indexação em botões de busca, porque às vezes é um crime que, de tanto ser indexados e reindexado pelos botões de busca, vitimizam ainda mais a própria vítima que não consegue ter o seu direito de esquecimento, o que inclusive também está sendo matéria regulada pelos senhores. Queremos passar o máximo de informações, mas em respeito aos colegas encerro a minha fala, porque já avancei demais.

Obrigado a todos pela atenção. *(Palmas.)*

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Muito obrigada, Dr. Fabrício. Vamos aguardar também a apresentação e as sugestões que o senhor tiver a dar a esta Comissão Parlamentar de Inquérito.

Concedo a palavra à Delegada Mayana Rezende, do Grupo de Repressão a Estelionato da Delegacia Estadual de Investigações Criminais de Goiânia. **A**

A SRA. MAYANA REZENDE - Primeiramente, quero cumprimentar a todos os presentes.

Meu nome é Mayana Rezende, chefe do Grupo de Repressão a Estelionato e Outras Fraudes da DEIC do Estado de Goiás. Eu vou ser breve. Eu vou me ater a explicar como é que conseguimos prender essa associação criminosa e de que forma ocorria a fraude.

As investigações perduraram por aproximadamente 2 anos. *(Exibe imagem.)* Primeiramente, nós identificamos uma daquelas pessoas ali, que é o Wagner, que praticava crimes cibernéticos, focado na clonagem de cartões e também no pagamento de boletos bancários. Eu vou pegar uma parte do que Fernando explicou aqui, aquela situação em que ele diz que um vírus é encaminhado para o seu computador e ele começa a captar dados de cartões. Esses números de cartões foram parar na mão daquele Wagner.

De que forma ele conseguiu isso? Ele conseguiu através da própria Internet. São as chamadas bases de dados. Você compra pela Internet bases contendo dados de inúmeros de cartões: meus, seus e de qualquer um que pode estar aqui. A partir desses dados, ele faz a clonagem de cartões, só que o foco dele não é dar um cartão clonado para quem o procurasse e de repente pagasse uma porcentagem. Eu lhe dou um cartão clonado e você, uma porcentagem do que você conseguir passar. Não era assim. O foco dele era agenciar comerciantes dispostos a ser coniventes com esses golpes. Aí, é onde entra o Alex, que foi um dos comerciantes que conseguimos prender. Ele, através da distribuidora de bebidas dele, cedia os terminais eletrônicos dele para que fossem utilizados com cartões clonados.

O que apuramos é que os comerciantes ficavam com pelo menos 40% do valor dos cartões clonados que eram passados ali na distribuidora. Então, nós tínhamos ali o Wagner e o Danilo, que eram as pessoas detentoras dessas bases. Inclusive, nas apreensões que nós fizemos, nós conseguimos identificar em seus computadores centenas de dados de cartões de crédito e dados bancários de pessoas que eram utilizados na clonagem desses cartões. Mais abaixo vêm os comerciantes, que eram coniventes, e outras pessoas também, que eram agenciadores dispostos a buscar comerciantes no mercado que fossem coniventes com essa fraude.

Eles chegaram a falar que tiravam 20 mil reais por semana, mas conseguimos materializar isso com o comerciante Alex. Uma coisa é você saber que o crime está sendo cometido, está sendo praticado; outra coisa é você fechar todo o *iter criminis*, como estava dizendo o Dr. Fabrício, isso virar uma denúncia e, posteriormente, uma condenação. O crime cibernético é muito difícil de ser investigado, não só pela técnica que nem sempre a polícia consegue ter, mas também por ser cometido geralmente por pessoas que estão no Estado. Geralmente, pratica-se o crime em um Estado e fazem-se vítimas em outros. Para quê? Para dificultar a investigação. Isso realmente, às vezes, chega a até inviabilizar a investigação. Muitas vezes nós não temos estrutura nos órgãos públicos para nos dar esse suporte. Gostaria muito de ter o Fernando sempre do nosso lado ali, para conseguir levantar e buscar a autoria desses crimes, mas nem sempre o Estado consegue ter esse suporte.

Além dessa associação criminosa, nós identificamos uma outra que era especializada em fazer transferências bancárias fraudulentas. Nesse caso, nós conseguimos identificar o líder da associação criminosa. Estão abaixo os operadores, depois os agenciadores e os laranjas. Como é que funcionava esse golpe? Bom, era da mesma forma. Quem está lá no topo, que é o líder, era quem detinha os programas e as bases que permitiam fazer essas transferências fraudulentas. Para isso, ele precisava de operadores, que operavam esses programas e também as bases de dados contendo *e-mails*. Pode estar lá o meu e o seu, que também são adquiridos pela Internet.

Ele encaminha um *e-mail* malicioso, em que você clica, ou às vezes até mesmo por aplicativo, e você acaba instalando ali um vírus no seu computador que permite que ele faça o controle remoto do seu computador. Ele acaba operando de forma remota. Por isso, quando você vai às vezes atrás do IP que fez aquela fraude, vai dar o IP da vítima, do meu computador. Então, isso aí já quase que fere de morte a investigação. Você não consegue levantar a autoria, é muito difícil. Mas, nesse caso aqui, nós somos muito felizes. Nós tivemos cem por cento de êxito nas investigações.

Identificamos, então, quem tinha esses programas, quem eram os operadores, que era para quem ele repassava esses programas e fazia os ataques às contas de terceiros. Depois que eles faziam os ataques e subtraíam o dinheiro da

conta de inúmeras pessoas, o dinheiro precisava ir para a conta de alguém. As contas dessas pessoas precisavam ser agenciadas, então vem a figura dos agenciadores.

Nós conseguimos identificar três desses agenciadores. Essas pessoas eram convencidas a emprestar as suas contas bancárias, para onde eram transferidos fraudulentamente esses valores. E a fraude tem que ocorrer rápido, porque eles sabem que, se a instituição financeira perceber a fraude, vai fazer o bloqueio, vai fazer o estorno, e eles não vão conseguir obter a vantagem ilícita. Então, a partir do momento que eles conseguem fazer a subtração e transferir esse dinheiro para a conta de um laranja, o laranja tem que estar disposto a ir imediatamente à agência bancária e fazer o saque daquele dinheiro, até porque, às vezes, horas, para eles, é fundamental, pois podem perder aquele valor que foi transferido.

Qual foi então o diferencial nessa investigação? Foi exatamente a identificação de toda a cadeia. Nós conseguimos identificar quem detinha os programas, quem eram os seus operadores, quem eram os seus agenciadores, que captavam essas contas de terceiros, e também os laranjas. Ao final, nós conseguimos o indiciamento de 26 pessoas.

Como já foi muito explicado aqui, trata-se de crimes bastante difíceis de ser investigados, principalmente porque hoje em dia o IP nem sempre quer dizer alguma coisa, nem sempre revela alguém que tem participação no crime. E, afinal, há aquela questão. Quando essas pessoas chegam à delegacia, elas infelizmente não demonstram nenhuma preocupação — isso é visível —, primeiro, porque sabem, pensam assim: *"Estou caindo agora, mas quantos outros crimes eu já pratiquei que não vão vir à tona?"*. Uma coisa é você saber que aquela pessoa está a todo momento cometendo fraudes eletrônicas; outra coisa é você dizer quem é a vítima dela, quanto ela subtraiu, qual é o valor que ela gerou de prejuízo, quem são as pessoas que detêm aqueles programas, quem promoveu o ataque — isso é outra história. E, para que haja denúncia e condenação, isso precisa ser identificado na investigação.

Então, quando essas pessoas caem, no fundo elas sabem que já fizeram muito e já lucraram muito. A investigação tem nos demonstrado que a consciência que elas têm é a de que o crime cibernético compensa, infelizmente, porque sabem

que, ao final, quando chegarem a cair, já lucraram e conseguiram cometer muitos outros crimes.

Aqui fica, portanto, esta questão, realmente precisamos ter mais estrutura. As empresas que vêm com essas tecnologias precisam estar mais dispostas a nos ceder essas informações de forma menos burocrática, para que consigamos ter uma polícia judiciária que atue de forma mais efetiva no controle da prática de crime cibernético, porque, do contrário, vai prevalecer essa história de que: *"Quando caio, para mim, já compensou o que eu fiz".* Infelizmente é assim.

E agora eu estou aberta a qualquer questionamento. Nós temos muitos outros casos de crimes cibernéticos, mas aqui, no caso da CPI, fomos convidados para falar especificamente em relação a esse crime.

Aliás, uma questão que eu queria ressaltar também é que essas pessoas quase nunca têm antecedentes criminais, exatamente por isto: são pessoas que vivem na sociedade acima de qualquer suspeita, que moram em condomínios, que conduzem carros de luxo. Estão convivendo entre nós assim, sem a menor suspeita da prática desses crimes. Então, essas pessoas não têm antecedentes criminais exatamente porque se trata de um crime difícil de se investigar, pois pouco suporte têm as polícias para isso, o que acaba gerando, infelizmente, a impunidade, um incentivo. *(Palmas.)*

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

Dando continuidade aos trabalhos, concedo a palavra ao Sr. Delegado Sílvio Kist Huppes, titular da Delegacia de Policiamento do Interior, na cidade de Encantado, Rio Grande do Sul.

O SR. SÍLVIO KIST HUPPES - Bom dia a todos! Quero cumprimentar V.Exa., Sra. Presidente, agradecendo pelo convite para estar aqui, e também os colegas na Mesa, os Deputados que acompanham esta reunião e as demais pessoas.

Vou falar basicamente de uma investigação. São duas investigações que ocorreram na cidade de Encantado, que tiveram uma repercussão muito grande na cidade, e também foram objeto desse programa da Rede Globo, pela repercussão que tiveram também no Estado do Rio Grande do Sul.

(Segue-se exibição de imagens.)

Quaro apenas contextualizar o porquê dessa repercussão tão grande — e isso pode se repetir em outras cidades, em pequenas cidades do Brasil; a cidade de Encantado tem cerca de 20 mil habitantes —, a repercussão desses crimes pela Internet. Na verdade, houve a exposição de duas moças, sendo uma delas menor de idade. Elas tiveram um vídeo e fotos íntimas divulgadas pela cidade. Sendo uma cidade com cerca de 20 mil habitantes, houve essa repercussão maior, até porque em Encantando há só uma rua principal, os bares são poucos, os restaurantes também. Então, quando alguma pessoa é vítima dessa exposição enorme, num centro pequeno assim, a repercussão é maior do que em centros maiores. Essa pessoa continua circulando por esses mesmos lugares e encontrando as pessoas.

Nós tivemos, basicamente, dois inquéritos policiais instaurados no mês de maio deste ano: um deles dessa vítima maior de idade, que teve uma fração de um vídeo íntimo divulgado e também algumas fotos em que estava nua; e o outro dessa outra jovem, com 17 anos, que teve três fotos dela nua também divulgadas através das redes sociais. Vou trata-los como Inquérito I e Inquérito II, apenas para facilitar a explanação.

Então, o Inquérito I é dessa moça maior de idade, que gravou esse vídeo antes do ano de 2010, quando terminou o relacionamento. Esse vídeo havia ficado armazenado apenas no computador desse ex-namorado, e agora, no ano de 2015, uma parte desse vídeo e as fotos vieram à tona. O ex-namorado disse que apenas emprestou o computador uma vez, neste ano de 2015, para serem copiadas músicas do HD desse computador. E, no final do mês de abril, então, através dos grupos, das redes socais, principalmente pelo WhatsApp, mas também pelo Facebook, essas imagens, de forma muito rápida, foram divulgadas pela cidade e pela região. Alguns grupos, como Hlera, Ousadia&Putaria, Roca é Inter, Motoqueiros de Encantado e Kabettos, entre outras centenas e milhares de pessoas, receberam essas fotos e essas imagens.

Essa fração de vídeo foi uma parte que tinha exatamente o rosto da menina. E, com relação às fotos, ela nos disse que eram dezenas, e apenas em cinco fotos aparecia ela nua mostrando o rosto. Ou seja, há aí um objetivo de denegrir a imagem. O vídeo, segundo ela, era de mais de 10 minutos, mas aparece

exatamente a parte que mostra o rosto dela. Ou seja, ficou claro esse objetivo de denegrir a imagem.

Isso gerou repercussão — nós tivemos a visita de vários Deputados da Assembleia Legislativa do Rio Grande do Sul também —, e não só comentaram sobre essa divulgação indevida, mas também recriminaram o comportamento das meninas.

Eu vou citar rapidamente aqui o que um dos administradores do grupo disse: *"E aí galera, o que acharam do nosso grupo ter ficado famoso que até saiu no jornal? Todos em sã consciência sabem que menina que faz isso é puta. Falo mesmo: puta!"* Foi o que foi divulgado. Excelência, eu peço desculpas, mas estou apenas relatando exatamente os termos que foram expressos. E outro comentário, do grupo Ousadia&Putaria: *"Ninguém roubou essas fotos, elas mandaram porque querem. Existem milhões de grupos como o nosso de homens que postam putaria o dia todo, só acho engraçado que quando é a filha de uma família nobre da cidade querem processar..."*.

E nós tivemos, ainda, um conhecido colunista que escreve no principal jornal da cidade que também postou no Facebook a opinião dele: *"Será que essas moças não têm dó dos seus familiares? Alguém disse que precisariam de acompanhamento psicológico. Tem uma boa cinta de couro de búfalo com uma fivela de metal que ajudaria em muito o psicológico delas. Vamos crescer e amadurecer..."*.

Enfim, isso gerou uma passeata de dezenas, de mais de uma centena de mulheres em Encantado por conta da liberdade que as mulheres têm de fazer o que quiserem, enfim, de filmarem o que quiserem entre quatro paredes. E houve não só essa repercussão por conta da divulgação, mas também inúmeros comentários recriminando o fato de elas terem feito essas fotos, o que gerou mais repercussão.

Nós realizamos uma operação no final de maio, cumprimos diversos mandados de busca e apreensão para apreendermos — desculpe-me a redundância — esse material dos suspeitos: computadores, *tablets*, enfim. Logo depois, nós encaminhamos esse material à perícia e até hoje, quinta-feira, 19 de novembro, nós não temos qualquer conclusão desse material em que nós buscávamos descobrir quem havia extraído essas fotos e quem havia, então, feito essa divulgação, se havia sido o namorado ou aquele amigo, e outras apurações possíveis.

Um parênteses, apenas: nós temos no Instituto Geral de Perícias do Estado do Rio Grande do Sul — IGP 2 mil protocolos de perícia. Um protocolo não é uma perícia. Um protocolo, como o nosso, são dezenas de perícias para serem realizadas. Existem quatro peritos de informática, e, apenas para se ter uma ideia, em média, um HD demora 2 semanas para ser periciado. Então, essa é uma dificuldade com relação à perícia de informática, quando nós conseguimos a apreensão de equipamentos nesse sentido.

Eu gostaria de salientar — e esta é uma das principais considerações que eu faço, farei novamente em breve — que a repercussão desse crime foi enorme na cidade, na região. Agora, a sanção desse crime de injúria, prevista no nosso Código Penal, que vem da década de 40, seria de 1 a 6 meses, acrescida de um terço. Então, nós teríamos um pouquinho mais de 1 mês de pena.

Nós também tivemos, em relação a um dos principais suspeitos — nesse caso do vídeo em que ela era a atual namorada desse indivíduo e em que ele queria denegrir a imagem dela —, por duas vezes, indeferido o nosso mandado de busca e apreensão para periciar o material dele. O despacho judicial foi de que *"a via eleita consistia na forma mais midiática e menos efetiva, que é a apreensão física dos computadores, sendo que a ofensa à imagem da vítima permanecerá ainda em circulação, considerando o funcionamento do armazenamento de dados da rede mundial de computadores"*. Isso é verdade. Mas também é verdade que nós precisávamos da apreensão do equipamento desse suspeito para a condução do inquérito.

Nesse caso, as principais dificuldades são: a rapidez da divulgação pelas redes sociais — não é um clique, é um simples toque na tela para se divulgar por grupos do WhatsApp e centenas, milhares de pessoas, em questão de segundos, terem esse material e o replicarem também, o que aumenta o número de suspeitos de forma muito rápida atualmente; a demora na conclusão do trabalho pericial — já são vários meses, e nós não temos qualquer tipo de resposta, e na verdade nós poderíamos ter apontado novos suspeitos ou outros rumos para a investigação; o indeferimento na apreensão de equipamentos; e a pouca ou nenhuma colaboração dos envolvidos — as pessoas não vinham até a delegacia para trazer esse material, as fotos, os vídeos, o que estava circulando na Internet, por medo de também serem

responsabilizadas caso trouxessem esse material e demonstrassem que tinham esse material.

A vítima, essa moça de 24 anos, nos disse que, logo após o fato, segundo ela, não teve o contrato de trabalho renovado. Ela trabalhava como secretária na cidade. Ela ficava em frente a um vidro grande, e inúmeros veículos de imprensa, curiosos e pessoas foram buscar informações com ela ou procurá-la nos dias seguintes. E, segundo ela, esse foi o principal motivo por ter o contrato de trabalho rescindido. Também ela nos disse que, se não tivesse tido o apoio muito forte da família nos primeiros dias, na primeira semana, ela teria feito alguma bobagem, como atentar contra a integridade física e contra a vida.

Parece exagero, parece demais, mas o colega até citou, a 100 quilômetros de Encantado, no ano passado, o caso de uma menina que expôs apenas os seios, uma menina de 16 anos — e eu digo “apenas” porque poderia ter sido muito mais, como foi nesse caso, partes íntimas ou até um vídeo praticando sexo com o namorado — que expôs os seios para um indivíduo que era amigo no Facebook, não era namorado, e esse indivíduo, no ano passado, encaminhou essas imagens, não para tantas pessoas — o WhatsApp não era tão usado ainda —, mas para algumas pessoas na cidade de Veranópolis. E essa menina, na iminência de os pais saberem disso — era uma educação muito rigorosa —, enforcou-se na sala da casa.

Portanto, não parece exagero o comentário dela. Isso é o que causa, como neste caso aqui, nas mulheres, o fato de terem, não só a honra, a intimidade, mas também a própria dignidade exposta de maneira pública, de forma tão rápida, como ocorre atualmente.

O Inquérito II é um pouco diferente. O Inquérito II é de uma menor de idade. A menina fazia fotos, tirava fotos, e nós conseguimos comprovar isso. E ela admitiu que pelo menos para seis indivíduos, não namorados, pessoas, meninos que ela conhecia no Facebook, ela encaminhava, por vontade própria, fotos dela nua. Ela disse que pedia para não serem divulgadas. E eles diziam que ela nunca fez um pedido assim. Essas fotos também foram divulgadas através do WhatsApp e do Facebook. Nós realizamos a apreensão de equipamentos. Neste caso, foi outro juiz quem analisou os pedidos, e ele deferiu todas as buscas. Nós estamos aguardando a perícia deste caso também.

E, por ser menor de idade, por ter 17 anos ainda — na verdade, olhando, é uma menina formada já; quem olha a foto não sabe se ela tem 16, 17, 18 ou 19 anos, enfim —, a nossa legislação, nesse caso, é, sim, mais rigorosa, prevendo o apenamento, pelo fato de simplesmente armazenar imagens de uma menor de idade, de 3 a 6 anos de reclusão, através do Estatuto da Criança e do Adolescente.

Eu vou fazer duas considerações finais aos senhores. A primeira é com relação à dificuldade nas investigações desses crimes contra a honra praticados através do Facebook, do WhatsApp e das redes sociais. O colega já falou bastante sobre isso também, bem como sobre o Marco Civil. Mas é importante, sim, que nós tenhamos — e os senhores podem ajudar o País nesse sentido — uma legislação sobre esses sistemas e esses programas, para que nós possamos, de uma forma mais eficaz e rápida, monitorar, interceptar e ter acesso a esses dados.

A segunda observação é com relação a esse tipo de crime. Nós estamos dispendendo enormes recursos, há toda uma repercussão na cidade, mas o apenamento parece-me brando demais. Parece-me que chamar alguém de idiota ou proferir qualquer outra injúria contra ele é muito menos do que expor a sua imagem ou intimidade dessa forma. E a simples inclusão como crime de injúria não abarca toda a violação, todo o ataque a moças, como o que essa mulher e essa menina tiveram.

Já está previsto para o crime de injúria racial, por exemplo, um apenamento maior. É um crime grave, cuja pena é de 1 a 3 anos. Então, nesse caso em que há toda uma violação à intimidade, parece-me que o apenamento deveria ser muito maior, como se fossem crimes cibernéticos. E na decisão judicial que deferiu parcialmente os mandados de busca, o juiz inclusive fez constar isso.

Os senhores saibam que, nesses casos, mesmo que nós comprovássemos que houve a divulgação de imagem, se não conseguíssemos comprovar que o objetivo foi o de denegrir a imagem, o decoro e a dignidade das pessoas, os envolvidos não seriam punidos. Então, nós estamos fazendo todo esse trabalho.

Esses fatos ocorrem no Brasil todos os dias, mas as pessoas não são punidas. Se um indivíduo encaminhar a imagem de uma moça sem conhecê-la, por exemplo, só porque achou bonita a foto dela nua, em princípio nós não temos como comprovar que ele tinha a intenção de denegrir a sua imagem e de injuriá-la.

Portanto não haverá, salvo melhor juízo, uma sanção criminal; poderá haver, sim, uma indenização na esfera cível. Agora, se for uma pessoa sem recursos, isso simplesmente passará ao largo da lei.

Portanto, basicamente eu quero reforçar que a nossa investigação foi sobre crimes contra a honra. Eu ampliei um pouco a minha exposição para falar sobre a intimidade e a própria dignidade dessas pessoas.

Deixo como sugestão para os trabalhos que seja avaliado um apenamento maior para esses casos, não se exigindo sempre o dolo específico de denegrir a imagem, porque o simples repasse dessas informações de forma tão rápida também contribui para a prática desses crimes.

Muito obrigado. *(Palmas.)*

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Vamos dar sequência à nossa reunião.

Gostaria somente de registrar a presença aqui na Casa do Prefeito João Miranda, de Pimenteiras do Oeste. Seja bem-vindo!

Neste momento nós vamos conceder a palavra aos inscritos. Eu tive que assumir a presidência dos trabalhos enquanto a Deputada Mariana Carvalho estiver ausente, mas, por ser Sub-Relator, tenho algumas perguntas a fazer.

Sr. Fernando, eu vou iniciar por V.Sa., até porque também está com problema de horário de voo. Eu gostaria de saber como V.Sa. se preparou para atuar na área de segurança da informação e se aqui no Brasil há cursos específicos que preparam adequadamente profissionais para essa área específica.

Levando em consideração a experiência que V.Sa. tem, quais são as principais vulnerabilidades que levam as pessoas a serem vítimas de crimes cibernéticos? Qual é o crime mais comum ou mais frequente na visão V.Sa.?

Também gostaria de saber a opinião e o grau de segurança cibernético em geral das entidades privadas e públicas do Brasil. V.Sa. tem notícia de algum ataque efetivado contra os órgãos públicos do Brasil? Caso afirmativo, qual foi o ataque e quais foram os prejuízos causados à Nação?

Qual é a sugestão de V.Sa. para melhorar a segurança na Internet?

O SR. DEPUTADO SILAS FREIRE - Sr. Presidente, ele vai responder por bloco ou vai responder logo a V.Exa.?

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Vamos fazer por bloco, para que ele possa sair.

Seguindo a ordem de inscrição, tem a palavra o Deputado Silas Freire. Em seguida, falarão a Deputada Alice Portugal e o Deputado Delegado Waldir.

O SR. DEPUTADO SILAS FREIRE - Sr. Presidente, ao fazer algumas interpelações ao Sr. Fernando, eu vou aproveitar para interpelar os demais.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Deputado Silas Freire, vamos fazer logo as perguntas ao Sr. Fernando. Eu também tenho várias outras perguntas a fazer.

O SR. DEPUTADO SILAS FREIRE - Tudo bem.

Dr. Fernando, a maioria dos bancos brasileiros incentiva os clientes de serviços *on-line* a instalarem um *plug-in* em seus computadores. Diante da sua experiência e da ciência que aprendeu no mundo cibernético, eu pergunto se essa ferramenta de fato impede que códigos maliciosos sejam executados durante uma operação de sessão bancária. Essa é a primeira pergunta.

Nós sabemos que existem *hackers* que podem conseguir o controle sobre uma empresa. Quais os principais riscos para as empresas? Como nós podemos também nos prevenir?

Seriam essas as perguntas ao Dr. Fernando.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Deputada Alice Portugal, V.Exa. tem algum questionamento ao Sr. Fernando Mercês?

A SRA. DEPUTADA ALICE PORTUGAL - É só para ele?

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Sim, por conta do horário.

A SRA. DEPUTADA ALICE PORTUGAL - Apenas quero saudá-lo. Eu cheguei apenas ao final da exposição, que achei muito útil. Parabéns, Sr. Fernando!

O SR. PRESIDENTE (Deputado Rodrigo Martins) - O Deputado Delegado Waldir também não tem questionamento.

Então, Sr. Fernando, fique à vontade.

O SR. FERNANDO MERCÊS - Sobre a primeira questão, do *plug-in* bancário, os bancos trabalham ativamente com empresas que desenvolvem esses *plug-ins* bancários, porque exigem que sejam instalados em dispositivos para que o acesso

seja feito. Esses *plug-ins* fazem, sim, um papel importante na prevenção contra ameaças bancárias.

No entanto, assim como um *software* antivírus, por exemplo, há certo comportamento reativo, ou seja, quando uma ameaça bancária é descoberta, é criada uma proteção para que ela não infecte mais, não funcione mais. E sabedores disso, os *cyber*-criminosos criam ameaças bancárias o tempo inteiro. No Brasil, somente em um dos pontos que eu recebo, há uma média de 40 novos vírus diferentes por dia, com o objetivo de atacar clientes de bancos brasileiros. E a resposta pode durar 1 ou 2 dias, seja ela das empresas de antivírus ou seja das empresas que desenvolvem o *plug-in* dos bancos. Mas o *cyber*-criminoso não espera mesmo que o seu vírus funcione mais do que esse tempo, pois já está criando o próximo.

Então, é uma proteção sim. Mas ela não garante 100%.

O SR. DEPUTADO SILAS FREIRE - A outra pergunta é com relação ao controle das empresas.

Eu quero aproveitar, Sr. Presidente, para fazer mais uma pergunta ao Sr. Fernando, porque eu esqueci.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Fique à vontade, Sr. Deputado.

O SR. DEPUTADO SILAS FREIRE - Na realidade, há o uso de cartões de crédito roubados em algumas operações, que são usados por pessoas com perfis falsos, por laranjas que acabam recebendo essas mercadorias também.

Na sua visão e pela sua experiência, há como acabar com essas compras fraudulentas da Internet?

O SR. FERNANDO MERCÊS - É um desafio muito grande para as empresas de comércio *on-line* identificar se a pessoa que está comprando é de fato quem ela informa ser. Então, acabar com essa fraude...

O SR. DEPUTADO SILAS FREIRE - Não há ferramenta para isso?

O SR. FERNANDO MERCÊS - Não. Esse tipo de comércio trabalha com o nome de usuário, a senha, os dados de CPF e o endereço, informações de praticamente todos os brasileiros que são vendidas inclusive no mercado paralelo.

O que um *website* pode fazer a mais? Se ele dificultar muito, cairá no problema da educação digital. Por exemplo, ele poderia exigir o que alguns bancos exigem: que você instale um aplicativo no seu *smartphone* — o que chamamos de autenticação em dois fatores —, que é mais um item que prova que você é você.

No entanto, com o *gap* que existe na educação digital, se ele fizer isso vai reduzir o seu poder de venda bastante, pois venderá a quem tem *smartphone* e a quem sabe fazer isso.

Portanto, nós vivemos realmente um problema em que a educação digital é um componente muito sério, para o qual não estamos olhando tanto.

O SR. DEPUTADO SILAS FREIRE - As empresas podem se livrar 100%, por exemplo, do controle de *hackers*?

O SRS. FERNANDO MERCÊS - Cem por cento é impossível. E eu falo isso do fundo da minha honestidade, trabalhando numa empresa que se propõe a proteger. Mas 100% é impossível.

O SR. DEPUTADO SILAS FREIRE - Estou satisfeito. Obrigado.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Sr. Fernando, agora vamos às nossas perguntas.

O SRS. FERNANDO MERCÊS - O.k. A primeira, então, foi de que forma eu me preparei para atuar nessa área. Essa é uma pergunta interessante.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Eu também quero saber se há cursos aqui no Brasil.

O SRS. FERNANDO MERCÊS - Se há cursos específicos no Brasil.

Segurança é um comportamento. Então, apesar de algumas universidades e alguns cursos se propuserem a ensinar segurança, não existe de fato uma matéria específica. Nós estamos falando de computação, ou seja, de programação e *web*, que têm algumas subáreas já predefinidas. E segurança é o mau uso delas.

Não existe outra área chamada segurança, um assunto completamente novo. Segurança trata simplesmente da subversão de uma transação que deveria funcionar de uma forma “x”, mas que foi subvertida porque quem fez o *design*, quem a desenvolveu, quem a estudou e implantou não pensou que um indivíduo poderia utilizá-la de uma forma “y”.

Então, apesar de haver cursos na área que podem ajudar bastante, eu acredito que a principal arma nossa contra o *cybercrime* seja contar com especialistas. Nós vimos na apresentação da delegada, por exemplo, uma rede com uma série de pessoas envolvidas, onde acredito que talvez a minoria seja especialista em informática. Mas as pessoas que criam as principais ameaças têm um nível de especialização muito alto. Essas pessoas não foram estudar tardiamente ou fazer cursos, são pessoas que nasceram já nesse ambiente, que talvez tenham estudado isso desde a infância ou a adolescência e hoje estão cometendo crimes digitais.

Portanto, não me parece muito efetivo achar que nós podemos enfrentar esse tipo de nova ameaça simplesmente pegando, por exemplo, um oficial ou um grupo que está acostumado com o crime tradicional aqui e dizer: *"Agora a gente vai trabalhar vocês contra o cybercrime*". É uma demanda que talvez vá demorar um tempo para existir.

Então, de que forma eu me preparei? Só para fechar, eu sempre trabalhei com isso, nunca tive outro emprego, sempre trabalhei na área de informática. Um dia eu ouvi falar sobre a subversão do uso do computador e, sim, o assunto segurança. E foi uma migração muito suave: bastou simplesmente eu entender que tudo aquilo que fazia podia ser feito de outra maneira.

Portanto, o recado que eu deixo é: não acredito que segurança seja algo ensinável completamente, mas, sim, conscientizável. O.k.?

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Sr. Fernando, eu sei do seu horário, então, para facilitar, se V.Sa. não se incomodar, deixo essas perguntas e peço que V.Sa. nos responda por *e-mail*.

O SRS. FERNANDO MERCÊS - É claro.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Mas antes de V.Sa. sair, eu queria que respondesse a um questionamento. V.Sa. falou na sua apresentação que existem inúmeros fóruns sobre segurança cibernética ou a falta dela, que muitos são debatidos e que o intuito principal é como prejudicar ou invadir um sistema.

Eu lhe questiono: esses fóruns são nas redes sociais ou em *sites* específicos e são de alguma forma mediados por algumas pessoas? Essas pessoas, no mínimo,

são coniventes. Elas podem ou deveriam ser processadas ou investigadas? Era só essa questão.

Deputado Silas Freire, V.Exa. queria fazer um complemento?

O SR. DEPUTADO SILAS FREIRE - Só para complementar — se ele não puder responder agora por causa do tempo, pode nos mandar por *e-mail*: além de permitir o acesso a qualquer parte do mundo, o armazenamento de dados em nuvens seria uma diminuição de gastos, uma maneira mais segura para os arquivos?

O SR. FERNANDO MERCÊS - Ok. Eu vou responder a isso primeiro.

O SR. DEPUTADO SILAS FREIRE - Sim.

O SR. FERNANDO MERCÊS - Diminuição de gastos, sem dúvida. Em relação à segurança, não resolve. Segurança não tem solução. Segurança é um comportamento, uma monitoração constante, para saber responder a um ataque, porque você vai ser atacado. Não existe a possibilidade de ser atacado: você vai ser atacado. Hoje, se a gente levantar um computador, colocar numa rede e começar a monitorar, os ataques começam a pipocar no mesmo segundo. Realmente vai ser atacado.

Voltando à pergunta sobre os fóruns, eles existem em várias camadas da Internet. Como o Dr. Fabrício comentou, na *deep web* existem fóruns, mas não é que sejam irrastreáveis. São irrastreáveis nos meios técnicos tradicionais. Não adianta você pedir um IP da *deep web*, vai vir um IP de um país do Oriente Médio, da China, da Ásia, não importa. Mas há outras técnicas de rastreamento, principalmente com inteligência. A gente consegue verificar, por exemplo, uma ameaça, um vírus criado, olhando como esse vírus foi criado ou como ele se comporta, e atribuí-lo a um grupo “x”.

O SR. DEPUTADO SILAS FREIRE - A assinatura.

O SR. FERNANDO MERCÊS - Exatamente. Mas existe na *deep web* e existe na *web* tradicional. Então, há fórum, sim, em que se digita de qualquer *browser* e se acessa inclusive do celular, e o pessoal tem trabalhado sem medo de punição, e em redes sociais, sem dúvida. A resposta é que eles estão em todos os lugares: em grupos de WhatsApp, em Facebook, e também em algumas redes, mas fora os fechados, onde não se entra. As redes chamadas GRC, uma tecnologia um pouco

antiga, mas ainda em uso, onde é impossível entrar. Eles só aceitam convidados dos próprios criminosos que já estão lá dentro.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Podemos, então, liberá-lo para não perder o horário do voo. Fernando, fica o nosso agradecimento a V.Sa. por ter participado. Ficamos à espera de suas respostas a essas questões que foram formuladas a V.Sa.

O SR. FERNANDO MERCÊS - Tudo bem. Sem problemas. Eu agradeço.

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

Eu teria algumas perguntas, eu já as entreguei aqui pessoalmente para cada um deles, mas, por economicidade de tempo, eles ficaram de nos responder via Internet. De forma objetiva, vou iniciar as minhas perguntas ao Sílvio, delegado que investigou aquele caso.

O primeiro questionamento é se existem na Polícia Civil do Rio Grande do Sul setores ou equipes especializadas no combate à ação delituosa em rede de computadores ou dispositivos de comunicação. Em caso negativo, se V.Sa. tem conhecimento se a Polícia Civil pretende estruturar uma equipe e quando ela pretende fazer essa ação. Questiono também se, na visão de V.Sa., a Polícia Civil está devidamente aparelhada para combater os crimes cibernéticos.

Pode falar, resumidamente, da Polícia do Rio Grande do Sul, onde V.Sa. tem um conhecimento de praxe.

Questiono também se V.Sa. já investigou, além desses dois casos, outros casos de crimes cibernéticos e qual a porcentagem de sucesso de conclusão de casos, se pegou algum culpado.

Aproveito para perguntar a V.Sa. se já teve que fazer ao Judiciário a solicitação de IP para chegar à origem de determinada postagem criminosa. Se isso já tiver acontecido, em caso afirmativo, qual o prazo médio em que o Judiciário analisa esse pedido.

Quero também fazer uns questionamentos, deixei outros, mas eu quero priorizar a Delegada de Polícia Civil do Estado de Goiás, a Dra. Mayana Rezende, mais ou menos com as mesmas perguntas: se a Polícia Civil de Goiás está preparada, se tem um núcleo específico, e, na visão de V.Sa., como a Internet tem

modificado a atuação das organizações criminosas no Estado do qual a senhora faz parte.

Muito do que foi apresentado aqui pelo Dr. Fabrício coincide em pensamento com o entendimento da Sub-Relatoria e dos consultores que nos assessoram nesta CPI. Eu questiono ao senhor se o Ministério Público está devidamente aparelhado hoje para combater os crimes cibernéticos; qual a importância, em sua visão, de um núcleo específico para tratar de crimes cibernéticos dentro do próprio Ministério Público; e se todos os Estados deveriam ter um núcleo específico para tratar de crimes dessa natureza.

Eu deixo por escrito as outras perguntas e fico no aguardo das respostas.

Concedo a palavra ao Deputado Silas Freire, pela ordem.

O SR. DEPUTADO SILAS FREIRE - Pois é, a questão desse tempo acaba nos prejudicando. Eu farei as perguntas e tenho também que me retirar.

Eu queria fazer uma pergunta ao Sr. Promotor de Justiça. Aliás, eu sugeri a esta CPI, através desta gravação e de um requerimento que eu encaminharei, que devemos pedir a associação do Ministério Público, em nível de Brasil, por meio de sugestões, para que nós possamos implementá-las como leis nesta Casa.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Sim.

O SR. DEPUTADO SILAS FREIRE - A fala do Promotor aqui foi muito clara, muito esclarecedora. Nós já tínhamos esses prenúncios que, no entanto, se confirmaram com a sua manifestação de que nós precisamos fazer um *link* da lei cibernética deste País com a lei penal, porque os tribunais estão negando. A nossa lei é nova, é moderna, mas ela não linca com a penalidade, com a lei penal, e, com isso, o Ministério Público fica atado, amarrado, ao tentar penalizar esses criminosos cibernéticos.

Eu vou fazer algumas perguntas a V.Exa. Os crimes mais comuns na Internet contra a honra são injúria, calúnia, difamação — o senhor até tocou no assunto — no âmbito das redes sociais, principalmente em períodos eleitorais, quando há muito disto: um candidato acusava outro de determinada conduta, para ver se conseguia diminuir os eleitores do outro. As mídias sociais — Facebook, Twitter e várias outras — são utilizadas nesse tipo de crime.

Na visão do Ministério Público, como nós podemos evitar esse tipo de crime? Até como políticos mesmo, como fazer essa defesa?

Outra pergunta diz respeito à necessidade urgente — V.Sa. pode falar — da ligação das nossas leis do nosso Marco Civil, que eu acho fenomenal, com o Código Penal.

Pergunto, então, aos dois delegados de polícia aqui presentes — um, do Estado de Goiás, se não me falha a memória; o outro, do Rio Grande do Sul — se as polícias estaduais têm essa estrutura. Aqui foi narrado pelo Ministério Público da Bahia que em alguns casos, principalmente neste inferno que é a *deep web* ou no WhatsApp, só a Polícia Federal tem tecnologias para adentrar esse submundo da *net*.

Eu tenho uma curiosidade, porque eu imagino que são Estados bem mais desenvolvidos do que o meu humilde...

O SR. PRESIDENTE (Deputado Rodrigo Martins) - O nosso.

O SR. DEPUTADO SILAS FREIRE - ...mas honroso Piauí, do Presidente também, que preside esta sessão. Gostaria de saber se vocês têm essa estrutura, se está havendo um intercâmbio da polícia estadual com a Polícia Federal. A própria Polícia Federal já esteve aqui, ela tem um determinado intercâmbio, mas ela tem limites, por exemplo, no acesso a informações que a polícia americana, como o FBI, tem hoje.

Eu ia sugerir, a propósito, que nós pudéssemos obter informações do FBI americano, mesmo diante das dificuldades de custo aqui nesta Casa. Seria interessante. Esta CPI precisa mostrar resultados.

Essas são praticamente as nossas indagações aos nossos convidados.

No mais, parabenizo a todos pela exposição. É claro que o delegado do Rio Grande do Sul trouxe um caso isolado. A delegada de Goiás trouxe informações de outra operação magnífica, conhecida no Brasil inteiro, e o Ministério Público, de forma mais abrangente, acabou clareando uma ideia que nós temos.

Nós vamos apresentar vários outros requerimentos, porque eu acho que esse *link* entre o crime na Internet e o Código Penal precisa ser feito urgentemente. Senão, vai haver aquela sensação de impunidade, e nós ficaremos marcando ponto

aqui no Marco Civil, na Lei da Internet. Se nós não criarmos a previsão legal para esse tipo de crime, esses caras vão continuar cometendo crimes.

Muito obrigado, Sr. Presidente.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Com a palavra a Deputada Alice Portugal.

A SRA. DEPUTADA ALICE PORTUGAL - Bom dia a todos e a todas.

Eu gostaria, primeiro, de parabenizar o Deputado Rodrigo por esta mesa, que é bastante consistente, porque traz o objeto concreto e a ampliação da visão, com a fala do Dr. Fabrício.

Eu queria saudar os delegados das capitais e do interior pela atuação e pela intenção. Tem sido uma luta para delegados e agentes enfrentar os crimes na Internet sem efetiva infraestrutura, sem equipamentos e técnicos, como muito bem colocou o último convidado, que precisou sair. Essa estrutura precisa, de fato, ser montada.

Algo que ele disse me parece muito interessante. Nós não vamos montar uma infraestrutura para investigação e apuração das denúncias de possíveis crimes na *web* com os mesmos técnicos em segurança pública que nós temos. A inteligência é outra vocação, outra vertente.

Nós estamos sendo, o tempo todo, superciosos nesta CPI. Isso, às vezes, incomoda, mas é necessário, para que encontremos o foco de trabalho real da CPI e possamos acrescentar consistência ao Marco Civil, por meio de uma atitude conteudística, capaz de fazer com que este ano possamos avançar no processo de investigação, criminalização e proteção — proteção no sentido da prevenção, conforme foi muito bem trabalhado pelo Dr. Fabrício.

Assim, eu queria que os dois delegados avaliassem que tipo de estrutura esta CPI poderia propor e definir como regramento legal, para que os Estados brasileiros pudessem dele dispor, do ponto de vista da própria constituição do sistema público, e o que nós poderíamos fazer, no que diz respeito a inteligências e capacitações nos concursos públicos, para montarmos essas estruturas nos Estados.

Como nós vimos, não é formal a educação desses jovens, que são talvez os que conseguem imergir com mais profundidade nos crimes mais graves que ocorrem no mundo virtual, como, por exemplo, crimes bancários de alta monta, ataques ao

sistema financeiro e, sem dúvida, às individualidades, por meio de *sites* como o Tudo sobre Todos.

Pergunto como nós conformaríamos uma instrução técnica para a absorção desses quadros. Trata-se de algo em que nós precisamos pensar. Como nós, Deputado Rodrigo, poderíamos promover a absorção desses quadros pelo sistema público? Isso se daria por meio de qual capacitação, de qual análise, já que decididamente não seria por meio da titulação da academia formal? Nós temos que ver isso.

Ao Dr. Fabrício eu quero registrar o meu agradecimento, tendo em vista a sistematização brilhante e a iniciativa de massificar a prevenção. Eu queria sugerir, Deputado Rodrigo, que nós e o Dr. Fabrício solicitássemos ao Ministério Público baiano uma consultoria permanente.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Já está acatada a solicitação de V.Exa., Deputada Alice Portugal.

A SRA. DEPUTADA ALICE PORTUGAL - Eu fiquei com medo de ser chamada ao plenário e, por isso, interrompi a fala da delegada, a quem peço desculpa. Mas consegui pegar o conteúdo da sua brilhante ação em Goiás.

Nós não podemos criar disciplinas. Essa é uma decisão do Conselho Nacional de Educação, até porque a toda hora surgem proposições aqui para criar outras disciplinas para o currículo formal dos cursos de segundo grau, de universidades e de institutos federais. Mas nós podemos interferir na inclusão de conteúdos.

Talvez esta seja uma questão fundamental. Nós temos que incluir na escolaridade do jovem brasileiro, em todos os níveis e esferas do ensino, elementos de conteúdo voltados para a prevenção de sua exposição em todos os níveis: dos seus dados pessoais, da sua vida pessoal, da sua família e do seu corpo.

Tudo isso é um processo educativo gradual. Evidentemente, para fazer isso, é importante termos uma consultoria para, junto com a Comissão de Educação, construir, no escopo da CPI, essas orientações para a prevenção.

Eu quero agradecer aos convidados. Realmente, foi uma aula a exposição dos três, dentro das suas áreas e seus âmbitos de atuação. Deixo registrada a sugestão que fiz em relação ao Dr. Fabrício.

Muito obrigada.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Fica acatada a solicitação da Deputada Alice Portugal por parte da sub-relatoria de segurança.

Concedo a palavra aos componentes da Mesa. *(Pausa.)*

Pode ficar à vontade, Dr. Silvio.

Deputada Alice Portugal, gostaria de convidá-la a presidir esta fase de encerramento, por gentileza.

O SR. SILVIO KIST HUPPES - Vou rapidamente responder a estes questionamentos feitos aqui.

A Polícia Civil do Estado do Rio Grande do Sul conta com apenas uma delegacia de polícia, localizada na Capital, que trata desses crimes cibernéticos, mas somente quando eles ocorrem em várias cidades do Estado. Nesses casos, a investigação é feita pela Delegacia de Repressão aos Crimes Informáticos.

Portanto, há um órgão específico, sim, que certamente não está suficientemente aparelhado, nem em termos de equipamento, nem em termos de pessoal. Há um déficit histórico nesse sentido na Polícia Civil do Rio Grande do Sul.

Eu não disse, mas a Delegacia de Polícia de Encantado tem, na verdade, apenas a mim como delegado. Portanto, nós atuamos como uma clínica geral e, às vezes, tratamos também de crimes cibernéticos, principalmente em crimes de estelionato e de furtos, estes já citados, relacionados às contas bancárias. Isso é algo bastante comum. Aliás, lá nós temos o banco SICREDI, em cujo sistema há uma incidência maior de crimes desse tipo.

Em caso de representação ao Poder Judiciário, nós também observamos uma demora média de alguns meses, até recebermos as respostas das operadoras, algo que também dificulta a investigação.

Gostaria de agradecer as palavras da Deputada com relação ao trabalho das Polícias Civis, cuja realidade — falo não só pelo Rio Grande do Sul — é de insuficiência de recursos materiais e humanos. Realmente há um grande esforço no sentido de atender à população. Certamente é muito importante que venha algo deste Congresso, desta Câmara, no sentido de aparelhar ou aperfeiçoar as Polícias Civis, porque nós observamos que esses crimes não têm fronteiras.

Se nós não aparelharmos todos os Estados brasileiros, se apenas um ou outro Estado com uma situação financeira melhor conseguir esse aparelhamento, conseguir policiais, agentes, delegados ou equipamentos, isso certamente não será tão efetivo.

Nós observamos uma realidade muito difícil em vários Estados, especialmente no Rio Grande do Sul. Não há contratação de policiais, não há investimento em equipamentos.

Portanto, o ideal é que se proponha algo que comece na área de segurança pública, sem interferir demasiadamente na atribuição dos Estados, já que as polícias são de competência estadual. Da mesma forma, é preciso propor alguma iniciativa pioneira na área de *cybersegurança*, de crimes cibernéticos, que não tenha relação com qualquer questão partidária, como o já criado Programa Nacional de Segurança Pública com Cidadania — PRONASCI, que investia em segurança pública.

Por fim, aproveito para sugerir que se pense em algo nesta Comissão com relação às Polícias Civis, que são responsáveis pela apuração das infrações penais, e ao Ministério Público, para que não tenhamos, nesses casos, disputas de competência entre o Ministério Público e as Polícias Civis.

Nós temos toda esta questão da investigação, e espero que neste caso haja união de esforços e que este não seja motivo para acirrar eventuais disputas, mas que haja, sim, a valorização das Polícias Civis.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Alice Portugal) - Sou eu que agradeço.

Passo a palavra à Delegada Mayana Rezende, do Estado de Goiás.

A SRA. MAYANA REZENDE - No Estado de Goiás, infelizmente ainda não existe uma delegacia especializada na investigação de crimes cibernéticos. Nós atuamos no Estado inteiro e temos a atribuição de investigar fraudes. Mas como não existe um grupo especializado, nós investigamos muito esses crimes, até mesmo porque são crimes que estão muito em voga e sobre os quais a sociedade cobra muito.

Nós sabemos que a administração tem o projeto, sim, de criar uma delegacia especializada. Mas, infelizmente, o déficit de pessoal é muito grande na Polícia Civil do Estado de Goiás. Então, faz-se o possível. Não adianta tirar de um grupo e

colocar em outro, porque o primeiro também vai precisar. Portanto, nós precisamos de efetivo. Sem efetivo, não tem como mudarmos essa realidade.

Agora, a maior dificuldade que eu vejo na investigação dos crimes cibernéticos é o suporte técnico, que nós praticamente não temos. Todas as apreensões de computadores que fazemos e fizemos inclusive nessa operação — que precisamos para materializar o crime e realmente chegar a uma denúncia e uma condenação —, nós encaminhamos para o Instituto de Criminalística, que é assoberbado de trabalho. E nós sabemos que, se a conclusão de uma investigação depender de um laudo pericial, isso pode não vai acontecer.

Portanto, nós tentamos buscar outros caminhos, como fizemos nessa investigação em que buscamos o caminho do dinheiro, fomos atrás do dinheiro — de onde saiu e onde entrou —, para definir quem eram os autores. Muitas vezes o laudo pericial chega quando o crime até já prescreveu, devido ao volume de serviço do Instituto de Criminalística.

E para investigar o crime cibernético, é preciso contar com uma pessoa ali do lado que tenha esse conhecimento técnico. O conhecimento acadêmico que nós temos está muito aquém dessa tecnologia, desses avanços que não conseguimos acompanhar. Então, nós precisamos casar o trabalho da Polícia Judiciária com esse conhecimento técnico, porque nem sempre o Estado consegue dar esse suporte.

Como o colega Fernando estava falando, realmente eu acho que o caminho é buscar pessoas de fora. Hoje nós sabemos que, se existe perícia oficial em Goiânia, no caso, nós não poderíamos nomear um perito *ad hoc* em tese. E isso atrapalha um pouco.

Mas nós temos buscado fazer, então, cópias desses HDs, temos buscado parceiros dispostos a auxiliar a Polícia Civil, para que a sociedade não fique sem resposta. Foi isso que nós fizemos nessa investigação em que conseguimos ter 100% de êxito e houve 26 indiciados, a maioria deles sem nenhum antecedente criminal.

Em relação aos nossos pedidos ao Judiciário, aqui no Estado de Goiás, ele leva em média 10 dias para atender a um pedido assim. Nós consideramos que esse é um tempo até relativamente rápido, pois sabemos que há colegas em outros Estados que enfrentam maiores dificuldades.

Quanto ao crime organizado, é lógico que quanto mais mecanismos essas pessoas conseguem ter, mais elas se mantêm no anonimato, para ordenar os seus ataques e os seus crimes. Então, é claro que essa tecnologia, esses crimes cibernéticos vão beneficiar o crime organizado de certa forma. Trata-se de mais um mecanismo para o anonimato e para dificultar a identificação de quem está no topo dessas organizações criminosas.

Nós esperamos que, com o tempo, a segurança pública venha a se estruturar melhor, para que tenhamos melhores condições de investigar esses crimes e chegar à identificação de mais autores. Tudo isso, essa noção de que "poucos caem" gera infelizmente uma sensação muito grande de impunidade e acaba virando um incentivo para esses criminosos, até mesmo pelo tanto que já lucraram. Nessa investigação, por exemplo, nós levantamos que o líder chegava a faturar de 80 a 100 mil reais por mês. Isso equivaleria a 65% do que eles conseguiam transferir de forma fraudulenta. E eles dizem: "*Eu caí uma vez e vou conseguir me safar facilmente*".

Essa sensação de impunidade é o que realmente gera indignação na sociedade e em todos nós que estamos do lado de cá. Em nós que fazemos uma investigação dessa monta — que consegue realmente individualizar e colocar na cadeia quem tinha o programa, quem era o operador, quem era o laranja, quem era o agenciador — e depois não vemos uma condenação, uma punição efetiva, isso também acaba gerando frustração.

É claro que isso não chega a ser um desestímulo para o nosso trabalho, muito pelo contrário: nós estamos estimulados e estamos perseverando para que haja efetividade, para que haja uma forma mais eficaz de investigação.

A SRA. PRESIDENTA (Deputada Alice Portugal) - Obrigada, Dra. Mayana. Parabéns pelo trabalho, Delegada Civil do Estado de Goiás.

Passo a palavra ao nosso último convidado, o Promotor do Ministério Público da Bahia, Dr. Fabrício Rabelo Patury.

O SR. FABRÍCIO RABELO PATURY - Estamos encerrando aqui. Primeiro, queria agradecer a todos pela paciência, pela oitiva, pela dedicação. Em nome da Deputada Alice Portugal... Sou testemunha, até por ser seu conterrâneo na Bahia, do excepcional trabalho que a Deputada desenvolve lá. Nós temos sempre que

reconhecer os que fazem muito, e a senhora faz muito pelo nosso Estado. Não é pouco merecido estar aqui representando o nosso Estado, Deputada. Então, parabéns pelo trabalho. Continue desenvolvendo esse trabalho que honra o nosso Estado e aqui, principalmente, na Câmara popular do nosso País.

Quero dizer que todas as instituições têm que se abraçar em tudo. Muito se luta — as instituições individualmente, isso é natural, as instituições procuram sua melhora —, mas nunca podemos deixar de nos completar e entender que fazemos parte desta *res publica*.

É com muita honra que estou aqui e com muita honra estarei quantas vezes a Casa precisar. Estou aqui para ajudar. É com muita honra que aceito o convite e estarei sempre, nem que tire do meu bolso o valor da passagem, porque eu quero sempre estar colaborando com o desenvolvimento do nosso País.

A Casa Legislativa é a Casa do Povo. É daqui que sairão as soluções. Não adianta ficarmos na luta lá quando o Judiciário diz: "*Não, não está previsto em lei. O artigo penal não encaixa*." A Polícia Civil fez o trabalho, o delegado fez o trabalho, o promotor fez o trabalho, mas no final vai cair, porque legislativamente falando não era o que estava previsto, de forma extrínseca, pelo legislador, e o STF vai acabar derrubando, e as impunidades vão sempre permanecer.

A senhora tocou num ponto excepcional: nós acreditamos, veementemente, que a prevenção é a chave dos crimes cibernéticos, pelo menos os crimes cibernéticos impróprios — os próprios não têm como, nós temos que lutar. Mas, para muitos da população, é o único crime contra o qual a pessoa capacitada tem condições de, antes de clicar, antes de aceitar aquele *phishing,* antes de aceitar aquele *spam,* antes de aceitar aquela provocação, aquela engenheira social, parar, refletir e não avançar. Então, se ela estiver preparada e entender que o ambiente virtual não é diferente do ambiente real, não é um Second Life — na verdade, é um único universo em que nós vivemos, é uma nova cultura cibernética —, temos certeza de que estaremos poupando muita repressão posterior.

Eu dizia aqui ao colega que eu vi o *crack* nascer. Eu sou especialista... Na verdade, a minha primeira faculdade foi em Ciência da Computação — por isso também o meu conhecimento. Depois, eu fiz Direito. Especializei-me na área penal, trabalhei nos GAECOs. Hoje subcoordeno a nossa área de Inteligência Criminal e,

ao mesmo tempo, estou na área de crime cibernético. Vimos o *crack* nascer e subestimamos esse nascimento. Nós subestimamos aquela droga pelo desconhecimento, achando que... Enquanto que, talvez, se tivéssemos agido com a prevenção naquele momento, hoje não estaríamos reféns, nos interiores, dessa droga.

Então, o crime cibernético está aí para isso. Ele está nascendo, ainda é incipiente em nosso País, num contexto global e num contexto de estrago. A hora de tentar agir é agora, Deputada. A hora de tentar agir é agora. Devemos tentar atuar na prevenção, atuar na capacitação. Ao mesmo tempo, estruturarmo-nos melhor para tentar reprimir aqueles casos em que a prevenção falhou e chegou até as nossas mãos.

O Deputado Silas me fez uma pergunta sobre a questão eleitoral: *"Como evitar esses crimes?"* Crimes cibernéticos impróprios são inevitáveis, porque é da cultura do brasileiro ser jocoso e é da cultura do brasileiro não saber diferenciar um ataque de uma brincadeira. Então, se é naturalmente assim no dia a dia, nas eleições, com a minha experiência de 5 anos de eleições municipais... A gente inclusive tem que transformar o patamar de injúria num patamar um pouco maior, porque vira efetivamente — vou dizer como na minha época — um Ba-Vi, vira um Boi-Bumbá e um Boi Garantido. É uma disputa em que se divide a população inteira.

Então, os ataques — e até mesmo as conversas de bar — sobrelevam qualquer racionalidade. E a tendência será, no momento em que todos têm agora facilmente um celular, um *tablet*, disparar. Antigamente, como sempre dizem nos congressos, quando se tinha que publicar algo, a pessoa que tinha interesse em publicar tinha que passar por um editor-chefe, o editor-chefe avalizava o filtro, para então publicar na rede social. Hoje todos são jornalistas. Sem filtro, sem medo de olhar para quem está atacando, disparam numa rede social, num *blog*, e, depois, há toda uma dificuldade de conseguir tirar, pela ausência do direito ao esquecimento, pela impossibilidade de proibir os motores de busca, a indexação, pela inviabilidade técnica de tentar apurar, numa velocidade rápida, as amarras construídas.

Embora seja excepcional o Marco Civil, como o doutor disse aqui, é preciso adequá-lo também à nossa realidade penal. O Deputado Silas foi muito feliz nisso aí. Quanto à questão da *dark web*, até o Deputado disse: "*Por que até agora só a*

Polícia Federal?" É porque eles têm um orçamento que facilita, não é falta de capacidade técnica; pelo contrário, os delegados que trabalham... Está aqui o que eles conseguem tirar com o pouco que têm. Capacidade os nossos delegados têm muita. Eu inclusive me sinto honrado por trabalhar ao lado de excepcionais delegados no meu dia a dia. Essas brigas entre Ministério Público e Polícia, eu acho, são mais federais do que estaduais, como estava falando com a colega aqui. Nós somos ombreados nas soluções diárias, no interior, nas capitais. Então, a capacidade é muita, mas a estrutura das Polícias, realmente, precisa ser olhada, precisa ser analisada, porque é o elo fraco da corrente orçamentária. Eles precisam dessa ajuda, sim, de todos nós.

A questão da *dark web* exige muito gasto de tecnologia, porque exige, pelo seu alto grau de "proxiamento", de cascas efetivamente cometidas. A gente chega naquele IP, mas não é aquele IP, está no sétimo IP, no sétimo ponto, precisa utilizar...

Só para terem uma ideia, há um vídeo circulando no YouTube, da Celebrity, que é um equipamento de quebra. Nós, Estados, temos outros não tão poderosos. Mas só para terem uma ideia, por um Celebrity daquele ali só a Polícia Federal tem condição de pagar. Nós utilizamos outros tipos de ferramentas, porque, inclusive lá no Estado da Bahia, ficamos 6 meses sem pagar a licença. Tínhamos a ferramenta, mas não tínhamos dinheiro para pagar a licença. E o Ministério Público acabou fazendo uma colaboração para poder pagar a licença, senão a gente ficaria sem as análises.

Realmente, esse é o elo que precisa do apoio, sim, do Legislativo. A Polícia Civil precisa, sim, ser fortalecida nessas áreas, e a gente tem consciência disso. Devemos enaltecer isso aqui.

Estou aqui à disposição, Excelência.

Há uma pergunta aqui do Deputado Rodrigo: "*Na visão de V.Exa., o Ministério Público está devidamente aparelhado para os crimes cibernéticos?*". Tal como os GAECOs, para nós é muito simples. Para nós, a nossa função é a parte processual. É claro que também envolve perfil. Como eu disse, eu tenho dois conhecimentos: na área da Ciência da Computação e na área do Direito, com especialização em investigação. Então, precisa de perfil, tal como os GAECOs precisam de perfil.

Então, temos. Temos, sim, capacidades, mas só cinco Estados do Brasil têm o NUCCIBER.

Da forma como nós pensamos, que é muito mais em apoiamento, não se... Assim como nós somos contra delegacias especializadas, porque é impossível especializar, porque praticamente todos os crimes do Código Penal têm viés cibernético. Então, vai acabar atraindo todos os crimes para uma única delegacia. É melhor ter uma delegacia que apoie as demais delegacias de bairro e distritais, para que ela dê o *know-how* e ela possam melhor se capacitar, para poder, em parceria com as delegacias distritais e de bairro, avançar nos crimes cibernéticos. A melhor formatação, eu acho, é essa. Inclusive foi essa que os NUCCIBERs — o primeiro NUCCIBER do Brasil foi o de Minas Gerais... E eles já mudaram, inclusive, como nós também mudamos, para dar o apoiamento ao colega de atividade finalística, porque, senão, nós estaríamos fazendo o *juris*, nós estaríamos fazendo tudo, porque o NUCCIBER atrairia todas as competências. E não é natural do Direito Penal a competência ser atraída pelo *iter criminis*; ou é pela pessoa, ou é pela matéria. Então, não se atrai competência pelo *iter criminis*.

"Qual é a importância, na sua visão, do núcleo específico?" É importantíssima por isto: porque é uma matéria nova, precisa de pessoas com perfil para poder colaborar com as demais.

E a última que o Deputado me pediu aqui — as demais vou responder por escrito: "*Qual é a prática de delito que tem mais acontecido, com frequência, nos meios virtuais?"* Aqui no Brasil, os crimes cibernéticos impróprios, mas chama a atenção hoje a grande, vamos dizer assim... Crimes patrimoniais são muitos? São muitos, mas são patrimoniais. Os crimes contra a pessoa são os que mais têm causado problemas, principalmente às mulheres. É preciso ter um olhar mais atencioso aos crimes contra a pessoa, notadamente as mulheres, crimes cibernéticos, porque estão causando mortes, estão causando suicídios, estão causando depressões, e o tipo penal de longe chega ao alcance da perniciosidade da atitude.

Ficam só essas aí. As demais, eu me ponho à disposição para responder. Obrigado a todos novamente.

A SRA. PRESIDENTA (Deputada Alice Portugal) - Nós é que agradecemos, em nome desta CPI. Tem sido um aprendizado muito grande. Eventualmente, é claro, o ambiente político é também conduzido aqui para o nosso colegiado, mas é uma CPI, que é formada por uma Presidente, pelos sub-relatores, sempre por Deputados muito jovens e muito afeitos à utilização dessas ferramentas. Isso tem sido muito útil, também, para essa construção, na minha compreensão. É claro que cada contribuição aqui teve um enorme valor, porque, na ponta do sistema, o valor é o da construção da prevenção. Eu acredito muito que possamos sair desse trabalho, digamos, com um conteúdo que possa colaborar e enriquecer o Marco Civil da Internet, que também nasceu com um grande trabalho desta Casa.

Quero lembrar o papel da Deputada Manuela D'Ávila, do Rio Grande do Sul, nessa discussão, que foi fundamental, até porque é alguém que usa, em grande escala, as redes sociais para o seu trabalho, como jovem política e mulher. Isso também tem um rebote. Foi um momento muito especial da Câmara dos Deputados.

Eu gostaria muito de agradecer ao Promotor Fabrício Rabelo Patury e à Delegada Mayana Rezende, do Estado de Goiás; ao Delegado Silvio Kist Huppes, da cidade de Encantados, do Rio Grande do Sul; e ao já ausente, por motivos de viagem, analista Fernando Mercês.

Nada mais havendo a tratar, quero agradecer à Consultoria. Acho que os consultores, talvez, terão um trabalho nesta CPI que, se comparada a outras, vai ser gigante, gigante na busca de um afunilamento de soluções. Acredito que esta Mesa tenha sido muito útil nessa construção. Agradeço aos consultores, à imprensa, aos assessores presentes.

E nada mais havendo a tratar, declaro, em nome da Presidenta Mariana, encerrada a presente reunião, antes convocando reunião ordinária da Comissão para a próxima terça-feira, dia 24 de novembro, às 15 horas. Hoje, não houve a apreciação de requerimentos, mas eles serão apreciados na próxima reunião do dia 24 de novembro.

Declaro, portanto, encerrada a presente reunião.

Muito obrigada.