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: 1623/15	DATA: 03/09/2015	
LOCAL: Plenário 11 das Comissões	INÍCIO: 10h14min	TÉRMINO: 13h42min	PÁGINAS: 80

DEPOENTE/CONVIDADO - QUALIFICAÇÃO

EDUARDO LEVY CARDOSO MOREIRA - Presidente do Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal — SINDITELEBRASIL.
MARCOS VINÍCIUS FERREIRA MAZONI - Diretor-Presidente do Serviço Federal de Processamento de Dados — SERPRO.
RENATO MARTINI - Diretor-Presidente do Instituto Nacional de Tecnologia da Informação — ITI.
CRISTINE HOEPERS - Gerente-Geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil — CERT.br.

SUMÁRIO

Debate acerca da gestão e da regulamentação da Internet no Brasil.

OBSERVAÇÕES

Houve exibição de imagens.
Houve intervenção fora do microfone. Ininteligível.
Há palavra ou expressão ininteligível.
Há falha na gravação.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Declaro aberta a 9ª Reunião Ordinária da Comissão Parlamentar de Inquérito que investiga a prática de crimes cibernéticos.

Comunico o recebimento dos seguintes expedientes, já deferidos pela Presidência da Casa:

Ofício nº 363, de 2015, da Liderança do PR, que *"retira a indicação de membro titular do Deputado Cabo Sabino".*

Ofício nº 582, de 2015, da Liderança do PT, *que "indica a Deputada Margarida Salomão para ocupar uma vaga de suplente"*.

Ofício nº 84, de 2015, da Liderança do PSOL, *que "indica o Deputado Edmilson Rodrigues para uma vaga de suplente".*

Esta audiência pública conta com a participação de entidades que participam da gestão e regulamentação da Internet no Brasil: o Serviço Federal de Processamento de Dados — SERPRO; o Instituto Nacional de Tecnologia da Informação — ITI; o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil — CERT.br, órgão do Comitê Gestor da Internet; e o Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal — SINDITELEBRASIL.

A audiência decorre da aprovação do Requerimento nº 10, de 2015, de autoria do Sr. Deputado Daniel Coelho, do PSDB de Pernambuco, dos Requerimentos nºs 14 e 17, de 2015, de autoria do Deputado João Arruda, e do Requerimento nº 29, de 2015, de iniciativa da Deputada Alice Portugal.

Gostaria de mais uma vez agradecer a presença das pessoas que acompanham os trabalhos da CPI e dos convidados que atenderam ao chamado da CPI e se dispuseram a colaborar com a realização desta audiência.

Convido para compor a Mesa o Sr. Eduardo Levy Cardoso Moreira, Presidente do SINDITELEBRASIL *(pausa)*; o Sr. Marcos Vinícius Ferreira Mazoni, Diretor-Presidente do SERPRO *(pausa)*; o Sr. Renato Martini, Diretor-Presidente do ITI *(pausa)*; e a Sra. Cristine Hoepers, Gerente-Geral do CERT.br, órgão do Comitê Gestor da Internet. *(Pausa.)*

Solicito a atenção de todos para os procedimentos que iremos adotar nesta audiência. Cada convidado disporá de 15 minutos para sua apresentação. Lembro

que não deverá haver apartes. Ao final das exposições, será passada a palavra ao Relator, aos Sub-Relatores e aos autores dos requerimentos. Os convidados responderão a esse bloco de indagações. Em seguida, respeitada a lista de inscrição, os senhores membros poderão interpelar os convidados por até 3 minutos. Os expositores responderão às indagações desse bloco de inscritos, podendo haver réplica. Por fim, haverá as considerações finais.

Feitos esses esclarecimentos, vamos iniciar a nossa audiência.

Concedo a palavra ao Sr. Eduardo Levy Cardoso Moreira, Presidente do Sindicato Nacional das Empresas de Telefonia e de Serviços Móvel Celular e Pessoal — SINDITELEBRASIL.

O SR. EDUARDO LEVY CARDOSO MOREIRA - Bom dia a todos. Muito obrigado pelo convite.

Eu vou fazer uma exposição bastante rápida e acredito que atenda ao tempo previsto.

(Segue-se exibição de imagens.)

Primeiro, quero passar alguns números do setor de telecomunicações.

Nós temos hoje 281 milhões de *chips* ativos no Brasil e 220 milhões de acessos em banda larga. Em 2014, investimos 32 bilhões de reais. Este é o setor de infraestrutura que mais investe no Brasil, há 15 anos. Também temos 45 milhões de telefones fixos e 20 milhões de tevês por assinatura. E somos um dos grandes recolhedores de impostos no País. Em 2014, recolhemos 60 bilhões de reais em tributos.

A Constituição Federal diz em seu art. 5º que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer. E a Lei nº 9.296, de 1996, em seu art. 10º diz claramente: *"Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei".*

Eu queria agora me fixar bastante neste desenho que está aqui e tentar fazer um paralelo com a evolução das telecomunicações ao longo do tempo.

Eu iria começar pelo exemplo de uma determinada data, até que, de manhã, a Cristine comentou comigo sobre o telégrafo. Quando o telégrafo existia — perdoe-me usar os dados —, ele era muitas vezes utilizado para passar informações sigilosas da época, até questões de guerra. E telecomunicação, ou aquilo que prestava o serviço, nada mais era do que o fio que levava essa informação. Um pouco disso continuou depois com o telefone: também um fio leva a conversa, seja para dar os parabéns a alguém, seja para combinar um crime.

Depois disso, nós temos outros tipos de comunicação, como, por exemplo, a radiodifusão, em que o meio é levado por telecomunicação, como no caso da tevê por assinatura, mas também esse conteúdo não tem nada a ver com aquilo que eu estou representando aqui hoje. E é até bom que assim seja, pois nós não podemos conhecer, de forma nenhuma, o que está no conteúdo daquela informação. Somos apenas — talvez uma parcela das mais importantes — um caminhão que transporta caixas cujo conteúdo nós desconhecemos, inclusive por força legal, e tem que ser assim mesmo. E muitas vezes, por uma informação ou um conhecimento legal, somos orientados, somos solicitados, conforme aquilo que foi falado da lei de 1996, a não entregar o pacote que está dentro daquele caminhão. No caso da Internet, é "pacote" mesmo o título. Enfim, nós somos o caminhão que leva a informação, porém não sabemos o que está dentro dele.

O nosso pacote carrega vídeo, a exemplo do Netflix; carrega comércio, feito por Submarino, Amazon, Magazine Luiza, etc.; carrega educação, em portais de universidades; carrega serviços públicos como passaportes, certidões; carrega entretenimento, a exemplo do Youtube. Nós somos o instrumento pelo qual essas informações chegam aos usuários, e temos que zelar para que essas informações sejam mantidas invioláveis pelas atividades que nós prestamos. Não podemos ter acesso ao conteúdo dessas informações. Mal comparando, dois motoristas de táxi levam pessoas para um mesmo local: uma delas vai participar de uma festa, a outra vai preparar um assalto àquela mesma festa. O motorista do táxi não conhece o conteúdo, não conhece a pessoa que ele está transportando naquele momento. Nós somos esse táxi, somos o motorista do táxi. Nós apenas transportamos essas informações.

Isso tem nome: nós somos provedores de acesso e conexão, não somos provedores de aplicação e conteúdo. Nós oferecemos o acesso para a infraestrutura de navegação, apenas transportamos os dados. Já os provedores de aplicação são aqueles que colocam as mercadorias dentro dos pacotes, que nos são entregues fechados, etiquetados. Nós não sabemos, mas eles sim sabem o que foi colocado ali dentro. E boa parte dessas empresas atua fora do Brasil, de forma quase virtual, muitas vezes não gerando nenhum emprego, muitas vezes não tendo sequer CNPJ no Brasil.

Nenhuma empresa operadora fornece ou facilita informações que possam quebrar o sigilo. Isso vem de uma história longa.

E nós temos, por uma outra característica, que manter dados no País. Então, todos aqueles dados que nós utilizamos para transportar essas mercadorias são guardados e armazenados por um período de tempo estabelecido pela legislação e ficam à disposição da Justiça para o caso de serem solicitados.

É sempre importante lembrar que o que nós guardamos não é aquilo que foi carregado no pacote do caminhão, por dentro. Nós não sabemos o que é aquilo. Mas nós sabemos que um caminhão levou uma mercadoria de um ponto para outro ponto. Essa informação é guardada e armazenada por um período. O que havia dentro dessa mercadoria eu não faço ideia do que era, nunca pude vê-la, não devo vê-la, sou proibido de vê-la, eu apenas a transporto de um ponto a outro e tenho essa informação.

Fazendo uma analogia com a telefonia, que talvez seja mais simples, nós guardamos todas as informações de uma ligação de um telefone para outro: quando foi feita a ligação, quanto tempo ela durou, de que horário a que horário foi feita. O que conversaram eu não sei, nunca soube, não saberei, não posso saber, sou proibido de saber, e é bom que assim seja.

Essas informações que nós guardamos, elas têm acesso restrito, e, mais importante do que o acesso restrito, os acessos são rastreáveis. Então, toda vez que nós acessamos uma informação que é restrita e está guardada, a informação só pode ser dada a quem a solicitou.

Nosso histórico é de anos e anos, desde o telégrafo, talvez. A telefonia mostra que nós temos uma credibilidade em inviolabilidade da intimidade, da vida

privada e do sigilo de comunicações dos usuários. Estamos aqui falando dos crimes cibernéticos, e a questão é, em tese, a mesma da telefonia. A telefonia é mais fácil de entender, mas ela tem toda a complexidade da rede de Internet. A rede de Internet, ela foi montada de forma a garantir inúmeras vantagens à sua utilização, ao se ter a confiabilidade dos dados que nela são trafegados, que podem ser recuperados, passados de um ponto a outro. E, em contrapartida, há certas dificuldades na obtenção de conhecimento do que estava ali dentro.

Mas vamos fazer uma comparação com a telefonia. Muitas vezes nós recebemos uma solicitação para buscar dados de um determinado número telefônico. E nós fazemos isso. Se porventura é solicitado por órgãos policiais que se dê a partir daquele momento conhecimento do conteúdo daquela informação, também de uma forma correta, a nosso modo de ver, porque isso dá garantias à sociedade como um todo, nós simplesmente transferimos a capacidade de obtenção do conteúdo para o órgão policial que o solicitou. Em nenhum momento, mesmo quando há solicitação de conhecimento do conteúdo da informação por um órgão policial ou por um órgão de Justiça, o setor de telecomunicações pratica essa atividade. Não, ele simplesmente desloca a informação para um ponto solicitado, onde os órgãos de Justiça e os órgãos policiais fazem o conhecimento, fazem a escuta, etc. Então, também não há por parte das empresas de telecomunicação conhecimento daquilo que está sendo solicitado pela Justiça, em nenhum momento, o que também é bom para o País. Nós simplesmente bloqueamos, no caso da Internet, os endereços IPs, bloqueamos as URLs, fornecemos os dados dos usuários e desviamos o pacote de dados para a autoridade policial. Nós informamos esses dados. Não armazenamos nada que tenha a ver com o conteúdo. Nunca! Nunca. Nós apenas guardamos a etiquetinha que foi colocada num pacote: saiu do endereço A, foi para o endereço B. Raciocinando com telefonia, talvez seja fácil de entender o processo e as dificuldades que existem muitas vezes.

A intenção que se tem ao buscar informação nas empresas é, obviamente, conhecer o conteúdo, para poder agir, e é necessário que assim se faça. Então, muitas vezes, na telefonia, quando se pede para bloquear ou para desviar a informação de um telefone, eu posso simplesmente, se por algum motivo eu tenho conhecimento de que alguma coisa foi feita, posso combinar aquele crime, fazer

aquela conversa através de outro número. Então, muitas vezes, quando é feito o pedido de bloqueio de um determinado IP... O endereço IP nada mais é do que um conjunto de números ou de informações único, como é único um número telefônico, no mundo inteiro. Este número aqui é único, não existe outro igual no mundo. Se me pedirem para bloquear este número, eu bloqueio este número. Se me pedirem para bloquear um determinado IP, se as empresas receberem esse pedido, elas bloqueiam esse IP, e nada por esse IP ou por esse número passa na rede. Mas aquilo que foi colocado dentro do pacote pode ser encaixado em outra caixa, em outro pacote, e transmitido por outro IP, por outro número. Não temos como saber disso.

Então, muitas vezes, a ação nos nossos IPs, nos nossos números, ela é eficaz sob o ponto de vista daquilo que nos é solicitado, mas não necessariamente é eficaz a ponto de impedir que a informação continue trafegando na rede, porque pode-se utilizar outro instrumento, que nós vamos deixar passar livremente na rede, porque não sabemos o que está dentro do conteúdo de outros IPs. Nós só bloqueamos o IP que nos é solicitado. Se o conteúdo de uma caixa é um brinquedo de criança, isso nós não sabemos. Se mandam impedir a entrega daquele pacote, nós seguramos o pacote, ele não trafega na rede. Mas se alguém depois pegar um segundo brinquedo igualzinho e colocá-lo em outra caixa, pode transmiti-lo através de outro IP. Ele vai passar na nossa rede. A rede vai deixar trafegar aquilo que não é objeto de bloqueio, e, por força da legislação, do Marco Civil da Internet, ela tem que tratar igualmente os pacotes que ali passam, com exceção das solicitações da Justiça.

Eu adiantei que o bloqueio do IP não impede que este mesmo IP seja modificado e que o conteúdo seja acessado em outras redes. Então, para que a restrição seja efetivamente total, é necessário que aquele que tem o conhecimento da informação é que a restrinja.

Há um exemplo interessante que gostaria de compartilhar com V.Exas., um caso público de solicitação do Ministério Público Federal a respeito da interceptação de um determinado aspecto, e no caso não foi nem o IP. Foi o seguinte: a um determinado *site* foi solicitado que fosse bloqueado tudo que era trafegado daquele *site.* Sem ter conhecimento do IP, fizemos uma varredura na rede. Os senhores

imaginem a dificuldade natural disso. Tomamos as providências devidas. Porém, logo depois o próprio MP determinou que fosse solicitado ao país tal, via Departamento de Recuperação de Ativos da Secretaria Nacional de Justiça do Ministério da Justiça, a retirada provisória da Internet do *site* X, ou Y ou Z, hospedado naquele país.

Nós procuramos segurar dentro da rede brasileira todos os IPs conhecidos de acesso. Mas, se depois, 1 semana, 10 dias, for acessado de outra forma, ele está no outro país. Só dá para ser feito se for retirado daquele país. Então, a complexidade das questões é muito maior do que efetivamente podemos observar, e muito mais será se nós tivermos o entendimento de que o bloqueio do IP feito numa rede brasileira vai fazer com que não se possa mais acessar aquela informação.

O Marco Civil da Internet também coloca determinadas questões de que já falei aqui de que ele obviamente tem, e está na lei, e é bom que esteja assim... Quer dizer, a rede não é responsabilizada pelo conteúdo do que é trafegado nela. Ela carrega, eu já tinha falado. E também nos veda o bloqueio de pacotes. O que tem uma visão perfeita. Quer dizer, não cabe à empresa de telecomunicações impedir, por visão dela, o tráfego de determinados dados. O espírito ali colocado é para fazer com que haja por parte de todos aqueles que colocam as informações na rede igualdade de acesso de todos. Isso é bom, mas gera certa dificuldade natural ao se observar o conteúdo.

O Marco Civil também nos obriga a guardar por um período de 1 ano os registros de conexão que nada mais são do ponto A para o ponto B e a adotar procedimentos que garantam mais uma vez o sigilo e a privacidade dos dados. Mesmo assim, nós temos procurado trabalhar, porque a empresa está dentro da sociedade brasileira, tem que contribuir com tudo aquilo que vá em benefício dessa sociedade e procure ajudar naquilo que possa ser exatamente o oposto: cartilhas de segurança sobre o uso da Internet, em parceria com a OAB; *links* em nossos *sites* para denúncias de crimes, campanhas de combate à pedofilia, com divulgações em contas, cartões telefônicos nos *sites*, etc.; criação de processo de internos permanentes. É uma operação extremamente complexa e cara que existe dentro das empresas de telecomunicações para combate aos crimes cibernéticos.

O que é essa operação? É algo que trará segurança para a comunidade, de tal forma que aquilo seja feito num ambiente de maior segurança possível dentro da empresa. Por outro lado, que seja algo que ocorra o mais rápido possível para se dar uma resposta, a mais rápida, para a sociedade. É muito simples interromper um *chip* de celular de trafegar na rede. É muito complexo muitas vezes. É muito complexo, muitas vezes, conseguir atender a solicitações que vêm mais vagas. Por favor, não, tem que não deixar cursar tráfego de determinado *site*, como foi o exemplo que eu dei. Isso exige uma pesquisa muito grande, porque não vem identificado o IP para onde ele trafegue, e mesmo assim ela pode não ser totalmente segura sob o ponto de vista daquilo que foi necessário.

Obviamente, nós agimos dentro da lei, o que é muito importante, porque veio uma história na época... Os senhores se lembram do caso de Edward Snowden. Nós não temos nenhuma parceria com órgãos estrangeiros, não realizamos nenhuma escuta nem acesso de dados. Como eu expliquei, toda e qualquer ação de escuta ou de informações de conteúdo são desviados para os órgãos que nos solicitaram, e eles sim procedem ao conhecimento do que ali é trafegado.

Nós repudiamos, como não poderia deixar de ser, qualquer tipo de crime cibernético e procuramos colaborar o mais ativamente possível com todos os órgãos policiais.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Dr. Eduardo Levy Cardoso Moreira.

Concedo a palavra ao Sr. Marcos Vinícius Ferreira Mazoni, Diretor-Presidente do Serviço Federal de Processamento de Dados — SERPRO.

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - Bom dia a todos e a todas. Quero agradecer à Deputada Mariana Carvalho o convite e ao ilustre Deputado João Arruda, o requerimento para estar aqui.

Eu quero fazer duas introduções antes da minha apresentação.

Minha militância na área é antiga. Eu fui projetista de central telefônica no Estado do Rio Grande do Sul, implantei as primeiras centrais digitais no Brasil — a segunda central de telefonia celular, em Porto Alegre —, fui presidente da empresa de informática do Estado do Rio Grande do Sul, no Governo Olívio Dutra, e

presidente da empresa de informática do Estado do Paraná, no Governo Roberto Requião. Estou há 8 anos e meio no SERPRO. Nós vimos acompanhando há bastante tempo todo esse debate.

A segunda introdução que eu quero dizer é que nós atuamos no sentido de como fazer uma simetria com uma seguradora. Então, as questões que vou colocar aqui nós chamamos de vulnerabilidade. O que nós queremos dizer com isso? Nós não estamos dizendo que essas coisas acontecem, estamos dizendo que podem acontecer e que atuamos a partir das possibilidades de acontecimento. O que nós chamamos, então, de vulnerabilidades.

Vou passar rapidamente o que são vulnerabilidades no nosso entendimento nos mais diferentes ambientes e como procuramos atuar. Então, vamos falar das nossas atuações em cima dessas possíveis vulnerabilidades.

No Governo Federal brasileiro, há mais de 20 anos, existe uma divisão de responsabilidades sobre essa questão de proteção cibernética do País. Existe o Centro de Defesa Cibernética, de responsabilidade do Exército Brasileiro, no sentido da defesa do País, dos nossos patrimônios que podem ser vigiados através do uso de recursos cibernéticos. Isso é de responsabilidade do Exército Brasileiro. Existe a segurança institucional do Governo brasileiro, de responsabilidade do Gabinete de Segurança Institucional da Presidência da República, que atua de forma global.

Ao SERPRO, a maior empresa de tecnologia da informação do Governo Federal — não é a única —, cabe a responsabilidade de segurança da informação. Nós temos base de dados, serviços importantíssimos para o cidadão brasileiro, para a sociedade brasileira. Por exemplo, nós fazemos todo o trabalho do Imposto de Renda, tanto de pessoa física quanto de pessoa jurídica, e essas bases precisam ser protegidas.

É claro que a grande maioria das bases em que atuamos deve ser de conhecimento público. Nós atuamos, por exemplo, em todo o orçamento da União. Isso, quando consagrado, ou seja, quando liquidado, são bases e informações abertas, não há nenhum problema de serem observadas. Nós protegemos o processo e depois isso tudo vira informação aberta. A grande maioria das informações em que atuamos deve ser sim de acesso universal, e não de acesso restrito. As informações individuais, tanto de pessoas físicas quanto de pessoas

jurídicas, essas sim são informações que nós protegemos, porque aí há sigilo fiscal, sigilo bancário, que envolvem a cidadania brasileira.

Então, o que eu vou colocar aqui para os senhores é um pouco do que estamos fazendo em cima das nossas vulnerabilidades. Acho que Levy Cardoso colocou aspectos muito importantes. Eu resumiria inclusive dizendo que foi um grande debate naquele momento do Marco Civil, que era a questão da neutralidade da rede, o que comprova tudo o que Levy Cardoso colocou aqui.

A rede é neutra, ela não pode abrir os pacotes para saber o que tem dentro. Se ela não tivesse neutralidade, poderia abrir pacotes para ver se esse tráfego passa ou não e aí violaria o sigilo da informação. Esta era a preocupação que tínhamos à época com a neutralidade da rede: exatamente a rede não poder abrir pacotes e fazer a discriminação de algum tipo de tráfego. Essa discriminação é feita hoje pela velocidade, simplesmente pela velocidade: se eu contrato mais velocidade, eu posso trafegar com pacotes maiores; se eu contrato menos, vou trafegar com pacotes menores.

(Segue-se exibição de imagens.)

O que colocamos como vulnerabilidades nos diferentes ambientes em que nós atuamos: nós atuamos na rede mundial de computadores, que é a Internet mundial; nós temos a rede do Governo, que vai ter vulnerabilidades; nós temos a nuvem, tanto do Governo quanto externas, em que atuamos; nós temos vulnerabilidade em centros de dados; nós temos as aplicações do Governo, que é o ponto mais crítico em que atuamos; e nós entendemos também que, no processo de comunicação, há possibilidade de vulnerabilidade. Eu vou passar um pouquinho sobre cada uma delas.

Na rede mundial de computadores, há uma concentração muito grande da governança da Internet em ambientes fora do Brasil, muito embora o comitê gestor tenha feito um excelente trabalho nesses 20 anos — comemoram-se 20 anos exatamente este ano —, trazendo governança cada vez mais para dentro do nosso País, o que é um trabalho importante. Mas nós ainda temos muita governança de Internet fora do País. E isso é natural, é assim que vai continuar sendo, só que nós precisamos tratar desses elementos como vulnerabilidades.

Redes físicas de cabos e satélites. Eles possuem vulnerabilidades. Há possibilidade de rastrear cabos de fibra ótica, por exemplo, por indução. Então, nós temos que cuidar também das redes físicas e satélites, quanto as suas vulnerabilidades.

Redes lógicas, como roteadores, servidores, endereçadores, os DNS — *domain name system*. É como descobrimos esses endereços. Então, isso tudo são pontos de possíveis vulnerabilidades.

Predominância de armazenamento de dados sob legislação estrangeira. Não só o uso dos bancos de dados fora do País, como os *softwares* e até mesmo os *hardwares* que armazenam esses bancos de dados terem obediência à legislação estrangeira. Nas licenças de vários produtos está escrita inclusive a cláusula de proteção do Governo norte-americano, por exemplo, que garante a ele o acesso absoluto àqueles bancos de dados, mesmo que esse produto tenha sido comprado por nós, esteja instalado nos nossos centros de dados, o produto garante a possibilidade de acesso a qualquer momento, basta um pedido do Governo norte-americano. Isso está escrito nas licenças dos produtos.

Então, também temos que cuidar desse tráfego de saída que temos no nosso ambiente. Muitas vezes protegemos o tráfego de entrada, mas nos esquecemos de proteger o tráfico de saída. Portanto, esses produtos têm essa capacidade que chamamos de *backdoor*. Os chamados *backdoors*, são essas proteções do fabricante, especialmente norte-americano, que tem essa legislação. Fabricantes chineses também têm esse tipo de licença. Ou seja, está escrita na licença essa autorização prévia ao Governo norte-americano.

Como procuramos atuar nisso? Quais são nossas ações contra essas vulnerabilidades? Um protagonismo do Brasil na governança da Internet. Eu mencionei aqui o comitê gestor, e temos feito, como Governo, a proposta de que o comitê gestor internacional tenha a mesma característica do comitê gestor brasileiro, que é um exemplo para o mundo todo, é multissetorial e tem a participação de vários agentes do processo da Internet. Essa é a ideia. Existe uma entidade gestora da Internet mundial, que se hospeda na Califórnia, Estados Unidos, e já há uma evolução no debate para que venha a ser em Genebra. Nós ainda não conseguimos

avançar na multissetorialidade do comitê gestor da Internet mundial. Mas essa é uma das nossas propostas.

A outra questão aqui é distribuição geográfica e política de *cores*, de servidores. Nós hoje temos uma troca de tráfego baseada no nosso ambiente. As operadoras têm bastante troca de tráfego baseada no Brasil. Mas ainda existem alguns outros pontos de troca de tráfego, especialmente quando lidamos com tráfego de telefonia celular de diferentes operadoras — quando o tráfego é da mesma operadora no Brasil, todas fazem trocas de tráfego no Brasil —, fora do território nacional. Esse, portanto, é um ponto de vulnerabilidade. Isso não significa que aconteça alguma coisa, mas é um ponto de vulnerabilidade.

Instalações de mais cabos de conexão de rede no continente e em ligação com outros continentes.

Por isso o projeto do cabo de fibra ótica que liga o Brasil não só aos Estados Unidos, mas diretamente à África e à Europa. Esse é um projeto de que não só o Governo participa, mas operadoras brasileiras participam também, no sentido de que o nosso tráfego, muitas vezes, antes de ir para a Europa, tenha que passar por um roteamento nos Estados Unidos, por exemplo.

Desenvolvimento de satélites.

O Brasil está fazendo todo o trabalho de lançamento satélite. Vai estar em operação até o final do ano que vem um satélite brasileiro com foco na Internet. Os satélites que nós temos hoje não são focados em Internet. Então, eles não têm uma boa *performance*. O pessoal da área de segurança tem uma frase de que eu gosto muito. Eles dizem que são contrários a tudo o que nós pensamos no que diz respeito ao uso da tecnologia da informação. Quando nós pensamos em usar a tecnologia da informação, nós queremos *performance*, nós queremos velocidade, nós queremos muita facilidade. O pessoal de segurança, quando atua, cai a *performance*, porque eles entram com elementos, inclusive, restritivos, o que é natural.

Então, a ideia do satélite é nós podermos ter uma segurança maior, mantendo *performance*, mantendo velocidade. Isso está sendo trabalhado pela TELEBRAS.

E o fortalecimento do CGI, que é o Comitê Gestor de Internet Brasileiro, que vem fazendo esse trabalho e é referência mundial. Nós temos acompanhado a comemoração dos 20 anos, as palestras todas que estão sendo feitas por vários

construtores da Internet mundial, e temos visto que eles acham que é uma boa referência até mesmo para a governança internacional.

Na nossa própria rede de Governo, nós temos várias vulnerabilidades também. Uma delas é a predominância de redes de operadoras de telecomunicações.

Quando nós usamos a camada de transporte das operadoras, o.k., os pacotes estão completamente fechados, como o Levy já colocou aqui. Mas muitas vezes nós usamos roteamentos que podem até acontecer fora do território nacional. Então, o nosso foco depois vai ser continuar usando as operadoras de telecomunicações, mas ter cada vez mais capacidade de inteligência em roteamento.

Dados não criptografados.

Não se usa de forma intensa a criptografia, porque, exatamente, perde a *performance*. Nós acabamos usando pouco a criptografia, apesar de termos essa tecnologia, essas facilidades. Como o uso da criptografia tira a *performance*, nós acabamos nos desprotegendo, muitas vezes. É muito natural nós trocarmos *e-mails* não criptografados.

Fragilidade de segurança nos *softwares, esses backdoors,* que nós temos nas nossas instalações.

Nós temos os nossos centros de dados, mas usamos produtos que têm legislação internacional e que têm *backdoors,* ou até mesmo aqueles que não têm legislação internacional, mas que nós sabemos que possuem *backdoors* introduzidos por *softwares* até mesmo após a sua comercialização.

Exposição de roteadores de borda.

Nós fazemos uma grande proteção do ambiente central da nossa rede, que nós chamamos de core, mas, se nós vamos falar lá na ponta, vai passar por um roteador que pode estar num pequeno provedor local, pode estar até mesmo dentro das nossas instalações e que tenha também *backdoor.*

Domínio da infraestrutura e das aplicações usadas por empresas privadas.

Nós usamos muitas soluções que são fechadas e que nós não conhecemos como efetivamente operam. O que nós fazemos com isso? Nós temos uma infraestrutura pública de comunicação. No caso de Brasília nós temos a INFOVIA,

uma rede de fibras óticas do Ministério do Planejamento, gerida pelo SERPRO, e nós interligamos todos os Ministérios. Estamos tratando do core. É claro, entretanto, que esses Ministérios têm atuação nacional. Portanto, nós vamos ter aquelas bordas lá, chegando com algum nível de fragilidade. Mas pelo menos no nosso ambiente interno de Brasília nós temos INFOVIA.

Em algumas cidades nós também temos INFOVIAs, como, por exemplo, no caso de Porto Alegre, que tem uma INFOVIA própria. Estamos instalando INFOVIA própria agora no Estado do Pará. Nós temos uma parceria de INFOVIA no Rio de Janeiro. Estamos construindo uma parceria de INFOVIA em Curitiba. Então, nós estamos aumentando um pouco as nossas parcerias junto com a TELEBRAS para ter a borda um pouco mais protegida também.

Gestão, monitoramento e auditoria pelo Governo. Nós fazemos a gestão do tráfego sainte, exatamente para nos proteger. É muito natural que nós falemos das proteções do tráfego entrante. Todo mundo sabe que nós, no SERPRO, por exemplo, naqueles 3 meses de Imposto de Renda, é natural que venhamos a ser bombardeados por tentativas de invasão, de ataque ou, até mesmo, de simples negação de serviço, os chamados “DDoS”. Nós chegamos a ter alguns *petabytes* de tentativa de ataque nos períodos de Imposto de Renda, que basicamente nós entendemos como diminuir a nossa *performance,* para que nós tenhamos, talvez, até uma necessidade de prorrogação de prazo, coisa que felizmente nunca aconteceu — nós nunca chegamos a ter mais do que 65% do nosso ambiente de rede ocupado nos picos dos dias de entrega de declaração de Imposto de Renda, que chegam a 3 milhões num dia.

São 28 milhões de declarações totais no Brasil. Para os senhores terem uma ideia, a Inglaterra faz isso numa janela de 12 meses, e nós fazemos numa janela de 3 meses. Eles sempre perguntam como é que nós conseguimos fazer isso em tão pouco tempo, com esse padrão de *performance.* Isso é possível porque nós fazemos uma coisa muito simples também: nós entregamos para o cidadão brasileiro, para o contribuinte, um *software,* e ele faz a declaração no seu computador. Portanto, eu estou usando a capacidade computacional de cada contribuinte. Então, o meu grande processamento, no dia da entrega, é exatamente rede; é receber esses pacotes. A Inglaterra faz com máquina aberta. Portanto, eles

processam instantaneamente, e nós processamos à noite. Em compensação, nós fazemos a devolução no próprio ano, porque fechamos toda a malha 3 dias após o final da entrega, e eles fecham a malha em 6 meses e fazem devolução no ano seguinte ao da entrega das declarações, enquanto nós fazemos no próprio ano.

Outro país que faz no próprio ano é a Letônia. Mas a Letônia tem 3 milhões de contribuintes, e nós temos 28 milhões de contribuintes. Além disso, a Letônia é um país completamente novo. Então, tem toda uma estrutura nova. Nós temos uma história. O SERPRO tem 50 anos de história. Então, nós temos que lidar com plataformas diferenciadas.

Protocolos de segurança da informação seguros e livres.

Nós trabalhamos com protocolo somente de código de *software* aberto, *software* livre, para que possamos ter controle absoluto de como esses códigos funcionam na rede. Não adianta também eu ter um *software* de proteção que é fechado, que é dominado, por exemplo, pela NSI. É muito comum isso acontecer. Então, nós usamos *softwares* de proteção de código aberto, de *software* livre.

O *hardware* nacional no core da rede.

Amanhã, inclusive, junto com a Universidade Federal do Pará, lançaremos uma máquina que supervisiona todas as redes em cima de *softwares* de código aberto, chamado *OpenFlow*, com um *software* todo desenvolvido na Universidade do Pará. Então, nós temos essa infraestrutura.

Temos, com a Universidade Federal de Santa Catarina, um trabalho importante de criptografia. É nossa parceira já há muitos anos. Nós temos um trabalho de longa data com a Universidade Federal de Santa Catarina para fazer toda a parte de criptografia.

Temos uma parceria importante com a Universidade Federal do Paraná na parte inclusive de gestão de banco de dados de *software* livre.

Nós temos, com a Universidade Federal de Minas Gerais, um trabalho também de mineração de dados, todo ele baseado em *software* livre.

Com a Universidade Federal do Rio de Janeiro, nós também temos um trabalho importante no que diz respeito a desenvolvimento de sistemas.

Na Universidade de Pernambuco, toda uma metodologia de desenvolvimento de sistemas baseada também em ambiente de desenvolvimento seguro.

Uso de criptografia — já mencionei.

Ampliação dos investimentos em *cyberdefesa*.

Nós passamos a ter uma linha de investimento no SERPRO exclusiva para defesa cibernética.

Nós sempre fizemos isso ao longo do desenvolvimento das nossas ampliações, das nossas necessidades de crescimento. Para os senhores terem uma ideia, o SERPRO, quando eu assumi, há 8 anos, tinha em torno de 180 *terabytes* de dados armazenados, e hoje nós passamos de 5 *petabytes* de armazenamento de dados. Isso é muito pesado e se deve, evidentemente, ao crescimento da nota fiscal eletrônica, mas a nossa quantidade é muitas vezes superior ao que nós tínhamos antes.

Criptografia. Pouco uso.

A criptografia existe, mas é muito pouco usada. Nós temos tem um jeito de não usar a criptografia, exatamente pela questão de *performance*.

Algoritmos de criptografia criados em países estrangeiros. E aí o ITI é fundamental nessa internalização. É claro que nós precisamos também de um maior conhecimento de matemática, especialmente matemática quântica, para que possamos cada vez mais ter proteções no que diz respeito à criptografia, mas fazemos esse investimento junto com as universidades do Brasil. O ITI tem inclusive mais autoridade para falar do tema.

Hardware criptográfico controlado por países estrangeiros. Nós vamos citar aqui o que temos feito sobre isso.

Uso de chaves criptográficas fracas devido aos algoritmos utilizados. Então, muitas vezes se adotam os algoritmos internacionais disponíveis na rede, e esses algoritmos são desenvolvidos dentro do NSI. Então, é claro que quem mais tem facilidade de quebrar um algoritmo desses é o próprio NSI, que colabora na construção dos algoritmos internacionais que estão disponíveis na rede.

Por isso é importante nós termos o nosso desenvolvimento — e aí volto a insistir — na matemática, na matemática quântica, o que resultará em dados criptográficos mais sólidos, elementos de criptografia mais sólidos.

Então, precisamos investir em projetos de formação e pesquisa em criptografia. Mencionei aqui a Universidade Federal de Santa Catarina.

Criação de grupos de especialistas em criptografia.

Nós temos grupos, hoje, que discutem a questão de criptografia com as universidades. Aqui na UNB também. Nós temos equipes de criptografia dentro da universidade.

Ampla adoção de criptografia no Governo.

Estamos incentivando cada vez mais que até mesmo um *e-mail* pessoal possa ser criptografado, tanto no conteúdo quanto na camada de transporte.

O uso do ICP-Brasil.

Devemos usar intensamente a nossa criptografia, controlada por nós, com os algoritmos feitos por nós, tudo controlado dentro do ITI — Instituto Nacional de Tecnologia da Informação.

Parcerias com outros países, para que tenhamos esse desenvolvimento, de novo, até mesmo pela matemática e depois pela construção.

Auditoria das soluções em uso. Quer dizer, precisamos conhecer como é que as soluções que nós já usamos estão funcionando.

Nuvem de Governo.

A nuvem de Governo é um elemento também muito importante, porque hoje em dia se atua intensamente em nuvem. Vou dar um exemplo: o rascunho do Imposto de Renda é uma aplicação de nuvem desenvolvida por nós, e, se nós hospedarmos essas aplicações... Nuvem é diferente de Internet num aspecto principal: nuvem precisa ter resiliência. Todo mundo, quando fala em nuvem, acha que é Internet mais rápida. Não é. Eu poderia ter simplesmente a Internet com mais velocidade. Quando eu falo nuvem, eu quero dizer que estou hospedando em mais de um lugar, e, nesse lugar, eu tenho mais de uma estrutura de resposta à situação de queda. Então, eu tenho que ter dois ambientes, no mínimo, de preferência dois ambientes separados.

Para os senhores terem uma ideia, o Facebook tem cinco: quatro dentro dos Estados Unidos e um na Suíça. Dentro desses cinco, ele tem outros cinco em cada um. Então, ele tem 25 ambientes. Cada dado do Facebook está replicado em 25 ambientes. Eles não têm sala-cofre, não têm nada disso, porque a preocupação deles é a que, se cair, a percepção do usuário seja a de que não caiu, porque levantou em outro lugar. Isso é chamado de resiliência.

Isso vale muito bem para a tecnologia, mas eu odeio quando se diz isso para as pessoas — que a pessoa tem que ter resiliência. Ela é esgotada e, no dia seguinte, está revigorada de novo. O pessoal da área de recursos humanos é que gosta de citar isso. Eu odeio. Mas, para a tecnologia, funciona muito bem. Nós precisamos dar a sensação de que não caiu.

Nos nossos ambientes, por exemplo, de Imposto de Renda, nós funcionamos com o nosso Centro de Dados de Brasília e o Centro de Dados de São Paulo. Então, se eu tenho uma queda, os senhores, como contribuintes, não têm nenhuma percepção de que houve queda. Nós tivemos disponibilidade neste ano de 100%. Significa que os nossos centros de dados funcionaram 100%? Não; nós tivemos quedas, sim, tanto no Centro de Dados de São Paulo como no Centro de Dados de Brasília. Felizmente, nunca dos dois ao mesmo tempo. E isso é resiliência.

Então, nuvem é guardar em mais de um lugar. Todos os provedores de nuvem internacional têm essa preocupação. O Facebook é um deles, o Twitter é outro, a Amazon, o Google, todos eles têm em vários ambientes. O Google tem até um no Chile. Significa que a sociedade chilena está protegida porque tem um centro de dados do Chile? Não, porque ele faz a replicação, por exemplo, nos Estados Unidos, pode fazer a replicação na Europa. Então, esses dados podem estar também replicados em outros lugares.

Então, nós entendemos que nuvem de Governo tem que ter essa replicação absolutamente no território nacional. Nós não podemos usar nuvens para dados sigilosos — não significa que todos os dados são sigilosos. Então, nós temos que ter uma etapa de classificação de dados. Nós precisamos estar com eles todos dentro do território nacional, em função até mesmo da legislação.

Uso de *softwares* proprietários e fechados.

Essa é uma preocupação que não é só nossa; é uma preocupação mundial. Das dez maiores nuvens no mundo, só uma delas, a nona colocada em termos de tamanho, usa *software* de código fechado, usa *software* proprietário. Não é por nada que essa nuvem é da própria empresa que produz o *software*, chamada Microsoft. As demais todas — Google, Facebook — usam *software* livre para fazer o seu ambiente de nuvem, porque ninguém quer ficar na mão de um *software* fechado, a

não ser a própria empresa que é dona do produto. E, se ela não o usasse, inclusive nós faríamos *marketing* contrário: se nem mesmo ela o usa...

Falta de gestão na integração de nuvens.

Esse *software* aberto nos permite ter um negócio que na nuvem chamamos de orquestrador, que é um *software* que fala com todas essas nuvens, que faz esse trabalho de balanceamento, que virtualiza esses diferentes ambientes. Então, esse *software* nós entendemos que precisa ser aberto também, claro, porque não adianta ter infraestrutura totalmente aberta e, em cima, ele estar fechado. Mas muitas nuvens usam *softwares* proprietários.

O que nós estamos fazendo com isso? Nós criamos uma nuvem do Governo. Nós somos um provedor de nuvem. O SERPRO é um provedor de nuvem, com nuvem própria dentro dos nossos ambientes, nos nossos três centros de dados, em São Paulo, Brasília e Rio de Janeiro. Nós operamos integralmente com *software* de código aberto, com a nuvem toda desenvolvida pelos técnicos do SERPRO lá no Paraná, em Curitiba. E hoje operamos no nosso ambiente.

Então, aquele rascunho da declaração de Imposto de Renda que eu mencionei está rigorosamente dentro da nuvem do SERPRO; não usa nenhuma nuvem privada. A nossa nuvem tem um orquestrador em que começamos a investir 3 anos atrás, chamado *OpenStack,* porque ele é aberto. Esse *software*, quando começamos, há 3 anos, era usado exclusivamente por nós. É uma produção internacional, mas desenvolvido em conjunto pela nossa equipe com a Universidade Federal do Paraná.

O que nós temos hoje de retorno disso? As grandes nuvens mundiais estão todas migrando para o *OpenStack*. A IBM e todo mundo está usando o *OpenStack* como orquestrador de nuvem. Então, Deputado, a experiência que começamos lá no seu Estado é, hoje, uma experiência internacional de gestão de nuvem, e a usamos para o Governo brasileiro.

Coordenação e gestão da nuvem para obter qualidade similar entre diferentes nuvens.

Com esse orquestrador eu posso decidir, sim, usar nuvens que não são do Governo. Mas eu decido o que vou usar nessas nuvens. Por exemplo, os nossos ambientes de homologação, na hora em que eu vou testar se um produto está bom

e ele não tem carga de dados ainda — eu estou testando o produto —, eu posso usar nuvens que são privadas.

Nós temos 2.500 desenvolvedores hoje no SERPRO, em 11 polos de desenvolvimento no País e, evidentemente, nós desenvolvemos tudo em nuvem, usando uma ferramenta de desenvolvimento também toda ela feita em *software* livre, o que acabamos trazendo da experiência do Paraná, que é uma solução que nós chamamos de *Demoiselle*.

Por fim, o uso de *software* livre, então, para todos esses nossos ambientes. Eu já citei bastante isso.

Centros de Dados no Governo.

Que vulnerabilidades nós temos?

Acesso indevido a dados e aplicações.

A maior dificuldade de controle de uma rede desse tamanho... Imaginem, nós somos 8 mil funcionários e 2.500 desenvolvedores que lidamos com todas as informações. Então, se há uma vulnerabilidade externa, a vulnerabilidade interna é maior ainda. Nós temos muitos acessos autorizados feitos por dentro da própria rede. Então, nós temos que estar com tudo absolutamente logado. Eu tenho que saber o que cada funcionário fez, com que base ele entrou, o que ele acabou fazendo. Isso, em todo o País. Então, nós temos que cuidar de todos esses acessos.

Uso de *data centers* privados, inclusive fora do Brasil.

Muitos dados estão em *data centers* privados. Nós seguidamente somos chamados a fazer a internalização de dados sensíveis brasileiros para dentro do centro de dados do SERPRO.

Dependência de sistemas operacionais fechados.

Se não for no banco de dados, pode ser no sistema operacional desses sistemas, que têm *backdoor*. Então, nós precisamos verificar essas situações de *backdoor* ou usar, como nós usamos, em todo esse ambiente, *softwares* de código aberto, mais especificamente, LINUX. Não que não seja possível invadir o LINUX — é possível, sim —, mas, pelo menos, eu tenho acesso aos códigos; eu sei o que ele faz. Código é a receita do bolo. Eu sei quanta farinha, quanto leite ele coloca, então, eu posso, inclusive, fazer alterações para melhorar o processo de segurança. Quando o *software* é fechado, eu compro o bolo e não sei como ele foi construído.

Aprisionamento.

Há muito aprisionamento. Eu tenho produtos assim: *"Olha, eu não tenho como tirar daqui".* Como eu disse, é uma empresa de 50 anos, nós temos ambientes que têm 30 anos e que, para fazer um processo que chamamos de migração, é muito caro. Então, eu tenho que me ater às vulnerabilidades desses produtos aos quais estou aprisionado.

O que, então, estamos fazendo?

Gestão, classificação e documentação de dados.

Nem todos os dados com que lidamos são dados de sigilo. Eu não preciso trabalhar com os meus 5 *petabytes* imaginando que todos eles precisam ser sigilosos, até porque muitos desses dados nós transferimos para um ambiente chamado Dados Abertos do Governo Federal Brasileiro, que é exatamente de acesso amplo à população brasileira, aos pesquisadores, aos Deputados. Todo mundo tem que ter acesso aos dados de Governo. Então, eu preciso separar o que é restrito e o que não é restrito.

Gerenciamento de identidades.

Como eu disse, dentro da nossa rede, há muita gente mexendo. Eu preciso saber o que cada um está fazendo; se ele sai de férias, nós cortamos seu acesso; se ele está em um treinamento, nós cortamos o acesso. Então, nós precisamos administrar todo o acesso a partir de gestão de identidade.

Uso de protocolo de segurança aberto e livre.

Nós usamos todos os nossos protocolos de segurança. Todo o nosso ambiente de desenvolvimento é em *software* livre. E há auditoria das soluções de *hardware* e *software,* que é essa verificação que chamamos de, pelo menos, caixa fechada, para saber o que entra e o que sai de uma caixa dessas. Essa caixa que eu estou mencionando pode ser um produto de *software.*

Isso aqui é um pouco da nossa infraestrutura de dados; como funciona o ambiente do SERPRO. Nós temos os três *data centers*, em que está concentrada a nossa maior capacidade, mas nós operamos nos 27 Estados brasileiros. Nós temos no mínimo um escritório em cada um dos 27 Estados, com roteamento local, com infraestrutura de atendimento local.

Esse é o nosso ambiente em Brasília, que eu até convido a Comissão a conhecer. Nele está armazenado um conjunto muito grande de soluções.

Temos todo um processo de segurança física, porque também há necessidade dessa segurança.

Os nossos centros de dados, então, são descentralizados e interligados por redes de alta velocidade.

Inclusive, Levy, redes de operadoras e de telecomunicações compõem a nossa solução e também os nossos provedores privados.

Alta disponibilidade: nós trabalhamos 24 horas, 7 dias por semana.

Nós fazemos todo o controle de entrada e saída de mercadorias do País, através do SISCOMEX. Então, se nós pararmos em um domingo, serão alguns milhões de guias de importação e exportação que não serão feitos. Então, nós trabalhamos 24 horas mesmo.

Todos os DETRANS... Se nós pararmos, para o DENATRAN e há o rompimento de toda atividade de produção de veículos novos, porque nós acompanhamos desde o seu nascimento na fábrica até todo o processo de transferência desses veículos nas pontas, feitas pelos DETRANs. Então, nós temos que trabalhar 24 horas por dia.

Todas as compras do Governo Federal são feitas através dos nossos ambientes.

No SIAFI, que é o sistema de gestão financeira da União, todos os convênios são feitos por nós. Inclusive o SICONV, em que há as emendas que os Parlamentares colocam, todo é administrado por nós.

Adequação ágil aos modelos de tendência de mercado.

Implementamos ontem uma sexta norma de segurança interna no SERPRO, porque o mundo vai mudando, a tecnologia se altera, os comportamentos se alteram, novas formas de trabalho vão se alterando; então, temos que estar constantemente nos atualizando.

Altos níveis de segurança, disponibilidade e desempenho.

Esse é o nosso ambiente no centro de dados.

Não vou cansar os senhores com esse aqui, mas vou aproveitar estes minutos finais para falar das aplicações de Governo, de como nós desenvolvemos

as aplicações, o que eu acho que talvez seja a coisa mais inédita de que podemos falar.

Nós estamos neste momento, por exemplo, desenvolvendo as aplicações que estarão em produção no ano que vem. Imposto de Renda de pessoa física é uma delas. Como nós desenvolvemos essas aplicações? Nós temos uma rede de 2.500 desenvolvedores, em 11 capitais brasileiras.

Nós tivemos que desenvolver as aplicações. Antigamente, o SERPRO comprava ferramentas de mercado e fazia o desenvolvimento das aplicações. Hoje, nós temos uma ferramenta em *software* livre, construída dentro do SERPRO — na verdade, ela foi construída dentro da CELEPAR, no Paraná, para fazermos o DETRAN do Paraná, e depois foi trazida para o SERPRO. Nós fizemos uma série de melhorias e evoluções. Acabamos de colocar no ar a versão 2.5 do Demoiselle. Com o Demoiselle, que é essa ferramenta de desenvolvimento, todos os nossos desenvolvedores trabalham. E a nossa equipe de segurança explode o Demoiselle a todo instante para ver se há alguma falha de segurança. Nós explodimos também as nossas próprias aplicações. Então, as aplicações, depois de desenvolvidas, passam pelas equipes de teste, para ver se elas funcionam e, depois, passam pelas equipes de segurança, onde são explodidas, para verificar se há alguma falha de segurança.

Tudo isso é desenvolvido com ferramentas de *software* livre. Então, nós procuramos evitar que até mesmo no nosso desenvolvimento tenhamos qualquer dificuldade.

Aqui são aquelas vulnerabilidades que eu já mencionei: a predominância de licença de *software* sujeito à lei norte-americana. A base de notas fiscais eletrônicas, por exemplo, toda é baseada em um banco de dados *(ininteligível)*, que é um banco de dados livre também. Então, nós temos a certeza de tudo o que acontece dentro desses ambientes.

Nós usamos uma quantidade muito grande de *softwares* de código aberto e precisamos de formação de profissionais na área de segurança, o que é muito importante, porque é uma área sempre secundária dentro do nosso ambiente — já que, primeiro, queremos *performance*, para depois ver como a coisa funciona. Nós estamos invertendo isso, com a segurança acompanhando todo o trabalho de desenvolvimento das nossas aplicações.

Por último, nós entendemos que o correio eletrônico, que é uma ferramenta do dia a dia, também merece cuidado. Hoje não conseguimos trabalhar sem o correio eletrônico, e as licenças disponíveis no mercado são de produtos fechados. O que nós fizemos foi desenvolver um produto de *software* de código aberto.

Reitero que começamos esse projeto no Paraná, no Governo Requião, e depois o trouxemos para o SERPRO. Temos uma equipe de desenvolvimento em Porto Alegre e em Curitiba que desenvolve essa ferramenta chamada Expresso.

O Expresso contempla hoje em torno de 1 milhão de contas no Brasil. Todas elas são administradas por nós? Não. Nós administramos um conjunto de cento e poucas mil contas. A Previdência, vários Governos estaduais, as universidades, as escolas técnicas, vários órgãos e muitas empresas privadas se utilizam do Expresso, que é uma solução que procuramos copiar das soluções de mercado. É uma ferramenta de correio para qualquer tipo de *device:* telefones celulares, *mobiles* de toda ordem. Nossa ferramenta oferece videoconferência, agenda, catálogo, *workflow.* Há também o Expresso Drive. Nós procuramos copiar tudo o que existia no mercado em *software* livre.

Hoje, a nossa experiência de correio aberto é considerada a maior no mundo. Nós já superamos a comunidade alemã, que originou todo esse desenvolvimento na Alemanha para a Prefeitura de Munique, e até por eles somos acompanhados agora como a maior comunidade desse tipo de *software* no mundo todo.

Em geral, não existe preocupação com esse tema. Resolvemos, então, transformar o Expresso numa ferramenta segura e de alta rentabilidade, de alta *performance*, com possibilidade de criptografia embutida usando a criptografia do ICP-Brasil.

Outra dificuldade que nós tínhamos com as ferramentas importadas era usar a nossa certificação. Aqui ela já é nativa dentro dos nossos ambientes.

Era isso que eu queria mencionar. Acho que consegui cumprir o tempo.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Agradeço as palavras.

Com a palavra o Presidente do Instituto Nacional de Tecnologia da Informação, Sr. Renato Martini.

O SR. RENATO MARTINI - Bom dia a todos e a todas.

Quero cumprimentar a Deputada Mariana Carvalho, que preside esta CPI, e os demais integrantes da Comissão que estão conosco nesta reunião.

Agradeço, sobretudo, a oportunidade de o Instituto Nacional de Tecnologia da Informação — ITI poder estar aqui, dando uma pequena contribuição a este debate que eu reputo urgente e atualíssimo.

Vou fazer uma apresentação muito breve, em 20 minutos, e já queria deixar o ITI, que é um órgão público, uma autarquia federal, à disposição da CPI. Evidentemente, o tema não vai se esgotar nas nossas apresentações. Por isso, o ITI estará à disposição, a qualquer momento, para ajudar e colaborar, pelo acúmulo de experiência que tem em alguns temas ligados aos crimes cibernéticos e aos chamados crimes eletrônicos. Nós estamos absolutamente à disposição da CPI para qualquer ajuda, apoio e colaboração ulteriores a este debate.

Antes de entrar na minha apresentação, quero fazer algumas considerações de cunho conceitual.

(Segue-se exibição de imagens.)

Quero apresentar o ITI às senhoras e aos senhoras, dizer o que é a infraestrutura de certificação digital e lincar com algumas matérias legislativas que estão aqui na Casa. Basicamente, essa será a minha apresentação.

Um tema de cunho conceitual muito importante é a expressão “crime cibernético”.

O atributo ou adjetivo “cibernético” aqui não é um predicado fortuito e não é um simples e mero detalhe. Na verdade, eu estou falando de um aspecto essencial da questão do crime.

Todos nós temos alguma noção, como cidadão — não é preciso ser um especialista em segurança pública, advogado, o que seja —, do que é crime, do cometimento de um crime. Nós estamos falando de um novo desafio, de uma nova fronteira, em que o crime se torna cibernético, ou eletrônico. Ou seja, ele é executado e se difunde nas redes computacionais — e a mais badalada e conhecida das redes computacionais é exatamente a Internet, que tem transformado a vida de todos: os governos, os países e a economia.

Vimos, na última década, uma migração da vida civil para a vida civil eletrônica. Ou seja, nós estamos levando os nossos sistemas para a Internet, para o

mundo eletrônico — não é uma experiência brasileira; não estamos fazendo isso isoladamente.

Foi pensando nisso — aqui eu começo a minha apresentação — que há mais de 1 década o País, o Governo brasileiro, construiu uma infraestrutura, um Sistema Nacional de Certificação Digital.

O Instituto Nacional de Tecnologia da Informação — ITI é uma autarquia da Casa Civil da Presidência da República que tem o papel precípuo de credenciar, auditar e fiscalizar um conjunto de entes, entidades, prestadores de serviço que entregam à empresa e ao cidadão brasileiro o chamado certificado digital.

Ele executa a identificação presencial do cidadão e da empresa. Feita essa identificação, eles recebem um certificado digital, que nada mais é, de forma muito resumida, do que uma forma de identificação do cidadão e da empresa no novo mundo eletrônico, já que eu estou levando os meus sistemas para a Internet.

Se eu pensar, por exemplo, numa nota fiscal eletrônica, que o Mazoni citou há pouco, eu estou falando num documento eletrônico que tem vida eletrônica, que nasce como um documento eletrônico, que cumpre todo o seu ciclo de vida no mundo eletrônico e que precisa ser assinado. Obviamente, não se assina essa nota fiscal de forma manuscrita. Ela tem que ser assinada digitalmente, assim como um contrato de câmbio em formato eletrônico, um prontuário eletrônico de paciente, para falar na telemedicina, uma petição eletrônica. O documento eletrônico tem que ser assinado e, para isso, usa-se um certificado digital.

Esse conjunto de entes públicos e privados que nós podemos ver na tela são credenciados pelo ITI, auditados e fiscalizados. Eles são os emissores do chamado certificado digital, que vai possibilitar à empresa brasileira e ao cidadão interagir com esses novos sistemas, com essa nova fronteira que é a Internet.

Obviamente, para a consecução dessa missão, há um conjunto de padrões de segurança física e lógica que são organizados no País para dar conta de características de segurança desses novos equipamentos que o cidadão usa para, por exemplo, declarar o seu Imposto de Renda. As empresas que optam pelo sistema de lucro real e de lucro presumido que declaram o Imposto de Renda na Internet usam o certificado digital.

Toda essa padronização de segurança física e lógica é feita para haver todo o cuidado nesse processo, bem como a segurança jurídica desse processo.

Eu não estou falando só de cuidado tecnológico, mas da validade jurídica da assinatura. A lei brasileira, o ordenamento jurídico brasileiro dá à assinatura digital o mesmo valor probante da assinatura manuscrita. Então, a assinatura digital num contrato de câmbio no formato eletrônico tem o mesmo valor probante da assinatura manuscrita num contrato físico.

Esse conjunto de ferramentas, de práticas das chamadas autoridades certificadoras, que podem ser públicas ou privadas, como o SERPRO, o SERASA, a CERTISIGN, da área privada, a Caixa Econômica, que é um banco público, a Imprensa Oficial, que é uma empresa do Estado de São Paulo... Todas essas entidades entregam o certificado para garantir, na interface com esse sistema, as cinco características elencadas ali: autenticidade da informação; integridade; confidencialidade — segurança de que só receberá essa informação quem eu quero que a receba —, o não repúdio dessa informação; e, por fim, a validade jurídica de toda essa transação.

Já salta aos olhos — acho que já fica claro a todos nós — que o fraudador, o estelionatário, tem que também sofrer um *upgrade*, não é isso? Ele não vai ficar para trás. Ele tem que se adaptar a essa nova fronteira eletrônica, a esses novos desafios, a essas novas ferramentas, e ele o faz com enorme velocidade, com muito mais velocidade do que o poder público — até porque o fraudador, o estelionatário, o criminoso leva uma vantagem enorme em relação a nós, do Poder Público: eles são ágeis e, sobretudo, não cumprem a lei. Quer dizer, se o sujeito é criminoso, não cumpre a lei. Ele é ágil, ele é veloz, ele está assistindo a esta CPI. Ele acompanhará todos esses debates, trocará informações — está trocando informações neste momento em todo o Brasil —, usará os seus canais de informação. Hoje nós vivemos na sociedade da informação. Não é só para quem é do bem que a sociedade da informação vale; também para esse submundo a sociedade da informação vale. E ele está acompanhando detalhadamente, passo a passo, todas essas discussões, aqui ou em qualquer lugar do Brasil, seja lá onde se discuta a questão tecnológica.

Evidentemente, eu me refiro ao crime da posse material de coisas, não é? Ou seja, a economia migrando para essa nova fronteira eletrônica, transformando-se sua atividade no *cybercrime*, num crime eletrônico, ele se adapta, porque ele quer, evidentemente, usufruir o ganho e se apropriar do bem indevidamente. Essa luta contra a fraude, contra o estelionatário, é uma luta corpo a corpo, como nós chamamos — você tapa um buraco, ele vai explorar outro; você tapa outro buraco. É uma luta incessante.

A tecnologia é muito desafiadora, porque ela tem uma capacidade de transformação enorme, de barateamento dos seus recursos, dos seus ativos computacionais. E isso vale também para o fraudador e para o estelionatário. Então, é uma luta incessante. Quer dizer, em nenhum momento, ninguém que faz gestão de segurança da informação ou faz gestão de segurança tecnológica se acha contemplado, até porque há um princípio da gente que opera, que atua na área de segurança, de que a segurança da informação é medida exatamente pelo elo mais fraco da corrente: se você tiver uma corrente toda feita de titânio e tiver um elozinho só que é feito de ferro comum, a força da sua corrente é exatamente esse ferrozinho vagabundo; não é o titânio dos outros 15 elos da sua corrente. Então, é sempre a vulnerabilidade, é sempre o elo mais fraco que conta na segurança da informação e na gestão de segurança da informação.

O Instituto Nacional de Tecnologia da Informação...

Essa infraestrutura de certificação digital — acho que é importante ressaltar isso aqui nesta importantíssima CPI — é um criptossistema civil. Nós não operamos a criptografia, do ponto de vista militar ou de segurança de Estado. Ela é um criptossistema para atender a aplicações de governo eletrônico, aplicações do sistema financeiro, do sistema bancário — como exemplo, eu citei os hospitais — e para entregar à sociedade uma ferramenta importantíssima para a desmaterialização de processo, para a troca do velho e tradicional documento em papel por um documento eletrônico.

O grande efeito colateral negativo do crime cibernético é exatamente a sociedade querer fraquejar nessa migração. É bom que os nossos sistemas migrem para a Internet, migrem para as redes computacionais. Ela é uma tecnologia mais

sustentável, ela é melhor para o cidadão, que tem acesso a qualquer momento a esses sistemas. Então, esse efeito colateral, talvez seja esse.

Eu me adianto e já destaco isso nessa tela seguinte: todas as características que essas aplicações trazem para a sociedade brasileira.

Quando eu digo que o Brasil, hoje, tem bilhões de notas fiscais eletrônicas emitidas, quer dizer, documentos que têm vida eletrônica, estou dizendo o seguinte: se pensarmos numa nota fiscal em formato de papel, com três vias... Vamos fazer a conta: 3 milhões em notas fiscais, multiplicados por 3. Essa era a quantidade de papel que circulava na sociedade brasileira. E, como o papel não anda sozinho, alguém o transportava e, além de tudo, havia o impacto do carbono nesta nossa sociedade cada vez mais enlouquecida.

Então, o crime cibernético é extremamente danoso, porque ele pode, além, evidentemente, de se apropriar do bem indevido, do bem das pessoas, produzir na sociedade uma sensação de que no passado era melhor. E não era. Ele simplesmente migrou. Ele lavava dinheiro em uma empresa e produzia nota fiscal em papel e agora ele vai fazer isso de forma eletrônica. O que ele precisa fazer para produzir uma nota fiscal em formato eletrônico? Essa migração não está acontecendo para eles; ela já aconteceu; eles já estão nesse novo desafio e já assumiram esses novos desafios. A nós resta agora a contrarreação.

A contrarreação está dentro de uma expressão muito interessante, na minha tela seguinte, usada pelo Mazoni, que é a questão da vulnerabilidade.

Onde está a vulnerabilidade do sistema? O Brasil hoje tem um gravíssimo problema: seu sistema de identificação civil. Não há direito e obrigação que não se inicie com uma forma inequívoca de identificação. Se eu entro no sistema aeroportuário, eu me identifico; se eu entro em um sistema hospitalar, eu me identifico; se eu caso, eu me identifico; se eu entro para a universidade, eu me identifico; se eu viro servidor público, eu me identifico. A nossa identificação civil não está doente, não; ela já está morta; é uma identificação civil do século passado e já não dá provas de atender aos novos desafios.

Por isso, nós da infraestrutura de chave pública brasileira, do Sistema Nacional de Certificação Digital, estamos incrementando isso e fazendo a adesão

aos chamados sistemas biométricos, ao uso intensivo da biometria no nosso sistema de emissão de certificado digital.

Acho muito interessante essa frase que eu coloco na tela de um especialista americano na área de segurança da informação chamado Bruce Schneier. Ele diz assim: *"O roubo de identidade é um crime sério e, no mundo do crime, é a indústria que mais cresce".*

É o chamado roubo de identidade, que acontece no mundo analógico, no mundo do dia a dia, no mundo concreto, no mundo da vida, e já acontece intensamente nas redes computacionais no mundo da Internet.

O Brasil precisa encarar esse desafio, e a esse respeito há duas matérias — aí, eu já preparo o fecho da minha apresentação — de enorme importância nesta Casa Legislativa.

Uma delas discute o registro civil nacional. É um projeto de lei do Executivo, que quer realmente repensar em novos fundamentos a nossa identidade civil. é um projeto de iniciativa do Tribunal Superior Eleitoral junto com o Executivo federal. É um projeto de enorme importância. No momento atual, ele está em uma Comissão Especial. Eu acho que há uma sinergia, uma energia positiva desta discussão da CPI com esse novo desafio que o Brasil tem que encarar, repensar a questão da identificação civil em termos mais modernos, mais atuais para dar segurança a esse cidadão que adquire uma nova ferramenta para interagir no sistema eletrônico e que hoje está fragilizado, porque nós usamos o mesmo sistema de identificação do século passado.

Há outro tema tratando da questão da biometria que eu acho extremamente importante que regulamenta e disciplina esse uso indiscriminado do dado biométrico em nosso País. Hoje, qualquer tipo de academia, qualquer tipo de negócio se apropria da nossa biometria, colhe a nossa biometria, e nós não sabemos em que termos isso é feito, não há disciplina para esse compartilhamento. Se eu quero colocar a nova identificação civil em termos de biometria — e todos nós sabemos que o Tribunal Superior Eleitoral está exatamente pensando em usar a biometria como uma chave de acesso à urna eletrônica, e possivelmente usaremos a biometria para compor tantos outros sistemas de segurança —, não é possível que

qualquer um possa colher essa biometria e não se comprometa ao não compartilhamento ou ao não compartilhamento indevido dessa biometria.

Peço escusas à CPI por estar me imiscuindo na matéria legislativa, que não é a minha praia, mas eu acho que são temas de enorme sinergia com esta discussão que ocorre nesta CPI.

Destaco, ali, o Projeto de Lei nº 7.316, que é exatamente a nova lei brasileira para cuidar da certificação digital. Atualizando, ela se encontra na CCJ. Se esta CPI puder nos ajudar a, digamos assim, impulsionar... Esse também é um projeto de lei de iniciativa do Executivo que, para nós, é de enorme importância.

Eu encerro, mais uma vez, Sra. Presidente, agradecendo o convite, a oportunidade de o ITI poder fazer essas brevíssimas considerações.

Quero ressaltar, mais uma vez, a urgência e importância deste Comitê e nos colocar à disposição.

Nós só combatemos o *cybercrime*, a fraude eletrônica, com a troca de informações. Nós temos que ser tão ágeis quanto eles. Nós temos que trocar informações, compartilhar informações e recursos, o mais rápido possível e da forma mais acessível possível.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Presidente Renato, pela sua presença.

Com a palavra a Sra. Cristine Hoepers, Gerente-Geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil — CERT.br, vinculado ao Comitê Gestor da Internet, o CGI.

A SRA. CRISTINE HOEPERS - Bom dia.

Primeiramente, obrigada pelo convite para eu poder vir aqui e compartilhar com vocês o trabalho que temos feito no CERT.br.

Vou começar contextualizando um pouco o CERT.br dentro do próprio Comitê Gestor da Internet.

Já se falou do Comitê Gestor da Internet. O Sr. Presidente do SERPRO comentou sobre a sua importância.

O Comitê Gestor da Internet no Brasil é uma entidade multissetorial — ou seja, ela é composta por diversos setores —, criada em 1995, para coordenar e

integrar todas as ações de Internet no Brasil, e tem várias atribuições. Então, diversas pessoas conhecem o Comitê Gestor da Internet, dependendo da sua atribuição.

(Segue-se exibição de imagens.)

Relativamente ao tema que estamos discutindo, existem as recomendações de padrões e procedimentos técnicos para Internet no Brasil e, especificamente, a promoção de estudos e padrões para haver o uso mais seguro e mais adequado da Internet pela sociedade.

O Comitê Gestor da Internet no Brasil, sendo multissetorial, tem 21 representantes de Governo e de sociedade civil. Estão sentados aqui à mesa 2 membros desse Comitê Gestor: o Eduardo Levy, que é representante do sindicato de provedores de telecomunicações, um dos representantes eleitos pelo seu setor, e o Renato Martini, do ITI, que representa o Governo. Quer dizer, o Comitê é realmente multissetorial, integrando os atores que estão envolvidos para desenvolver a Internet e para fazer um melhor uso dela.

Então, temos esse comitê coordenado pelo Ministério da Ciência e Tecnologia, mas, para que ele possa implementar essas políticas estratégicas, existe uma entidade civil sem fins lucrativos chamada NIC.br, que é quem efetivamente executa, quem implementa todas essas estratégias e todos os serviços para a comunidade de Internet no País.

Então, aqui, estão só algumas dessas atribuições. Dentre elas, há essa atribuição de fazer tratamento de incidentes no País. Isso aí está no estatuto, que foi definido por uma assembleia geral — falei do NIC.br e esqueci de passar —, que é formada por todos os membros e ex-membros do Comitê Gestor, e existe um conselho de administração e uma diretoria.

Essa organização, que é sem fins lucrativos, mantém-se com o registro de domínios no Brasil. Quer dizer, ela se sustenta com isso, e todos os outros serviços são gratuitos, são serviços prestados como um retorno à Internet da contribuição de todos no registro de domínios sobre o “ponto br”. Quer dizer, os cidadãos, no Brasil, poderiam registrar o domínio sobre qualquer área, poderiam usar o “ponto com”, o “ponto org”, qualquer domínio, mas, toda vez que alguém usa o “ponto br”, está contribuindo para todos os serviços que estão sendo trazidos para a comunidade

brasileira. O CERT.br, que é a nossa área de segurança, é um dos primeiros serviços, mas há várias outras áreas que eu vou abordar ao longo da minha apresentação que contribuem para a segurança da Internet brasileira.

Falando especificamente do CERT.br, nós não somos um órgão em si, somos um dos serviços do NIC.br para o Brasil. Nós nos pautamos pela estratégia do Comitê Gestor. Inclusive a criação do CERT.br, em 1997, foi feita através de um estudo do Comitê Gestor da Internet de qual era o elemento faltante no Brasil para ajudar a ter mais segurança e ter mais capacidade de lidar com incidentes de segurança na Internet.

A principal atividade que nós fazemos é o próprio tratamento de incidentes, que é basicamente facilitar que as organizações consigam identificar problemas, identificar invasões, identificar fraudes, consigam entender o que está acontecendo e consigam dar o tratamento adequado.

Então, o nosso trabalho é todo colaborativo, não é um trabalho vinculado a nenhum trabalho de polícia ou a nenhum trabalho de combate ao crime diretamente, porque nós tratamos com incidentes de segurança antes de ver se isso está configurando um fato típico antijurídico.

O nosso trabalho é ajudar essas organizações a entenderem, a se recuperarem e de orientar, sempre que necessário, para que, aí, sim, se identificado um crime, isso possa ser levado às autoridades competentes.

Nós temos um foco muito grande na formação de profissionais, porque um dos grandes desafios para conseguir tratar adequadamente incidentes é ter profissionais qualificados — e eu vou tocar todas as áreas, acho que são as principais — e conscientizar sobre boas práticas, não só dos usuários de Internet, como de todos que mantêm serviços e que mantêm áreas da Internet no Brasil.

Então, eu vou falar um pouquinho mais de incidente de segurança — esse é um termo muito técnico, mas foi especificamente a requisição. Hoje nós recebemos notificações de incidentes de fora do Brasil e de dentro do Brasil. Elas são voluntárias. Então, nós temos hoje um catálogo que é acompanhado desde 1999 de pessoas que estão se deparando com problemas de segurança e que precisam de ajuda e nos procuram para tentar resolver esse problema. Esse incidente é qualquer fato adverso que possa impactar a segurança.

E quando nós falamos em tratamento de incidentes, isso significa o processo de identificar, de responder, ou seja, de recuperar o ambiente, de torná-lo seguro, de proteger os dados, de auxiliar cidadãos que estejam com problemas. E existem grupos, que são os Grupos de Tratamento de Incidentes, que são criados para lidar com isso.

A metáfora mais normal que se tem seria com brigadas de incêndio, em que se tem um problema e haveria um grupo atuante, mas ele tem todo um lado preventivo. Hoje, no Governo Federal, nós temos no GSI o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal — CTIR Gov, que é um grupo que trabalha com a administração pública federal, nós temos vários outros grupos, o Serviço Federal de Processamento de Dados — SERPRO possui um grupo específico, que é a ETIR, Equipe de Tratamento de Incidentes do SERPRO. E todos esses grupos trabalham em conjunto.

Nessas estatísticas que nós temos acompanhado, é possível observar uma curva que só sobe. Esse é o número de notificações voluntárias que o CERT.br tem recebido. No ano passado, nós recebemos um número maior do que nos anos anteriores — foram mais de 1 milhão de incidentes de segurança notificados. Como falamos, isso é voluntário, não tem como saber se isso é o total dos incidentes ou não é. Provavelmente isso é apenas um pedaço.

Os aumentos e as quedas, há vários fatores que influenciam. Nós notamos que, sempre que temos mais organizações conscientes dos problemas de segurança, isso também aumenta o número de notificações, quer dizer, nós temos mais pessoas vendo. Mas é bom lembrar que nós temos, no Brasil, uma Internet que cresce dia a dia, nós ainda temos muitos cidadãos que vão entrar, e a tendência é que aconteçam mais incidentes, porque nós temos mais gente usando a Internet; temos a Internet cada vez mais presente no nosso dia a dia, como uma parte fundamental.

O que é a maioria dessas notificações que nós temos? Nós temos muitas notificações que categorizamos historicamente como tentativas de fraude, a definição de dicionário mesmo: tentativa de uso de um ardil ou tentativa de obter vantagem econômica prejudicando alguém.

Como nós tratamos isso? A maior parte é de entidades da indústria — indústria de *software*, indústria de entretenimento — que nos notificam dizendo: *"Olha, existe algum conteúdo violando direitos autorais"*. Tudo o que nós fazemos é repassar a quem de direito para implementar políticas e verificar. Nós não fazemos nenhum outro tipo de atuação. Nós sempre esclarecemos que não vamos investigar, que não temos como fazer retirada de nenhum conteúdo, mas nós também não vamos ignorar essas notificações. Então nós repassamos às redes que porventura estejam hospedando isso, porque pode ser que elas tenham sido comprometidas e estejam realmente hospedando algum conteúdo ilegítimo. Então, a nossa função é fazer com esse conhecimento chegue até a ponta.

Outro grande ponto são notificações de tentativas de fraude com objetivos financeiros. E nós sempre orientamos que, se alguém realmente já tiver sofrido uma fraude financeira, procure imediatamente uma delegacia para fazer uma notícia-crime, que procure a instituição.

Então, as fraudes realmente efetivadas acabam não vindo para nós, e nós sempre recomendamos: *"Nós não vamos tratar com o crime já cometido"*. O nosso foco é tentar reduzir o número de vítimas. E reduzir o número de vítimas, para nós, significa tentar contatar quem está hospedando, por exemplo, um código malicioso — fala-se muito em cavalos de troia —, aquelas páginas falsas, que hoje não são só mais de bancos ou de cartões de crédito; existem pessoas fazendo páginas falsas de serviços de Internet, de redes sociais, para tentar pegar credenciais. Então, a nossa atuação é tirar do ar e contatar quem está hospedando, porque na quase totalidade das vezes são vítimas que foram comprometidas por algum criminoso e que nem sabem que elas estão ali participando de um esquema, de um ardil.

Então, a nossa função é tirar isso do ar. E, do ponto de vista de quando encontramos um código ou alguma coisa, nós informamos às instituições afetadas que há um novo tipo de tentativa de golpe, mas nós não atuamos especificamente em investigação.

Outra categoria que é extremamente comum são varreduras em redes de computadores. Isso acontece porque os atacantes normalmente varrem a Internet dia e noite à procura de sistemas vulneráveis e comprometem esses sistemas vulneráveis por falhas de programação, falhas de configuração, senhas fracas —

são muitas as maneiras. E, quando eles comprometem, dali eles começam a atacar outros.

Então, quando alguém nos notifica *"Olha, a rede tal fez uma varredura contra nós"*, nós entramos em contato com essa rede, porque provavelmente ela também é vítima e precisa saber que ela tem que tomar um passo. Então, este é um ponto grande que nós temos: tentar ajudar quem está fazendo parte da propagação de conteúdos maliciosos ou de ataques a se recuperar.

No ano passado, a categoria que mais cresceu foi a de ataques de negação de serviço. Não foi especificamente de organizações brasileiras sofrendo negações de serviço, ou seja, tentativas de tirar um *site* do ar, tentativas de tirar um serviço do ar, mas foi de muitas redes com problemas de configuração, muitos *modems*, muitos roteadores *wi-fi*, muitos computadores de usuários infectados, que estavam sendo abusados por terceiros para cometer crimes contra outros terceiros ainda fora do Brasil.

Então, nós fomos muito procurados por quem estava sofrendo esses ataques, para que tentássemos contatar as também vítimas no Brasil, para que elas pudessem se recuperar.

O nosso trabalho principal tratando esses incidentes é, primeiro, buscar um ecossistema de Internet saudável. É muito similar ao que nós vemos hoje na parte tanto de poluição quanto de saúde pública, quer dizer, é preciso que todos façam parte, para não emanar tráfico malicioso, ou seja, cada um protegendo a sua rede. E essa proteção tem que ser feita pelo dono de cada rede, pelo dono de cada celular, pelo dono de cada máquina. Não há como ter alguém extra. Isso pode ser via medidas de segurança, via educação.

Então, nós temos um trabalho muito grande com administradores de redes e sistemas, para ensiná-los a configurar melhor os sistemas, aplicar correções. Nós temos um trabalho grande com usuários de Internet, para que eles entendam os riscos, para que eles não tenham medo, para que eles entendam exatamente o que é esse novo ambiente, para que eles entendam que existem alguns riscos e que existem comportamentos que reduzem muito esses riscos. Quer dizer, não é diferente do que já é a educação no mundo tradicional, mas na Internet isso também precisa ser levado.

Há todo um trabalho de tentarmos chegar aos desenvolvedores, porque vulnerabilidades são inseridas por pessoas que estão programando, que, às vezes, por inocência, sem pensar como alguém pode querer abusar daquele sistema, transformam esses sistemas mais fracos.

Mas, mesmo melhorando tudo isso, os incidentes ainda vão ocorrer, ainda vai haver vulnerabilidades nos sistemas. Mas o que nós precisamos é reduzir o impacto, reduzir o volume. E se nós tivermos uma Nação preparada para lidar com esses incidentes, o impacto é menor. Se houver órgãos de Governo e empresas identificando mais rapidamente os problemas e resolvendo-os, há, com isso, um impacto muito menor.

Não há como trabalhar nessa área sem cooperação — sem cooperação nacional e sem cooperação internacional.

Aqui no Brasil nós temos feito um trabalho muito grande de ajudar a criação de novos grupos de tratamento de incidentes. Nós temos grupos em vários setores da sociedade — nós temos grupos em operadoras de telecomunicações, em órgãos de Governo, no setor financeiro. Existem dentro do próprio Governo várias outras equipes, e o objetivo é que todas essas equipes, trabalhando em cooperação, cada uma tratando incidentes da sua área, e nós, conseguindo auxiliar essas equipes a serem mais eficientes, vamos conseguir chegar a um nível melhor de segurança.

Como eu comentei, um grande foco nosso é de educação de usuários. Nós temos um documento cuja primeira versão é de 2000. Quer dizer, ele é um documento bastante maduro, composto por um livro que é gratuito, que é livre para uso na Internet. Quer dizer, nós damos uma licença livre. Impressões são muito limitadas, mas nós temos enviado com bastante frequência para escolas e para centros de inclusão digital que querem capacitar os seus usuários a entenderem a tecnologia e a entenderem as questões de segurança.

E, além desse conteúdo maior, nós temos o que chamamos de Fascículos de Segurança, que são doses mais homeopáticas em temas bem específicos. Esse é um material que... Recebemos um pedido muito grande de professores, de educadores, de elaboração de um material que pudesse ser impresso, que fosse ilustrado, que atraísse jovens e crianças, para possibilitar uma educação maior dessa faixa etária com um material já existente. Quer dizer, não somos nós que

vamos até os locais fazer essa educação, mas nós damos o material, damos as ferramentas, damos conjuntos de eslaides que podem ser usados para aula.

E um outro efeito hoje é que nós temos muitas empresas educando seus funcionários com esse material, o que é bom, porque todas essas pessoas vão para casa e passam esse conhecimento para amigos, para familiares, e eu considero isso uma parte para termos um ecossistema mais saudável. Existem, claro, outros materiais. Eu ia até comentar que existe um portal mantido por nós que é uma iniciativa do Comitê Gestor da Internet, que é o Internetsegura.br. Lá, não há material produzido por nós. O que há são *links* para todos os documentos que existem: a cartilha mencionada pelo Eduardo Levy, que é feita pela OAB, com as operadoras; outros documentos, de outras áreas, e a ideia é conseguir ter um ponto onde as pessoas possam buscar a informação.

Para encerrar, eu gostaria de falar um pouco mais de algumas outras iniciativas que aumentam a estabilidade e a segurança. Uma específica é lembrar que a Internet, embora dependa de telecomunicações como fio condutor, é formada por programas, por protocolos, e nós temos um conjunto desses recursos que são críticos para o bom funcionamento da Internet. Alguns desses recursos são os mais discutidos nos âmbitos de governança internacional, que são registros de domínios, sistemas de numeração, roteamento. São todos temas muito complexos, mas eu acho que o Jon Postel, que foi uma das pessoas que ajudaram a criar a Internet, tinha uma frase muito simples, que ele sempre dizia: *"o nome indica o que procurar, o endereço aponta onde encontrar, e a rota diz como chegar lá"*. Então, na Internet, nada funciona sem ter um endereço, uma rota e nomes dizendo o que se quer procurar.

E esses são recursos muito críticos, porque existem estratégias do Comitê Gestor da Internet e do NIC de contribuir na política internacional, de manter esses recursos com uma boa política nacional, de facilitar que as redes brasileiras obtenham esses recursos de maneira simples, e de haver mais resiliência em toda essa área.

Uma das áreas bem específicas no Brasil é toda a parte de nomes. O Brasil foi segundo país no mundo a implementar as restrições de segurança da área de resolução de nomes no mundo, e hoje o Brasil é o segundo país do mundo que tem

o maior número de servidores-raiz, em que todo o sistema de resolução de nomes depende de que se crie um nome e isso se propague, para que todos possam saber onde encontrar. E existe um conceito da raiz dessa grande árvore, que é quem aponta para onde estão os principais respondedores.

Então, o Brasil hoje está muito bem nessa área. Eu acho que é o segundo país com o maior número dessas cópias. A maior parte delas são mantidas pelo NIC.br, por uma decisão estratégica do Comitê Gestor da Internet. Nós temos um outro ponto, grande também, de melhora de estabilidade, que é ter pontos de troca de tráfego no País. Esse é um assunto que tem sido bastante discutido. Esse é um projeto de mais de 10 anos também do Comitê Gestor, que tem sido financiado e implementado pelo NIC.br. Hoje, temos 25 pontos no Brasil. E em que isso contribui para a segurança da Internet?

Contribui que as redes ficam mais autônomas, elas têm mais de uma forma de conexão com a Internet. Elas estão mais resistentes a ataques, e elas podem trabalhar melhor as suas políticas de redes. E o Brasil também, hoje, é o segundo país do mundo com o maior número de pontos de troca de tráfego. Esse é um trabalho muito grande que tem sido feito para que haja, sim, como termos mais eficiência, custo reduzido, e um tráfego ficando dentro do País, quando ele precisa ficar dentro do País.

Como eu disse, há várias outras iniciativas nossas de boas práticas para que cada um faça a sua parte de manter a Internet mais segura, de manter o nosso ecossistema mais saudável.

Outro ponto muito grande: todo esse trabalho tem que ser feito de uma maneira coordenada, de uma maneira cooperativa. E hoje há vários fóruns em que isso é discutido. São todos fóruns abertos, com eventos transmitidos pela Internet, com participação da população, das empresas, e isso é um fórum muito positivo, porque vemos os anseios da sociedade, vemos as dúvidas do cidadão, porque eles levam isso até esses fóruns.

E, finalmente, eu gostaria de agradecer. Eu falei rapidamente de algumas coisas que nós fazemos, mas estou à disposição para eventuais próximos esclarecimentos.

Muito obrigada.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Sra. Cristine Hoepers.

Encerradas todas as apresentações, vamos passar aos debates. Eu só gostaria de informar a todos os Deputados que já demos início à Ordem do Dia, e, também, de deixar um registro de que o Dr. Eduardo Levy tem um compromisso e um voo e terá que sair às 13h40min. Então, para que todas as perguntas tenham uma resposta, eu vou fazer apenas um bloco, com todos os Parlamentares já inscritos, para ele poder ser o primeiro a responder aqui, e dar tempo de poder contribuir com a nossa CPI.

Todos de acordo?

O SR. DEPUTADO DELEGADO ÉDER MAURO - De acordo. Que todos façamos as perguntas, e, depois, o Sr. Levy faça o posicionamento.

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

Com a palavra o Deputado João Arruda, autor do requerimento.

O SR. DEPUTADO JOÃO ARRUDA - Bom, eu queria parabenizar a Comissão, nossa Presidente, Deputada Mariana, os colegas Parlamentares e os convidados, agradecendo a presença de todos aqui. Eu tenho uma pergunta rápida. Quero me dirigir ao Dr. Mazoni, e não tenho muito a falar sobre o SINDITELEBRASIL. Na verdade, as empresas de telecomunicação podem contribuir com a investigação, mas elas não são investigadoras. Então, elas têm essa autonomia, e isso nós preservamos também através do Marco Civil da Internet.

Mas, Dr. Mazoni, eu lembro que na época da discussão do Marco Civil da Internet nós discutimos a possibilidade das mudanças na localização dos *data centers*, das unidades de processamento de dados. E, no meio daquela discussão, a Presidente Dilma, na época, teve suas informações ou dados governamentais ou pessoais delas invadidos pelos norte-americanos — o Edward Snowden foi quem confirmou essas informações depois. Daí, a Presidente pediu que nós obrigássemos, através do Marco Civil da Internet, que fosse feita a instalação de todos os *data centers* aqui no Brasil. E eu entrei em contato com o senhor, e o senhor me disse: *"Olha, não é por aí o caminho. O caminho é outro."* Na verdade, é quem administra esse *data center*.

E daí nós descobrimos e investigamos mais, estudamos mais o assunto, que o único meio... Falamos muito aqui de estrutura. Eu estou chegando à conclusão, à medida que fazemos cada vez mais audiências públicas, de que o problema não está na Internet. O problema de crimes acontece em qualquer lugar. Na Internet também acontece com muita força, é evidente, mas o problema não está na Internet. O problema está, na verdade, na falta de estrutura da polícia para fazer a investigação, e da estrutura, também, que nós oferecemos em alguns setores.

O SERPRO, por exemplo, tem uma estrutura limitada. Mas é o SERPRO que garante a segurança dos dados governamentais.

Na Lei Carolina Dieckmann, nós tivemos um problema no início da última legislatura, que a Lei Carolina Dieckmann não tem absolutamente nada a ver com o que nós aprovamos no início da última legislatura. V.Exa., Deputado Sandro, lembra bem disso, de qual foi o objeto principal do outro projeto. Mas, para não entrar nesse mérito aqui, eu quero te perguntar. Eu fiquei preocupado, porque eu ouvi do senhor que a DATAPREV e o DATASUS não integram a rede protegida pelo SERPRO hoje, ela tem independência. Isso coloca em risco, um risco maior, as informações que são gerenciadas por essas outras unidades de processamento de dados?

E confio muito no SERPRO. Acho que o Governo tem que investir mais no SERPRO, em novas estruturas, e, quem sabe, também inserir outros sistemas do Governo e até envolver Estados e Municípios. Com essa proteção, já há convênio. Podem, quem sabe, ampliar isso.

Mas o cidadão comum não tem. O cidadão comum e o empresário que querem proteção não têm acesso a essa estrutura. Então, qual seria a alternativa? Pela experiência que o senhor tem como Diretor do SERPRO, qual seria essa estrutura que o cidadão comum deveria buscar, semelhante ao SERPRO, para ter as suas proteções? A SINDITELEBRASIL pode até, quem sabe, contribuir e nos ajudar. Um *data center* para cada empresa? É muito caro. Não dá, não funciona! Qual seria uma alternativa?

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Com a palavra o Deputado Sandro Alex, Sub-Relator desta Comissão.

O SR. DEPUTADO SANDRO ALEX - Obrigado, Presidente.

Senhoras e senhores, nossos convidados, agradeço pela presença.

Quero colocar um pouco de números na nossa CPI e pedir aos nossos convidados números para a avaliação da nossa Comissão.

Sr. Levy, eu queria saber o número de quebras por mês. A Justiça solicita aos senhores um numero mensal de quebras, em média. Quantas quebras são solicitadas? Quantas quebras de IPs os senhores fazem por solicitação judicial?

Eu também gostaria de fazer um questionamento ao SERPRO sobre investimentos. Qual é o valor de orçamento do SERPRO hoje? Qual é o orçamento para este ano, 2015, e para o ano seguinte, 2016? Porque nós temos informações da falta de recursos. O senhor colocou aqui a vontade do SERPRO de investir, mas, enfim, nós sabemos aqui da realidade do Brasil e do Orçamento, que é a discussão desta semana no País.

Então, eu quero saber o volume de recursos. Isso é realmente suficiente? O senhor teve cortes neste ano? Quero que o senhor coloque isso em números, os investimentos, para nós aqui da CPI. Realmente existe a falta de recursos? Porque inclusive há informações de não pagamentos, de falta de recursos, de que o SERPRO está com débitos — eu não sei se com fornecedores, com operadoras. Enfim, eu quero que o senhor coloque se realmente existe essa deficiência e se o SERPRO também está com o orçamento negativo.

O senhor falou sobre a rede própria, que ela atende à Receita, à declaração de Imposto de Renda. O senhor declarou que isso se faz por um motivo: segurança. É isso? Então, o senhor tem um investimento na rede própria para a Receita devido à segurança.

Porém, nós temos outros organismos que não estão com rede própria, por exemplo, o Banco Central. Então ele está inseguro? Gostaria da sua declaração, porque o senhor disse que, para a Receita Federal, o senhor exige esse investimento da rede própria por uma questão de segurança. Então, isso significa que a Caixa Econômica, o Banco Central e outros órgãos que estão fora dessa rede própria estão desprevenidos? Eles estão mais vulneráveis? Eu gostaria de saber disso em números.

Nesses últimos anos, nós tivemos uma incidência maior de falhas. E aqui eu coloco inclusive um pedido do nosso Relator, o Deputado Esperidião Amin, a todos. As tecnologias são seguras? O representante do ITI falou muito sobre isso, e eu

quero saber. Estamos com tecnologias seguras? Houve casos de invasão? Esses casos estão aumentando ou estão diminuindo? Estamos sendo eficazes ou não? Quero números dessas tecnologias e desses casos de invasão.

Sobre o BR, eu gostaria de saber os requisitos para se ter o endereço com o BR. Isso está suficiente? Dentro do comércio virtual, quando existem falhas, crimes, informações, quais são as atitudes que os senhores tomam com relação a essas pessoas que têm esses endereços com o BR? Para ter o BR, é necessária a presença no Brasil ou não?

Finalmente, sobre o Marco Civil da Internet, de que todos nós ouvimos falar, eu gostaria de dizer que, com relação às exceções, que estão em discussão hoje no País, porque o Marco Civil deixou as exceções, a serem regulamentadas — não é isso? —, vemos hoje um avanço, na discussão mundial, dessas exceções. Por exemplo, temos hoje no Marco Civil a emergência e a prestação de determinados serviços como as exceções ao Marco Civil.

Recentemente, tivemos no Brasil um caso, que os senhores conhecem, de um *site* chamado Tudo sobre Todos, onde informações eram disponibilizadas. Através de uma cautelar, o juiz determinou, parece-me, que as operadoras inserissem obstáculos tecnológicos capazes de inviabilizar, até o julgamento definitivo do processo principal, acesso ao *site* Tudo sobre Todos, em todo o território nacional. Ou seja, foi uma decisão do juiz. Esse não seria o argumento para que realmente... Essa é uma exceção que deve existir no Marco Civil? Existe a certeza de um endereço que comete um crime, e muitas vezes ele não está no Brasil, mas fora do Brasil. A neutralidade deve ser quebrada para impedir que se acesse esse *site*? Se ele está no País, você tem a possibilidade do bloqueio desse endereço, mas, se ele está fora do País, é preciso impedir que se chegue até esse endereço.

Ou seja, quero falar um pouco sobre essas exceções à neutralidade, que é hoje o assunto que domina na Europa. A maioria dos países encaminha já legislação sobre isso. Não temos ainda a regulamentação. Essa foi uma decisão judicial, mas não temos a regulamentação. Temos que regulamentar isso. Então, eu gostaria de um foco também nesse assunto.

Deixo os demais comentários para os próximos oradores.

Obrigado, Presidente.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Com a palavra a Deputada Alice Portugal.

A SRA. DEPUTADA ALICE PORTUGAL - Deputada Mariana Carvalho, senhores convidados, convidada, serei muito breve. Não consegui chegar a tempo de ouvir a todos, mas gostaria de falar sobre algumas curiosidades.

Primeiro, Sr. Levy, segundo o Delegado da Polícia Federal que já esteve conosco em outras oportunidades — foram afirmações feitas por delegados da Polícia Federal —, algumas solicitações de *logs*, ou seja, registros de acesso ou de conexão são respondidos em forma de relatórios impressos. A minha pergunta é: isso procede? É exatamente a questão da confidencialidade, da segurança. É possível que esses retornos se deem em forma de relatórios impressos? É do seu conhecimento isso?

Eu iria abordar isso de maneira mais larga, mas tanto o Presidente do SERPRO como o Sr. Renato e a gestora da Internet abordaram de maneira clara que é o problema da assinatura eletrônica, da assinatura digital, o objeto da modernização da legislação. Então, em vez de perguntar, eu vou dizer que a sua contribuição em nos alertar sobre os projetos que já tramitam pode fazer desta CPI não só uma CPI que investigará casos objetivos de crimes cibernéticos — e nós temos já alguns sendo relacionados —, mas também uma CPI que auxilie na modernização da legislação no Brasil, ou seja, no aprofundamento e na utilização cada vez melhor do Marco Civil da Internet.

Acima de tudo, precisamos buscar contribuições na vida prática, nos especialistas, para que possamos contribuir com a modernização da legislação — inclusive uma das tarefas que podemos distribuir pelas subcomissões é o aprofundamento nesses projetos — e, ao final, apresentar à Casa um conjunto de normatizações que possam colaborar com o Marco Civil. Acho que esses especialistas podem ser — eu fiquei muito satisfeita em ver que todos se colocam à disposição da Comissão — muito úteis, para que possamos beber nessa fonte e melhorar cada vez mais a legislação no Brasil, garantindo neutralidade e democracia, facilidade de acesso, e também segurança.

Por último, eu queria só um comentário do Dr. Marcos Mazoni sobre o episódio Estados Unidos-Brasil. Está superado diplomaticamente — a Presidência já se colocou de maneira muito clara —, mas, ao seu olhar, de que maneira nós podemos nos preservar daquele tipo de situação?

O seu relatório aqui foi muito bem detalhado, foi uma aula, que, inclusive, nos deixa muito seguros sobre a natureza nacional soberana do controle da guarda dos nossos dados.

Com todos esses sistemas livres — uma nuvem brasileira —, *software* livre, mesmo assim, nós fomos surpreendidos com aquele nível de detalhamento, especialmente focado nas nossas empresas nacionais. Focado, direcionado para a engenharia nacional, para o desenvolvimento nacional. Se nós dissemos — sempre dissemos — que a inovação, a ciência e a tecnologia são questões de soberania e desenvolvimento nacional, a guarda dos dados, sem dúvida alguma, hoje se coloca também nesse patamar de proa em relação a essa questão. Como lhe parece a segurança dos dados e como lhe parece que estamos preservados hoje em relação a novos ataques e invasões como a que sofremos recentemente?

Obrigada.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Deputada Alice Portugal. Concedo a palavra ao Deputado Delegado Éder Mauro.

O SR. DEPUTADO DELEGADO ÉDER MAURO - Sra. Presidente, Deputada Mariana, Sras. e Srs. Deputados, Srs. Palestrantes, a quem nós agradecemos a participação, a CPI trata de crimes cibernéticos. Eu ouvi uma frase do Renato que para mim foi a frase chave de todos que aqui falaram. Para nós apurarmos crimes cibernéticos, nós precisamos de velocidade e de informação rápida. Infelizmente, isso não acontece no Brasil, não só pela questão de distanciamento das operadoras das autoridades policiais, como também pelo despreparo e pela falta de policiais qualificados, como disse o próprio policial federal que esteve aqui na última palestra: a Polícia Federal possui, salvo engano, 20 policiais em todo o Brasil para fazer esse tipo de investigação. Na Polícia Civil não é diferente. São muito poucos, e a qualificação também é muito pouca.

O que eu quero afirmar com isso? A Lei nº 12.850, de 2013, por exemplo, no art. 15, diz que a autoridade policial poderá ter o acesso, independentemente de

ordem judicial, aos dados cadastrais do investigado, seus endereços e todos os dados. A Lei nº 12.830, de 2013, legitima a autoridade policial a fazê-lo, através do delegado. Porém, hoje as operadoras em geral não obedecem esse tipo de coisa. Algumas acham ainda que precisam de uma ordem judicial, conseguida pelo delegado de polícia, para que possa fornecer esses dados. Isso já atrasa e muito uma investigação do caso.

Nos crimes de estelionato, pedofilia e outros, que são feitos não pelos meios móveis, mas pelos meios fixos, como é o caso dos *cybers*, dos *notes*, dos computares fixos, que só são identificados também pelos IPs, a meu ver também não é preciso autorização policial para conseguir os dados cadastrais, bastando a autoridade policial requerer às operadoras. Mas isso também não é feito, porque as operadoras têm a cultura de que só com ordem judicial, e o distanciamento é muito grande.

Vou citar como exemplo o Estado do Pará, mas faço referência a todo o Brasil. No Estado do Pará, as redes de farmácia, as redes de qualquer comércio pequeno vendem aparelhos celulares em grande monta. Assaltos ocorrem todos os dias e todas as horas, inclusive com morte, fazendo vítimas. Sei que somente em São Paulo, hoje, através de uma portaria ou de uma resolução do Secretário de Segurança, algumas operadoras — salvo engano, a TIM é a única que estabelece esse tipo de serviço — bloqueiam, inutilizando os IMEIs de aparelhos que são roubados em grande monta das lojas. Se fosse obedecido esse tipo de coisa pelas operadoras, com um simples requerimento da autoridade policial; se com o número dos IMEIs dos aparelhos roubados, eles fossem bloqueados e inutilizados, os assaltantes não teriam mais o atrativo de roubar aparelhos telefônicos nas redes de farmácia ou em qualquer estabelecimento, porque não teriam utilidade lá fora para o receptador. Mortes seriam evitadas. Mas isso não acontece. Só em São Paulo, volto a dizer, e, salvo engano, pela operadora TIM.

Eu não sei se precisaria, Sr. Presidente, ser convocado aqui o Sr. João Rezende, Presidente da ANATEL, que é agência reguladora. E já deixo aqui um requerimento verbal para que isso aconteça, inclusive junto com as operadoras, para regulamentarmos esse tipo de coisa, porque vai facilitar, e muito, que as investigações possam fluir de forma rápida, como diz o Renato, porque senão nós

não teremos condições de chegar nem perto dos *hackers*, nem perto daqueles que mexem na Internet para cometer crimes.

Outro dado que eu não posso deixar de perguntar é a questão do WhatsApp. Hoje todos os dados são, por aquilo de que tomei conhecimento, criptografados. E esses dados, sim, são requeridos através de ordem judicial, porque quebra sigilo telefônico e chega à mão da polícia, e a polícia requer às operadoras os dados. Eles são fornecidos dessa forma. Mas a polícia não tem condição nenhuma de decifrar os dados. Então eu gostaria de saber de todos aqui presentes o que é preciso para que a tecnologia, que tanto foi colocada aqui, possa fluir para que as autoridades policiais possam ter esse acesso livre e rápido, porque hoje quase 50% das comunicações não são feitas mais na conversa, mas só pelo dedo. Então, a polícia precisa desses dados também. Essa é uma observação.

Para finalizar — e, claro, não tem nada a ver com a questão dos *hackers*, dos crimes cibernéticos, mas tem, com certeza, a ver com a questão da comunicação —, volto a citar, Mariana, o meu Estado do Pará, já que falaram tanto em tecnologia, falaram tanto em questões de investimentos. Mas acho que o Estado do Pará não é visto dessa forma, porque nós temos mais de 140 Municípios no Estado. Eu andei o Estado do Pará todinho, como policial, nos meus 30 anos. Eu acho que chega a 100 o número de Municípios no Estado que não têm sequer sinal de telefone móvel, imagine Internet! Eu gostaria de saber por que isso acontece, quando as operadoras de telefone têm condição de levar sinal de telefone, que deveria ser como o Luz para Todos. Então, sinal de telefone, sinal de Internet deveria ser para todos, não só para quem mora nas capitais, mas principalmente para a população que mora no interior. E falo pelo meu Estado, mas eu sei que no Brasil acontece em vários setores. Mas, na região do Marajó, na região do nordeste do Estado, há cidades que nem sequer têm sinal telefônico. E isso é um absurdo! Eu gostaria que as operadoras e aqueles que têm condição de fornecer nos digam o que está faltando. É questão de investimento, ou é questão de interesse, que não tem no Estado do Pará, nessas cidades, que não têm retorno? Eu gostaria de ter essa resposta.

Obrigado, Sra. Presidente.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Deputado Delegado Éder Mauro. Peço-lhe que faça o requerimento também por escrito, para colocarmos em apreciação nesta Comissão.

Com a palavra o nosso Primeiro Vice-Presidente, Deputado Leo de Brito, do PT do Acre.

O SR. DEPUTADO LEO DE BRITO - Obrigado, Sra. Presidenta Mariana. Saúdo aqui todos os Deputados e Deputadas, também fazendo um agradecimento especial aos expositores. Quero até fazer uma sugestão de que, no nosso *site* da CPI, constem todas as apresentações, que vão desde as apresentações relacionadas à segurança.

E aí eu queria fazer aqui um registro especial, Cristine, acerca do trabalho que está sendo feito pela CERT do ponto de vista preventivo, em relação à orientação aos usuários. Isso é fundamental. Nós estamos falando de crimes. Portanto, nós estamos falando de uma política de segurança pública também. E, quando falamos de segurança pública — está aqui o nosso Delegado Éder e vários outros membros que trabalham nessa área —, o trabalho preventivo tem um papel de grande relevância. Então quero saudar a CERT por esse trabalho que está sendo feito.

Passo, então, às perguntas, iniciando pelo Presidente Marcos Mazoni, sobre o Marco Civil. O Marco Civil da Internet está servindo de exemplo para outros países, como é o caso da Itália, do Reino Unido, Jordânia e outros, que têm seguido os passos deste Parlamento brasileiro. Como o senhor vê o Marco Civil da Internet no que tange à proteção da inovação na esfera da Internet no Brasil? Essa é uma pergunta.

Outro ponto que me chamou muito a atenção na exposição de V.Sa. diz respeito à questão do *software* livre, à utilização do *software* livre como mecanismo de segurança. O senhor compreende que seria interessante que a adoção do *software* livre em larga escala pela população seria uma parte da solução para muitos dos problemas de segurança cibernética e também um mecanismo de prevenção dos crimes cibernéticos.

O senhor falou da utilização na administração pública. Eu me somo à preocupação da Deputada Alice, no caso da NSA, e pergunto: em que medida o

sistema de processamento de dados do Brasil foi atingido por esse caso especificamente e como isso foi tratado pelo SERPRO? Houve algum incidente específico? Eu gostaria que o senhor explicitasse isso neste momento.

Para o Sr. Renato Martini a pergunta diz respeito ao Marco Civil. Na sua opinião, o Marco Civil veio contribuir para privacidade e segurança da Internet brasileira?

Para finalizar, Sra. Presidente, tenho duas perguntas para a Cristine. O Marco Civil da Internet estabelece que a legislação brasileira deve ser aplicada em caso de empresa de Internet, mesmo estrangeira, que preste serviço a brasileiros. O argumento de que a empresa é controlada por um grupo estrangeiro ou de que a empresa não esteja em território nacional é irrelevante. O Marco Civil da Internet expressamente exige que a legislação brasileira seja aplicada a esses casos. Como a senhora vê o Marco Civil da Internet como ferramenta jurídica para o auxílio ao bom funcionamento da Internet no Brasil?

Há uma questão importante que foi levantada pelos delegados da Polícia Federal, quando estiveram nesta Comissão Parlamentar de Inquérito. Durante a apresentação deles, na audiência, foi relatada a possibilidade de adoção do IPv6 como possível solução para a questão de segurança, uma vez que cada usuário teria IP fixo, e não mais IP dinâmico, como é hoje. De que maneira a adoção do IPv6 pode contribuir para maior segurança na Internet brasileira?

Seriam essas as perguntas, Sra. Presidente.

Muito obrigado.

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

Concedo a palavra ao Deputado Alexandre Leite.

O SR. DEPUTADO ALEXANDRE LEITE - Sra. Presidente, convidados, a minha pergunta é para o Marcos Vinícius. Se ocorresse uma catástrofe nas instalações do SERPRO, em Brasília, como funcionaria o Sistema SIAFI?

A segunda pergunta vem de alguns problemas que tivemos recentemente, devido a ataques direcionados ao Senador Aécio Neves por um dos Diretores do SERPRO, o Sr. Márcio de Araújo Benedito. Eu gostaria de saber se alguma providência foi tomada, no sentido de se instaurar sindicância ou algum

procedimento administrativo com relação a isso, que nos preocupa muito. Eu gostaria de saber como o SERPRO se protege.

Em 2013, nós tivemos um caso em que a Polícia Federal prendeu funcionários do SERPRO, uma quadrilha, devido a uma fraude de mais de 1 bilhão de reais. Todos os ataques foram desferidos de dentro do SERPRO. Eu gostaria de saber como o SERPRO se protege de si mesmo.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Para concluir esse bloco de perguntas, convido o Deputado Rafael Motta, Sub-Relator para casos de crianças e adolescentes, envolvendo também a pedofilia.

O SR. DEPUTADO RAFAEL MOTTA - Obrigada, Sra. Presidente, Deputada Mariana Carvalho. Devido ao avançado da hora, deixarei de fazer alguns questionamentos, pois já fui contemplado pela fala de alguns expositores. Mas ainda tenho duas perguntas que talvez sejam pertinentes nesta rodada. Serei direto.

Uma pergunta seria para a Sra. Cristine Hoepers. O nosso mandato teve acesso a alguns dados e estatísticas a respeito de *spam*. Essas informações foram reunidas por vocês a partir de reclamações nas plataformas SpamCop e Abusix. Entre essas informações, existem algumas que tratam da incidência da pedofilia. No sistema, salvo engano, a pedofilia aparece como incidentes de segurança. Gostaria de saber como se dá essa incidência e se existe alguma forma, através desses *spams*, de rastreio dessas crianças e adolescentes. E também queremos saber se o envio coletivo de mensagens pode ser utilizado para compartilhar imagens com conteúdo de pedofilia. São basicamente esses os questionamentos dirigidos à Sra. Cristine.

Tenho mais uma pergunta, que se direciona ao Eduardo Levy, Presidente do Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal. De acordo com o Marco Civil, as operadoras de telefonia não podem impedir o compartilhamento de informações, mesmo que contenham conteúdo de pedofilia. No caso, a retirada desses conteúdos só poderia ser feita através de decisão judicial, o que eu considero uma forma absurda, em vista do tempo em que essas divulgações ocorrem — o tempo na Internet é relativo em relação ao nosso tempo. Então, a pergunta é: após a decisão judicial que impede esse compartilhamento de imagens de exploração sexual de crianças e adolescentes,

quanto tempo a operadora tem para agir, ter essas informações a respeito das imagens e tirá-las de circulação, desses meios de divulgação?

É basicamente isso, Sra. Presidente.

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

Concluindo nossa rodada de perguntas, eu concedo a palavra ao Presidente do Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal — SINDITELEBRASIL, Eduardo Levy Cardoso Moreira. E já aproveito para agradecer a ele a presença e por ter aceitado o nosso convite para vir a esta Comissão. O senhor pode aproveitar para no final já fazer todas as suas conclusões e agradecimentos por estar nesta CPI, tendo em vista o horário do seu voo. Desde já, muito obrigada, em nome de toda esta Comissão.

O SR. EDUARDO LEVY CARDOSO MOREIRA - Muito obrigado, Deputada Mariana. Eu me coloco de antemão à disposição para retornar quantas vezes forem necessárias.

Vou procurar responder a todas as perguntas que me parecem que são para as empresas provedoras de conexão. Vou responder fora da ordem. Vou começar pela pergunta da Deputada Alice Portugal, porque eu percebi que, quando ela se referiu à Mesa, ela começou com a Cristine, que estava aqui presente.

As solicitações, Deputada, são respondidas como se queira. Muitas vezes, é solicitado que elas sejam impressas, porque elas vão integrar inquéritos. Então, vem uma informação oficial da empresa em papel para que ela possa integrar o processo. Mas, se quiser que seja em meio digital, também é feito em meio digital. Não há nenhuma restrição da nossa parte em relação a isso. Normalmente, a informação vai da forma como ela é pedida, como ela é solicitada.

Deputado Sandro Alex, a questão de solicitação de informações é tratada com tamanha restrição e sigilo dentro das nossas empresas que eu vou procurar lhe dar uma estimativa de quantas quebras de IPs são feitas. Eu tenho dificuldade de receber das empresas as informações, dada a restrição que nós temos, o cuidado que nós temos. Eu vou inclusive fazer algumas considerações a respeito disso *(falha na gravação)* dá mais de 10 mil por mês.

Respondendo um pouco aos outros questionamentos sobre as informações que nos são solicitadas e a rapidez com que isso é feito, Deputado Rafael Motta, o

atendimento é feito, em tese, imediatamente. Mas, como também comentou o Deputado Delegado Éder, são muito complexas as questões que são tratadas na Internet, porque não é como um celular que se pede: *"Bloqueie o número"*, e eu tenho aquele número e acabou. No caso da Internet, muitas vezes, alguém diz: *"Bloqueie determinada coisa"*, sem dar a informação do IP. Ou diz: *"Bloqueie tudo o que está acessando aquilo"*. O tamanho das redes e a quantidade de IPs geram um trabalho que é, mesmo conhecendo os dados, feito na medida em que se vai trabalhando, um passo depois do outro. Mas, muitas vezes, as informações vêm com poucos detalhes, trazem dificuldade na identificação. Então, a necessidade de se ter mais qualificação é realmente muito importante.

Eu falei, aqui, em tese, em mais de 10 mil bloqueios de IP por mês, mas nós tivemos uma vez uma solicitação de bloqueio de mais de 20 mil IPs. Uma só solicitação, envolveu um volume de trabalho, em uma determinada empresa, equivalente a 8 meses de trabalho que ela tinha na média. A resposta àquilo demandou um tempo maior do que a resposta a outras solicitações, em função simples e exclusivamente do volume requerido.

Eu vou tomar a liberdade de me meter em uma pergunta que não foi dirigida diretamente a mim para dizer que o setor de telecomunicações privado foi, por uma decisão do Estado brasileiro, privatizado. E 100% das comunicações brasileiras passaram a ser feitas através das redes de telecomunicações. O Imposto de Renda é feito por todo cidadão. Na eleição, todos votam, e toda a transmissão daquilo que fica na urna é feita pelas redes privadas de telecomunicações. Todos os bancos brasileiros, que tratam de toda a compensação bancária, todas as empresas que têm dados sigilosos — todas elas — não só fazem as suas transmissões através das redes privadas brasileiras, como armazenam seus dados nas principais empresas de telecomunicações brasileiras. Eu não posso aceitar que não seja considerada uma rede segura a rede de telecomunicações brasileira privada, que faz todo o transporte dessas informações no Brasil.

O Deputado Delegado Éder falou a respeito da informação e da venda de aparelho celular, que talvez não seja o tema principal, aqui, na nossa audiência, e também sobre o WhatsApp e sobre a própria cobertura de celular no Brasil.

Quanto à venda de telefone celular, quem já teve a experiência de ir a outro país e adquirir um c*hip* para utilizar durante o período de estadia ali sabe que, normalmente, o que se pede é o cartão de crédito, para fazer o débito do valor relativo ao uso do *chip*. Não se pede nem o passaporte — nem passaporte! Quem for a outros países verá que não se pede o passaporte. No Brasil, existem regras estabelecidas pela ANATEL que exigem determinadas informações que, infelizmente, são muito fáceis de serem fornecidas de outras pessoas. Existe também, felizmente, um serviço no Brasil, prestado por uma empresa que domina uma série de dados de consultas que são feitas, que é a SERASA, e ela informa quando alguém faz uso do seu CPF ou das suas informações para buscar alguma coisa.

Muitas pessoas já tiveram celulares colocados em seu nome, no seu CPF, sem ter o menor conhecimento disso. Mas, para evitar que haja proliferação disso e utilização de uma forma indevida, existem sistemas utilizados pelas empresas e que muitas vezes não são de conhecimento das pessoas.

Todos os que estão aqui presentes, se discarem dos seus aparelhos a sequência: asterisco, jogo da velha, zero, seis, jogo da velha, verá que aparece na tela uma sequência de números enorme. Este é o chassi deste “carro” aqui! Este é o chassi deste aparelho! O número é único no mundo. E este número que está aqui se chama IMEI, uma sigla americana.

(Intervenção fora do microfone. Ininteligível.)

O SR. EDUARDO LEVY CARDOSO MOREIRA - A sequência é: asterisco, jogo da velha, zero, seis, jogo da velha. Vai aparecer um conjunto de números. Esse número é único para o aparelho no mundo — único! Muitas vezes, na hora em que o aparelho é roubado, as pessoas têm por hábito, uma coisa que é da cultura mundial e brasileira, solicitar à empresa de telefonia celular que faça o bloqueio daquele número. O número é bloqueado. Quanto ao aparelho, se é encontrado, tira-se o *chip*, coloca-se outro *chip* e se utiliza o aparelho.

Na medida em que se possa fornecer o número desse chassi para as operadoras, esse número vai compor uma base brasileira de dados que tem um convênio com mais de 30 países, com mais de 97 operadoras no mundo, em uma

integração mundial para que não se possa usar aquele aparelho, mesmo fora do Brasil.

O cadastro brasileiro de aparelhos bloqueados já tem 5,5 milhões de aparelhos. O que nós procuramos fazer para ainda tentar aprimorar o processo e auxiliar não só os órgãos policiais, mas também as pessoas que foram furtadas? Nem sempre as pessoas se lembram de fazer isso ou têm conhecimento sobre isso, mas como em toda ligação telefônica existe algo que ouvimos, como o toque da campainha, o som de ocupado, a conversa que se faz — Mazoni sabe melhor do que outros aqui o que se passa na rede —, há algo que as pessoas não ouvem, como a troca de informações para saber onde você está, próximo a que Estação Radiobase você se encontra, se você está fora do Brasil, se aquele número está habilitado para receber a chamada, uma série de informações que são trocadas. E entre elas está a informação do IMEI, que também é enviada na troca de informações das empresas.

Nós estamos aprimorando, como disse o Deputado Delegado Éder — e não apenas na empresa que ele citou, mas em todas as empresas, com a exceção de uma, que já está pronta —, o sistema para que, ao se informar apenas o número, se o cliente quiser que se bloqueie o aparelho, nós buscarmos na ligação que ele fez por último o IMEI que foi usado e bloquear aquele IMEI. Isso já está sendo feito.

Não há também a necessidade mais de boletins policiais no Brasil inteiro; basta apenas a comunicação do cliente. Qual é o cuidado que se tem que ter sempre? Quanto maior a facilidade para que isso se faça, também maior a facilidade de alguém bloquear o aparelho de um terceiro. Então é preciso cuidado para se identificar muito bem quem está fazendo a solicitação.

No caso do WhatsApp, a questão é muito mais séria, muito mais grave. Nós somos o caminhão que transporta a informação, e existe uma plataforma em cima que utiliza as redes de telecomunicações para fazer as comunicações, entre elas o WhatsApp. O WhatsApp, que todo o mundo aqui usa, não tem CNPJ no Brasil e nenhum funcionário. Como é que se vai buscar a informação? Como se quer fazer o bloqueio ou se quer fazer enxergar o que está ali? Nós bloqueamos o número, nós transmitimos informação. O WhatsApp seria o equivalente do torpedo, da mensagem. Nós não armazenamos o conteúdo da mensagem passada. Nós

podemos, através de uma solicitação judicial, transferir para o órgão que nos solicitou a capacidade de enxergar o que por ali passa. Se o que por ali está passando é criptografado, não nos cabe mexer naquele conteúdo, naquela informação. É a vida global que nós temos que é assim. A vida global é assim.

Nós temos no Brasil, nas teles, 500 mil empregos diretos — 500 mil empregos! — e fazemos um investimento de 30 bilhões de reais, como eu mostrei aqui, por ano. Mas isso é para transportar as informações. Não vou dizer apenas porque sem esse transporte não existiria o resto, mas serviços que são caracterizados como serviços de valor adicional nem regulamentados são pela ANATEL, eles são livres.

Muito daquilo que se tem visto na imprensa quanto às nossas discussões em relação a esses serviços é exatamente por isso. Nós aqui pagamos impostos, aqui empregamos as pessoas, aqui fazemos as comunicações e temos muitas vezes competição — e nós não temos receio de competição, estamos muito acostumados com isso, todos aqui sabem —, mas a competição tem que ser equilibrada, não pode ser assimétrica, como ocorre com esse tipo de serviço.

Em relação ao Estado do Pará e aos demais Estados, o Brasil também tomou a decisão de, ao fazer a operação do serviço celular, estabelecer uma série de regras para que o serviço seja utilizado. Uma das regras diz respeito à abrangência geográfica do serviço.

O Brasil é um país enorme. As regras, no Brasil, são feitas de maneira uniforme, o que muitas vezes traz prejuízo, principalmente, a Estados como o do Pará, pelo tamanho do Estado e pela distribuição populacional. As regras brasileiras de telecomunicações preparadas pelo Estado brasileiro e implementadas pela ANATEL, através dos leilões celulares, estabelecem que há uma obrigação de se cobrir 80% da área geográfica do Distrito sede — 80% da área geográfica do Distrito sede.

O maior Município brasileiro em área geográfica é Altamira. Altamira tem um distrito que fica a 900 quilômetros de distância. A única obrigação estabelecida nas leis brasileiras, nas regras brasileiras, nos editais estabelecidos pela ANATEL, é cobrir 80% da área geográfica do Município de Altamira.

É fácil consultar o nosso *site*, o *www.telebrasil.org.br*. Todas as antenas estão lá. E todas as antenas estão dentro daquilo que estabelecem as regras de atendimento e são fiscalizadas. Mas é pouco.

O segundo ponto em relação à telefonia celular: não há obrigação de cobertura de um só metro de uma só estrada no País. Então, muitas vezes, os senhores, ao se deslocarem de um Município para outro, têm a queda da ligação, não há cobertura, porque ali não há uma obrigação de cobertura. Essa obrigação foi estabelecida. E, na hora em que se compra o direito para se poder fazer a implantação do serviço celular, tem-se um compromisso no valor do edital em relação à cobertura que se quer.

Poderia ser mais? É claro que sim. Só para o Fundo de Fiscalização existente no Brasil já foram recolhidos 60 bilhões de reais, e não se utilizou, até hoje, nem 10% disso. A implantação de uma Estação Radiobase custa, em média, 500 mil reais por *site* que se coloca. É só fazer a conta: há em caixa 50 bilhões de reais, cada estação custa 500 mil, em média. Quantas antenas o Brasil poderia ter a mais? O Brasil tem hoje em torno de 66 mil, 67 mil antenas de telefonia celular.

Para finalizar, novamente volto ao Deputado Sandro Alex, que comentou o *site* Tudo sobre Todos, perguntando se a neutralidade deve ser quebrada. Nós temos casos interessantes. Antes dessa questão sobre aquele conteúdo, eu vou falar sobre uma coisa um pouco técnica chamada Porta 25.

O que é a Porta 25? Foi só eu dizer Porta 25, e ela riu. Ela sabe o que é perfeitamente, mas é natural que quase ninguém conheça. Eu não a conhecia, antes de ser chamado a tratar do assunto. A Porta 25 é uma porta existente em computadores para fazer a comunicação entre as redes de computadores de uma mesma empresa. Normalmente ela não é utilizada pelos nossos computadores individuais, em nossas residências.

Através de *hackers*, através de criminosos, são colocadas, nas informações que nós baixamos da Internet, *softwares* ou informações nos nossos computadores, em casa, e esses computadores passam a ser verdadeiras máquinas de liberação de *spam*, passando *e-mail* para tudo quanto é canto, através da Porta 25, que por nós não é utilizada, mas, ao ser inoculado aquele *software*...

Estou certo no que estou falando? Mais ou menos, não é?

A SRA. CRISTINE HOEPERS - A metáfora está boa.

O SR. EDUARDO LEVY CARDOSO MOREIRA - A metáfora está boa.

O que foi feito dentro do Comitê Gestor, inclusive com a participação de órgãos de defesa do consumidor? Nós, empresas de telefonia, passamos a bloquear toda e qualquer mensagem que é originada de Porta 25 de computadores residenciais. Isso é quebra na neutralidade. Nós não estamos deixando sair a informação. Nós a estamos bloqueando na nossa rede, num acordo com o Comitê Gestor e com os órgãos de defesa do consumidor. E criamos problemas, porque alguns pequenos escritórios de advocacia, consultórios dentários utilizavam a Porta 25 para fazer saírem mensagens aos seus clientes, e elas foram bloqueadas.

Essa é uma ação positiva no mundo. O Brasil era um dos campões mundiais de *spam*, gerando um tráfego espúrio enorme. O País saiu da lista dos principais países que geravam *spam*, trazendo um benefício extraordinário.

É necessário entender que a neutralidade de rede é muito importante, mas a rede que existe no mundo precisa ser gerenciada, como qualquer rede de grande porte: redes de automóveis, redes de estradas, redes de rios. É preciso ser feito um gerenciamento. Nós não queremos, em nenhum momento, conhecer o conteúdo.

Também vem a pergunta do Deputado Rafael Motta, que fala sobre tirar conteúdo. Nós não tiramos conteúdo; nós bloqueamos o IP. Nós não sabemos o que está se passando ali dentro. Em relação à Porta 25, entendeu-se por todos que o que passava por ali era um crime. Por isso foi bloqueada.

Nós vamos ter daqui a pouco automóvel sem motorista. Vamos ter cada vez mais cirurgias feitas em localidades remotas, sendo acompanhadas por médicos especializados num determinado ponto, assim como nós temos um *e-mail* mandando uma informação para uma pessoa ou outra. Não é possível que sejam tratadas da mesma forma essas informações que são passadas na rede. Nós não podemos fazer isso. Temos que ter uma segurança muito grande em determinadas questões. Basta ver o exemplo dos *data centers*. Eles têm uma segurança de ar-condicionado e de energia elétrica melhor do que 99% dos hospitais brasileiros.

Obrigado.

O SR. PRESIDENTE (Deputado Rafael Motta) - Obrigado, Dr. Eduardo Levy. Sabendo que o seu tempo está um pouco exíguo, já que tem que pegar um voo,

agradecemos a sua presença e deixamos esta CPI à disposição para qualquer assunto a ser dirimido.

Queria aproveitar e passar a palavra para o Sr. Marcos Mazoni, Presidente do SERPRO, lembrando que, se possível, os nossos expositores sejam diretos em suas respostas aos questionamentos dos Deputados, visto que a sessão plenária já está na Ordem do Dia, inclusive com votação nominal.

Então, agradeço mais uma vez ao Sr. Eduardo e passo a palavra ao Sr. Marcos Mazoni.

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - A primeira questão colocada objetivamente foi sobre se o nosso ambiente é seguro. Sim, o SERPRO tem um ambiente bastante seguro. Não significa que os nossos outros parceiros de tecnologia no Governo também não o tenham. A DATAPREV tem um ambiente com muita segurança, o DATASUS também. Nós somos parceiros inclusive dos comitês de segurança. São características diferenciadas. O SERPRO tem uma característica de instantaneidade; a DATAPREV tem uma característica de longevidade. Os dados guardados na DATAPREV dizem respeito à vida das pessoas ao longo de todo o processo de relacionamento com o Estado brasileiro. Nós temos uma necessidade maior de estarmos no ar a todo instante, 24 horas por dia.

E aí a diferenciação que eu acho importante nessa questão da tecnologia. Quando falamos de Internet, nós estamos falando de uma coisa. Quando falamos de nuvem, nós estamos falando de algo um pouco diferente.

Eu brinquei um pouco com a palavra “resiliência”, para entendermos bem qual é a diferença. Por isso, eu comentei, naquele momento em que falava do Marco Civil, que, para mim, a coisa mais importante era a neutralidade, e não necessariamente os ambientes de *data center* estarem no Brasil. Se um provedor é internacional, não adianta colocar um *data center* no Brasil, porque a sua resiliência vai se estabelecer à medida que ele multiplicar esse dado em outros ambientes.

Eu mencionei que o Chile tem um *data center* que compõe a rede de nuvem do Google. Não significa que os dados dos chilenos estejam exclusivamente no Chile. Eles podem estar replicados, inclusive, no Brasil. Então, essa diferença, para mim, é importante.

Quando discutimos onde vão estar hospedados os dados, se a tecnologia utilizada é de Internet, é uma coisa, se é de nuvem, é outra. Então, como nós trabalhamos com as duas questões, como o SERPRO trabalha tanto com a Internet quanto com a nuvem, nosso ambiente é todo no Brasil. Nosso ambiente é todo dentro do nosso espaço territorial. Existe legislação específica, inclusive, dizendo que os dados têm que estar hospedados no Brasil. Então, nós usamos as duas tecnologias — tanto de nuvem quanto de Internet — dentro do ambiente brasileiro.

Não podemos ter dados fora do Brasil? Sim, podemos ter. Por isso, a classificação de dados é importante. Para dados públicos, abertos ou de testes de momentos de tecnologia, é claro que podem ser usadas plataformas desses provedores. Não significa que por não estarem aqui eles são inseguros. Significa que eles têm maior vulnerabilidade. Essa é a relação com que trabalhamos.

Quando falamos das vulnerabilidades, nós não estamos acusando nenhuma empresa, nada disso. Só estamos dizendo que há possibilidade de que alguma coisa aconteça. É como trabalhamos no caso dos seguros. Então, diminuímos as possibilidades de algo acontecer, diminuímos os riscos de vulnerabilidade do tamanho do investimento necessário, porque há essa relação: quanto vai me custar ter uma segurança absoluta de tudo? Fazemos isso na nossa vida, com os seguros que contratamos. Nós também trabalhamos nesse mesmo sentido.

Os *data centers* da DATAPREV, por exemplo, que estão no Rio de Janeiro e aqui em Brasília se replicam. São *data centers* de altíssima segurança. E o DATASUS, inclusive, utiliza-se dessas estruturas para fazer a sua replicação de informações. Então, nós temos uma cooperação bastante grande. E é evidente que eu, como Presidente do SERPRO, falei da estrutura do SERPRO.

Foi feita uma pergunta sobre o orçamento. Nós tínhamos, até 2006, um orçamento de investimentos que ficava na casa de 100 milhões de reais e pulamos para aproximadamente 300 milhões de reais por ano. Só na área de segurança, nós investimentos 50 milhões por ano.

Sim, tivemos problemas de fluxo de caixa no ano passado. O SERPRO não é só orçamento, o SERPRO fatura com os clientes do Governo Federal. É uma relação contratual. E, quando os nossos clientes têm o seu orçamento de custeio

diminuído, eles têm dificuldade de pagar as nossas faturas. Para eles, nós somos despesa. Nós não somos investimento para eles.

Nosso faturamento é algo em torno de 2 bilhões de reais, e nós investimos de 250 milhões a 280 milhões de reais por ano. Temos um custeio, por exemplo, com as operadoras de telecomunicações de 200 milhões de reais por ano.

Quando os nossos clientes têm dificuldades orçamentárias de cumprir com os compromissos com as nossas faturas, deixando faturas nossas em atraso... Neste ano, há atrasos de alguns fornecedores. Fizemos toda uma negociação com os nossos fornecedores e estamos reestabelecendo o fluxo financeiro.

Diminuímos o orçamento de investimentos deste ano, que era de 300 milhões de reais, para 180 milhões de reais. Como fizemos isso? Usando, inclusive, o avanço da própria tecnologia. É claro que seria muito bom se nós tivéssemos mais recursos para investir. Não há dúvida sobre isso. Nós tivemos que fazer escolhas e fizemos escolhas nas áreas que estão com alguma criticidade, que é o caso do CORE da nossa rede, da substituição dos roteadores de grande porte na nossa rede e da plataforma de *mainframe*, que precisa ser expandida para o ano que vem.

Nós estamos com total segurança neste ano, mas no Imposto de Renda da Pessoa Jurídica, por exemplo, vamos ter a entrada do eSocial. E há uma série de outros projetos que vão entrar e que vão precisar de mais capacidade de máquina para suportar tudo isso. Então, nós fizemos uma restrição, mas focamos nesses investimentos para que nós tenhamos certeza de que nós suportaremos os serviços que vão entrar no ano que vem.

Isso é um pouco técnico, Deputado, mas a entrada dessa nova ferramenta que nós desenvolvemos, a Demoiselle 2.5, tira o processamento centralizado e joga mais processamento para as pontas. Nós falávamos muito aqui de tecnologias de nuvem, e nós estamos brincando agora, dizendo que nós estamos utilizando a tecnologia de *fog*. O que é o *fog*? Eu tenho uma nuvem, mas eu processo bem perto do chão, por isso essa brincadeira com *fog*. Essa ferramenta tirou 40% da necessidade de processamento. Então, isso me dá sobrevida, inclusive para a minha estrutura suportar aplicações de tecnologia baixa. Mas quanto às aplicações de tecnologia alta, que é o caso dos *mainframes*, eu precisei manter o investimento

neste ano para que eu possa suportar no ano que vem o aumento da demanda de novos serviços.

O nosso orçamento está na casa de 2 bilhões de reais. Mas nós utilizamos os avanços tecnológicos, porque nós tínhamos, em 2007, quando eu assumi o SERPRO, mil serviços no ar; hoje nós operamos 4.600 serviços do Governo Federal brasileiro. E o orçamento não cresceu. Fica em torno de 60% o crescimento do orçamento do SERPRO nesse período. Quer dizer, nós crescemos quatro vezes em termos de serviços, mas crescemos em torno de 60% em termos de orçamento, usando todas essas tecnologias. Quando eu saía de 180 *terabytes*, eu comprava área de armazenamento em *mainframe*, agora eu compro área de armazenamento para nuvem. O que eu faço agindo assim? Eu uso tecnologias que custam quatro vezes mais barato do que as que eu comprava antes. Então, eu consigo fazer essa expansão, mesmo com um orçamento que não cresceu no volume que nós precisaríamos, explorando ao máximo as tecnologias existentes.

O SR. DEPUTADO SANDRO ALEX - Presidente, então o orçamento era de 300 milhões de reais, houve um corte e este ano ficou em 180 milhões de reais, é isso?

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - Isso.

O SR. DEPUTADO SANDRO ALEX - E qual é o tamanho do débito que vocês têm?

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - Com fornecedores?

O SR. DEPUTADO SANDRO ALEX - Isso, o débito que está em aberto, segundo o senhor falou.

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - Nosso débito com fornecedores é em torno de 60 milhões de reais. Nós estamos colocando ele em dia. Provavelmente no mês de outubro nós encerraremos o débito com fornecedores. Ficaremos absolutamente em dia.

O SR. DEPUTADO SANDRO ALEX - Para o ano que vem qual é a previsão?

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - Para o ano que vem, a previsão do orçamento continua em 2 bilhões de reais, mas nós estamos inclusive procurando novos serviços que vão nos dar a possibilidade do crescimento. Existem alguns serviços, como, por exemplo — vocês devem ter ouvido nos noticiários —,

toda a parte de consignação que não era feita pelo SERPRO e, a partir deste mês de setembro, começa a ser feita pelo SERPRO. Isso é um acréscimo de 40 milhões de reais no nosso orçamento, valor que não é pago pelo Governo Federal, porque aquele recurso é um recurso pago pelos bancos. Então, nós passamos a prestar esse serviço para a rede bancária. Isso aumenta o nosso orçamento.

Nós estamos aumentando serviços na Casa da Moeda, que antes eram feitos por uma empresa privada — vocês também devem ter ouvido notícias sobre isso. Nós estamos entrando com alguns serviços lá para fazer essa substituição. Isso aumenta o nosso orçamento.

A Zona Franca de Manaus era atendida por uma fundação, e nós assumimos agora os serviços da SUFRAMA. Isso também representa um incremento de 40 milhões de reais no nosso orçamento. Já neste ano deve dar em torno de 20 milhões de reais e, no ano que vem, serão 40 milhões de reais.

Então, nós estamos crescendo em outros serviços para poder fazer o crescimento dos recursos, já que o orçamento da operação centralizada se manteve para o ano de 2016 igual ao do orçamento de 2015.

O SR. DEPUTADO SANDRO ALEX - E esse corte não comprometeu o trabalho de vocês?

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - Deputado, não comprometeu do ponto de vista de nós termos alguma situação de instabilidade, mas nos tira de uma área de conforto, sem dúvida nenhuma.

Nós resolvemos investir mais na área de segurança da informação e talvez alguns serviços que nós tivéssemos maior capacidade de atendimento, maior folga de atendimento... Na plataforma alta, nós trabalhamos muito no limite, porque um *mainframe* é muito caro. Se eu usá-lo pela metade, ele fica caríssimo. Eu tento usá-lo o máximo possível. Nós o usamos na casa dos 90%. Para vocês terem uma ideia, um computador desses aqui nós usamos na casa de 15% da capacidade dele. O *mainframe* nós usamos na casa de 90% da capacidade. Nós estamos batendo nos 95%. Então, eu preciso fazer um investimento para ele voltar aos 90%. O certo seria eu nunca ter saído da casa dos 90%. Ele funciona bem até 99%, isso é padrão. Em outros lugares dos quais já fui Presidente, como no caso da CELEPAR, nós trabalhávamos na casa dos 97%. O SERPRO trabalha na casa dos 90%, porque eu

tenho uma variação muito grande de serviços: serviço da folha de pagamento da União, o SIAFI. Eu tenho situações que são muito arriscadas — e eu até vou em seguida responder à pergunta sobre se houvesse alguma parada nos nossos ambientes —, mas o SERPRO tem uma vantagem em relação a essas outras estruturas que eu já administrei, porque nós temos mais de um centro de dados. Então, eu tenho balanceamento de serviços. Quando uma máquina está mais carregada, eu consigo distribuir mais geograficamente. Nós temos balanceamento geográfico — talvez seja uma das poucas aplicações do mundo que fazem isso — no ambiente de *mainframe*. Nós só falamos de nuvem num ambiente de plataforma baixa, mas no ambiente de *mainframe* nós conseguimos colocar no ar, uns 4 anos atrás, o balanceamento geográfico, que nos permite inclusive essa solução para o Imposto de Renda, usando os dois ambientes.

Então, nós estamos seguros da continuidade dos nossos serviços. É claro que o orçamento está restrito e nos cria algum nível de dificuldade. Se dissesse que não, eu estaria faltando com a verdade aqui.

O SR. DEPUTADO SANDRO ALEX - E o satélite TELEBRAS?

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - Bom, o satélite TELEBRAS — até faz parte aqui de uma das perguntas —, que estará no ar no segundo semestre do ano que vem, é um satélite estacionário que vai permitir que o Brasil tenha cobertura de Internet muito melhor do que nós temos hoje. Ele vai cobrir o território nacional. Ele é estacionário e é focado na Internet, não é focado em voz. Os satélites de voz são satélites também estacionários, mas que usam tecnologias que têm a mesma capacidade de *upload* e de *download*, e o satélite de Internet precisa de uma capacidade muito maior de *download* do que de *upload*. Nós subimos coisas na Internet em muito menos quantidade do que nós descemos. Nós vemos mais coisas do que carregamos para cima. Então, esses satélites que têm essas tecnologias estarão no ar em 2016.

O SR. DEPUTADO SANDRO ALEX - Mesmo com o corte do orçamento, não há risco?

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - Não, não há risco, porque é um consórcio que inclusive envolve várias empresas privadas também. Então, o satélite estará no ar em 2016 com certeza.

Aqui também foi colocada a questão da eficácia das redes, como, por exemplo, a do Banco Central. O Banco Central opera uma rede toda de comunicação do setor bancário, uma rede que trafega texto. Então, não é uma rede que necessita de *performance* muito alta, porque não existe imagem, não existe voz, que são os pacotes mais pesados. O setor bancário é um setor altamente desenvolvido, mas o tamanho do arquivo transacionado é muito pequeno. Nós conhecemos muito essa estrutura, porque no SIAFI nós temos uma rede paralela. Nós tiramos a arrecadação de D -1 para D 0.

Nós operamos hoje com 70 instituições bancárias. O SERPRO também tem uma rede parecida com a do Banco Central, e é uma rede de texto. Então é uma rede bastante tranquila de ser operada, e o Banco Central faz isso com muita eficiência, tanto é que ele fiscaliza o nosso ambiente também. Eu acho que estamos muito seguros com aquela rede, porque o padrão da FEBRABAN é um padrão bastante simples, com poucas agregações, como é o caso da nota fiscal eletrônica, que são imagens de texto que nós carregamos com muita facilidade dentro do nosso ambiente.

Quanto à relação Brasil-Estados Unidos, realmente nós tivemos que fazer uma intervenção um pouco mais pesada naquele momento. Não é nem uma questão especificamente de governos, porque os acordos de governos existem, mas a nossa preocupação era no uso de ferramentas que obedeciam à legislação norte-americana. As próprias empresas dos Estados Unidos questionam o Governo norte-americano sobre isso, porque se para nós é uma questão de preservar a privacidade do cidadão brasileiro eles entendem que é de preservar o sigilo do seu cliente. Eles entendem assim. As grandes empresas norte-americanas têm um grupo de trabalho junto ao Governo norte-americano. Eu participei desse debate na Câmara de Comércio Brasil-Estados Unidos, em Nova Iorque, onde eles pediram a sua absoluta liberação sobre esses padrões que são exigidos do Governo norte-americano. E nós temos tido uma excelente parceria com eles, inclusive na remoção desses elementos chamados de *backdoor*.

A Porta 25, na verdade, é um *backdoor* de um produto, de um sistema operacional. O sistema operacional não tinha sido pensado para trabalhar com a Internet e foi adaptado. Então, foram criadas adaptações para isso.

Nós não temos esse problema porque nosso ambiente é todo com Linux; então nós dominamos as plataformas. Não é que não existam *backdoors* em ambientes de *software* aberto; existem. Existe um produto chamado Ubuntu, por exemplo, que é Linux, que tem uma série de possibilidades de comunicação. Mas vamos lá e o desligamos. Essa é a vantagem. Temos acesso aos códigos. Vamos lá, nós o desligamos e resolvemos o problema.

Então, não estou dizendo aqui que um produto é melhor que o outro. A vantagem é que eu tenho acesso, e com esses acessos eu consigo fazer as minhas soluções. E eu não preciso ficar esperando as chamadas correções de *bugs*. Quem não teve que aplicar um *patch*? O que aplicar um *patch*? É quando um fabricante daquele produto avisa no mundo que o seu produto tinha um problema. E, quando ele avisa no mundo que seu produto tinha problema, ele diz: *"Olha, está aqui a ferramenta que resolve este problema"*. Quando ele diz isso, ele diz às pessoas do bem e às pessoas do mal. Aí, as pessoas do mal, então, têm um espaço. Até você aplicar aquilo na sua instalação, elas têm um espaço de usar aquela porta, usar aquele problema para operações maliciosas, vamos chamar assim.

No mundo do *software* livre, nós fazemos isso constantemente. Nós estamos sempre em rede, operando nas comunidades internacionais, e nós estamos fazendo as alterações e correções, o que é natural. Nenhum produto de *software* não tem problema. Não existe produto assim de *software*. O produto de *software* é um produto de engenharia, mas é também de inteligência individual. É natural que tenha problema. A gente não testa cem por cento um sistema operacional que coloca no ar — eu digo "a gente", o mundo da comunidade do desenvolvimento de *software* —, porque não se sabe todas as coisas. Senão, nós jamais colocaríamos o produto a tempo de ser usado, se o testássemos o tempo todo.

Então é natural que problemas sejam corrigidos. Só que existe uma forma, que a indústria faz, que é botar e avisar. Achamos um problema e o corrigimos. No outro, estamos trabalhando em rede constantemente, e por isso dizemos que *software* livre é realmente uma excelente solução para aumentar a segurança porque estamos constantemente atuando, resolvendo e melhorando. E temos acesso ao que ele faz, porque, muitas vezes, nesses outros produtos, poderíamos

até saber dos problemas antes da própria indústria, mas não sabemos porque não temos acesso aos códigos.

Então, nós achamos, sim, que a questão da política do *software* livre é muito importante. Eu coordeno o Comitê de Implementação do Software Livre no Governo Federal, e temos defendido intensamente isso. Nosso ambiente de nuvem é complemente em *software* livre; nosso ambiente de desenvolvimento é completamente em *software* livre.

Vou fazer uma pequena propaganda aqui. A nossa ferramenta de desenvolvimento chama-se Demoiselle, porque é uma homenagem ao Santos Dumont. Os irmãos Wright voaram 3 anos antes do Santos Dumont; só que eles queriam vender a patente do avião. Para isso, eles tinham que ter algo que fosse exclusivo deles. E eles fizeram algo exclusivo. Os aviões do irmãos Wright, os Flyers, para fazer curvas, torciam as asas. Vocês imaginam um avião, hoje, com 300 pessoas, torcendo as asas, como seria a sensação de quem está dentro do avião! Mas essa era a patente que eles tinham. Eles levaram 10 anos para desenvolver os Flyers.

O Santos Dumont, 2 anos depois que eles fizeram o implemento deles voar, foi convidado a fazer o mais pesado que o ar. O Santos Dumont o fez em 1 ano. Por quê? O Santos Dumont juntou todas as inteligências que existiam disponíveis na época, porque já existia, já se sabiam as regras da física, Pitot, Venturi. Tudo já se sabia. Já havia motor, já havia roda. O que ele fez? Ele juntou tudo aquilo. Quando ele foi chamado para fazer a patente do avião pela França, ele pegou a revista técnica da época. Ele já estava no número 20, que era conhecido por Demoiselle. Ele pegou a revista técnica da época, escreveu todas as especificações do seu avião, e escreveu embaixo: *"É possível copiar. É possível alterar. Não é possível patentear. Este é um bem que eu deixo à humanidade"*.

Então, a tecnologia com que nós voamos hoje é completamente de Santos Dumont, apesar de os irmãos Wright terem voado antes que ele. Então, o Pai da Aviação é Santos Dumont. Nós fizemos esta pequena homenagem a ele.

Sobre a questão do WhatsApp que já foi até mencionada, é isso mesmo que o Levy disse. Quer dizer, é um pacote que está fechado e é hospedado nos Estados Unidos. Então, para se conseguir os dados da informação, tem-se que fazer

requerimentos ao provedor onde ele está. Mesmo assim, a neutralidade da rede tem essa importância, porque senão todas as operadoras de telecomunicações, para quebrar a neutralidade da rede, por questões comerciais, teriam que conhecer o conteúdo dos pacotes: *"Aqui vai um vídeo". "Aqui vai uma imagem"*.

Então, hoje, que eles não são protagonistas nesse debate, passariam a ser protagonistas nesse debate, porque nós teríamos mais um ponto de fragilidade. Eles teriam que abrir os pacotes. Então, tudo o que Levy disse está corretíssimo; só que eles teriam que abrir os pacotes se nós quebrássemos

Nós teríamos mais um ponto de fragilidade e eles teriam que abrir os pacotes.

Então, tudo o que o Levy disse está corretíssimo. Só que eles teriam que abrir os pacotes, se nós quebrássemos a neutralidade da rede. Por isso é que eu dizia na época que, no meu ponto de vista, a neutralidade era muito mais importante do que a questão do censo de dados. O censo de dados é uma política industrial. É legal que todos tenham. As operadoras todas têm censo de dados no Brasil. É muito bom que tenham. Isso gera emprego e renda. Isso dá velocidade, dá performance. É muito bom que tenham. Mas isso não garante, nas tecnologias de nuvem — talvez nas de Internet, sim —, nenhuma proteção. Não elimina essa fragilidade.

Processo de inovação do marco civil: acho que ele está preservado também pela neutralidade na rede. Se nós queremos ir à inovação aberta — o mundo inteiro está indo à inovação aberta —, nós temos que deixar que os pacotes flutuem nessa rede. Se eu começar a achar que algum pacote de algo que está sendo desenvolvido, que não está pronto... Se eu tiver dúvida sobre isso, se eu cortar o pacote, porque tenho suspeita sobre o pacote, eu estou matando a inovação aberta que pode ser feita em cima da rede. Então, o marco civil, na própria questão da neutralidade, preservou um espaço de desenvolvimento aberto na rede. Para vocês terem uma ideia, as principais inovações que estão acontecendo no mundo são inovações que se dão dentro da Internet. O maior provedor de táxi do mundo não tem um táxi, chama-se Uber. O maior provedor de soluções de saúde não atua na área de saúde. E assim vai. E eles estão se estabelecendo onde? Eles estão se estabelecendo nos Estados Unidos. Nos Estados Unidos, eles têm uma preocupação de sigilo dos pacotes. Eles não estão acontecendo na China. Há uma empresa, inclusive, chinesa, recém-construída, que faz localização. Simplesmente,

você está entrando na Internet, você gosta de alguma coisa, marca e ela guarda aquela localização. Essa empresa chinesa está nos Estados Unidos. Era uma possibilidade de renda, inclusive na China. Foi para os Estados Unidos, porque, na China, eles abrem os pacotes de tudo. Então, a neutralidade da rede é fundamental para a inovação e para o crescimento.

A questão do IPv6, sim, para nós é algo superimportante. Os portais, hoje, da Presidência da República, todos eles já estão em IPv6, o que garante... Os *browsers* têm essa possibilidade. Não há custo para os usuários finais. Então, nós temos uma maior garantia, porque tem ali um *range* de endereços IP muito maior. Eu consigo dar um para um. Então, a questão do endereço IP é importante. Nós estamos implementando nos ambientes brasileiros.

Se houver alguma crise no nosso centro de dados de Brasília, o SIAFI levanta automaticamente em São Paulo. Então, esse balanceamento geográfico que nós fizemos com os dois ambientes — e eu estou falando só desses dois; não estou falando do Rio porque eu não tenho *mainframe* no Rio —, em tudo o que depende de *mainframe*, o balanceamento é entre Brasília e São Paulo. Este está balanceado. Nós temos 36 sistemas críticos que estão balanceados. Todos estão? Não. Nós operamos milhares de sistemas. Mas 36, evidentemente que o SIAFI e todo o ambiente da Receita Federal, estão balanceados, Então, se cai um, levanta o outro. Essa é uma garantia...

O SIAFI tem um padrão de carga que é bastante específico. O padrão de carga do SIAFI está sempre numa carga muito baixa, durante todo o ano. E ele aumenta muito a carga nos momentos de lançamento do Orçamento do ano seguinte. Depois que vocês fazem as alterações, as aprovações, esse Orçamento vai para o Ministério do Planejamento. E nós começamos a fazer carga de autorização legislativa para o ano seguinte. Então, esse é um momento de carga. Final de ano é um momento de carga para o SIAFI. Então, é um momento mais crítico. Nós podemos tirar prioridades de outros sistemas menos críticos, se acontecer uma situação dessas.

O SR. DEPUTADO ALEXANDRE LEITE - No caso de colapso de um, o outro suporta todo o armazenamento?

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - O outro suporta toda a operação. O SERPRO é a parte de armazenamento até pequena, é texto. Os dados são números e texto, não têm imagens. Ele é bastante leve de levantar em outro lugar. O SIAFI tem uma característica. Como todo ano ele tem aprovações diferenciadas, nós temos ambientes para cada ano. Então, nós ficaríamos com o ano em curso, sem nenhuma dificuldade. E eu posso tirar. Existe um produto que faz com que eu possa tirar prioridade de outros para jogar em cima dele. A gente já faz isso de maneira normal, em situações desses momentos de peso maior. E eu posso fazer isso numa situação de crise, tirar outros. Tirar significa dar menos prioridade de resposta a outros sistemas, para manter esses. Então, dos 36 sistemas críticos nós temos esse balanceamento geográfico entre Brasília e São Paulo. A gente garante estabilidade neles.

Deputado, V.Exa. fez referência à questão do ataque ao Senador Aécio Neves. Eu vou explicar um pouco. Primeiro, ele não é diretor do SERPRO. Ele é funcionário de Belo Horizonte. Todos os nossos diretores são aqui de Brasília. Nós somos sete diretores. Está lá o nome de todos no nosso portal. Ele é funcionário de Belo Horizonte.

O SR. DEPUTADO ALEXANDRE LEITE - Ele nunca ocupou cargo de chefia lá?

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - Ele é chefe de uma unidade dentro da nossa universidade coorporativa.

O SR. DEPUTADO ALEXANDRE LEITE - Ah, sim!

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - Ele é de um nível inclusive bem mais baixo. Nós só temos chefes departamentais nas regionais; nós não temos diretores e superintendentes — estão todos aqui em Brasília. E nós só somos cinco pessoas de fora da empresa. O resto todo é de funcionários mesmo. Eu sou um dos que sou de fora, porque dos sete diretores dois são funcionários estatutários. Esse funcionário fez acesso por uma rede externa do SERPRO, que não é uma rede do SERPRO, e foi aberta sindicância no Ministério da Fazenda a respeito desse caso específico. A sindicância está em curso, e não tenho como lhe dizer o que vai proceder. O Ministério da Fazenda e a Corregedoria fazem o processo de sindicância e mandam para nós. É assim que funciona, inclusive nos casos que o

V.Exa. citou. Eu sei especificamente qual V.Exa. citou. Dos casos que são muito noticiados evidentemente que V.Exa. se lembra. Houve aquele episódio, em 2010, de vazamento de informações também de um Senador do PSDB, na época, do Serra, da filha dele. Esses são acessos logados feitos em lojas da Receita Federal, que têm autorização, estão logados, e a partir de denúncias vai para a Corregedoria do Ministério. Naquele caso, as pessoas inclusive foram demitidas. Esses funcionários não ficam dentro do SERPRO. São 3 mil que trabalham nas unidades da Receita Federal. Então, quando eu falo 8 mil, na verdade nós temos 11 mil funcionários. Mas 3 mil eu não administro; esses ficam dentro das unidades da Receita Federal. Eles são logados como Receita Federal, mas nós temos todos os *logs* disso.

Implementamos, naquele momento inclusive, gestão de identidades. Como eu falei aqui, é logar todos os funcionários, inclusive todas as plataformas do SERPRO. Fizemos essa implementação. Hoje nós sabemos exatamente o que todos os nossos funcionários fazem. Eu sei que V.Exa. sabe exatamente porque o nosso maior risco de vulnerabilidade em uma rede desse tamanho com essa quantidade de gente mexendo é interna. Então, nós temos que ter toda uma preocupação de como a gente loga todo mundo, é claro que com alguns elementos de verificação. Esse elemento que V.Exa. colocou não foi um caso externo; foi um caso interno no Rio de Janeiro. A gente checa os lotes das devoluções de Imposto de Renda que vão para os bancos. Isso era uma manipulação que era feita. Foi feita uma manipulação em um lote que não estava mais ativo. Por isso é que alarmou, e nós chamamos a Polícia Federal, que inclusive fez uma perícia forense na máquina e tal. Claro que essa pessoa não foi só demitida, mas responde — está em liberdade — a um processo contra ela. Porque nós pegamos, com esse *software* de rastreamento que a gente tem, tudo o que acontece na rede.

Pode estar acontecendo alguma coisa agora? Pode estar acontecendo. Por esses *checks* que fazemos a gente consegue descobrir. Todos os dados que temos a gente guarda a vida inteira. Por isso, Deputado, é que a gente inclusive segregou a rede do SERPRO. Nós segregamos a rede do SERPRO, em acordo com o Ministério Público do Trabalho. Nós logamos absolutamente tudo o que é feito na rede profissional do SERPRO. Criamos uma rede *wi-fi*. Se o funcionário quiser usar

o *Gmail* ou outras coisas, ele não pode usar dentro da rede da empresa. Nós bloqueamos todos esses acessos internos. Então, o caso inclusive do Senador foi através de uma rede; não foi nem dentro do SERPRO, mas foi em uma rede, se eu não me engano, aqui da Escola de Administração Fazendária. A pessoa estava em curso na Escola de Administração Fazendária e fez um acesso pela rede *wi-fi*, fora do nosso ambiente. O Twitter e tudo mais é bloqueado na nossa rede. Nem eu tenho acesso a Twitter, dentro da rede do SERPRO. Então, é tudo bloqueado. Esses acessos são feitos em uma rede paralela que nós fizemos, porque o Ministério Público do Trabalho entendia que ou nós bloqueávamos tudo, ou nós liberávamos tudo. Então nós resolvemos bloquear tudo numa rede e liberar para uma rede particular, vamos chamar assim, para que os funcionários possam ter acesso. Às vezes, eles têm que ter acesso até para testar soluções. Nós estamos com uma solução agora, a do *Dialoga*, que é uma plataforma de democracia digital, que é preciso saber se funciona via *Facebook*, via outras aplicações também. Então, as pessoas até têm que testar, mas testam numa rede fora do nosso ambiente, porque o nosso ambiente é absolutamente bloqueado — todos os endereços dessas plataformas. Então é assim que o SERPRO se protege.

Eu creio que eu consegui passar por todas as perguntas. Estou à disposição para novas perguntas.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Agradeço ao nosso Presidente Marcos Vinícius Mazoni, Diretor-Presidente do SERPRO.

Concedo a palavra ao Diretor-Presidente do Instituto Nacional de Tecnologia da Informação, Dr. Renato Martini.

O SR. RENATO MARTINI - O meu vai ser bem rápido. Foi-me feita uma pergunta diretamente. Eu só quero fazer dois comentários, antes de tocar no tema que me foi perguntado de forma mais explícita.

Essa questão da criptografia de um aplicativo como o WhatsApp… Eu acho que é importante que a CPI tenha noção de que a criptografia de dados de qualquer aplicação, de uma certa forma, considerando-se a qualidade da criptografia — se ela é feita em *hardware* ou em *software* —, o tamanho da chave criptográfica que é usada torna-se inquebrável. Então, afora a questão de ter CNPJ, de não ter CNPJ, se você realmente intercepta com autorização um dado que é criptografado, se ele

tiver qualidade e se houver emergência no acesso a esse dado — é evidente que você pode aplicar *hardware* e tempo —, você pode até quebrar um dado criptográfico, mas você vai precisar de um poder computacional gigantesco em 1 ano, às vezes. E, às vezes, você não tem esse tempo. Então, de uma certa forma, é difícil fazer uma generalização, mas ele pode ser qualificado de inquebrável.

A observação que fez o Deputado Delegado Éder… Ele exemplificou aquilo que eu falei. Nós, do poder público, nós, que atuamos no lado do poder público, que obedecemos à norma e à legalidade, temos uma lentidão, não só por ter a obrigação de obedecer à lei, mas porque são estruturas mais pesadas, mais burocráticas, nós temos jurisdição, nós temos atribuições que têm que ser respeitadas, e o criminoso, o fraudador não tem nenhuma dessas restrições. Então, ele leva vantagem sempre e tem mais agilidade em relação a nós, do poder público. Estamos derrotados? Não. Eu acho que o que pode ser feito é o compartilhamento de informações, o trabalho cooperativado, fazer a informação circular com mais velocidade e com mais agilidade entre as diversas esferas do poder público. Mas acho que a fala do Delegado Éder exemplificou. E acho que ele tem a experiência concreta, mais do que ninguém, de ter percebido na prática isso.

A respeito da pergunta sobre o marco legal, eu acho que o Marco Civil da Internet, enquanto um marco legal, acho que foi importante para consagrar no Brasil uma visão de cidadania da Internet e para fazer a sociedade brasileira entender, assim como o Governo, que nós estamos falando de uma plataforma aberta extremamente complexa, em mutação, que faz colidir, de uma certa forma, o mundo que nós conhecemos no século XX. Por exemplo, falam muito de telecomunicações e Internet. As telecomunicações são um mercado regulado, que vem do século XX, e a Internet é uma nova fronteira, extremamente complexa relativamente ao mundo das telecomunicações. Então ela foi extremamente importante para isso, e trouxe o tema da privacidade, o sigilo da informação como um tema de cidadania muito importante. Mas acho que não se aportou grandes ferramentas, no que tange à segurança na Internet, à segurança do sistema de informação. Eu acho que ela demandará mais regramentos e leis mais específicas que possam contribuir e trazer mais segurança para o cidadão, para esta sociedade que cada vez mais se torna uma sociedade digital.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Concedo a palavra à Sra. Cristine Hoepers, Gerente-Geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil — CERT.br.

A SRA. CRISTINE HOEPERS - Muito obrigada. Vou tentar responder da maneira mais breve possível aqui aos questionamentos.

O primeiro é sobre os requisitos para se ter o domínio ponto br. Uma coisa que eu acho importante deixar claro é que o ponto br é um dos domínios de primeiro nível, como é chamado, mais restritivos que existem. Para você conseguir registar um domínio, você precisa ter um CNPJ ou um CPF e precisa estar estabelecido no País. E essa é uma restrição que há em poucos lugares. Então, ela já é bastante restritiva. Há um cuidado muito grande em fazer a checagem de documentação quando necessária, e os dados são todos tratados por um tratamento jurídico, por um departamento interno nosso.

É importante deixar claro também que no Brasil temos uma autonomia muito grande com relação à numeração IP. Quer dizer, é um dos comentários utilizados no mundo... Assim como o telefone tem que ter um número único, o IP, que é o endereço de qualquer dispositivo na Internet é único. A maioria dos países consegue essas numerações com os órgãos regionais, que são chamados de registros regionais.

O Brasil é um dos poucos países que têm uma autonomia. Nós temos o que é chamado de National Internet Registry, ou seja, nós temos o registro nacional e nós temos autonomia inclusive para colocar até mais restrições em relação a quem pode ou não ter um endereço IP. Eu acho que o Brasil está muito bem estruturado. Eu acho que tem um balanço muito bom entre a agilidade e... Porque você não pode também levar meses para ter um domínio para começar algo na Internet. Ele é rápido, mas eu acho que ele tem toda a coleta de dados que se faz necessária, se houver algum problema.

Portanto, eu creio que a nossa área jurídica teria condições de explicar isso melhor. Se alguém tiver mais dúvidas, favor entrar em contato com eles até para que expliquem isso melhor. Hoje, sim, há várias regras.

E, já que eu estou falando de numeração IP, tinha um questionamento do Deputado Leo de Brito sobre IPv6. É bom lembrar que, assim, o IP é único. A

primeira versão de numeração IP que foi implantada na Internet, quando do nascimento, mesmo oficial, desse protocolo, foi chamada de IP versão 4, IPv4. O grande problema é que acabou, a numeração esgotou. Não tem mais como aumentar isso. E, ao contrário, por exemplo, quando o CEP era muito restritivo, tivemos um período em que eram só cinco números. Agora, são cinco números mais três dígitos. O telefone celular aqui no Brasil, as capitais já estão começando... Lá em São Paulo já tem um número a mais. Na Internet você precisa colocar um novo protocolo, uma nova numeração.

O que está acontecendo hoje é que vai haver um período de coexistência entre a versão antiga e a nova, e a técnica que está sendo usada para esse período de transição está dificultando as investigações. Você acaba tendo, atrás de um único número IP, muitos números. Você precisa de mais elementos para fazer a investigação, você precisa de mais dados, que são difíceis de ser registrados por quem está fazendo as aplicações.

O que vai acontecer quando a gente tiver o IPv6 implantado — e isso é um trabalho muito grande de outra área lá do NIC.br, de treinar profissionais, já foram mais de 3 mil profissionais de operadores e provedores treinados — é que você passa a não precisar mais de ter um único endereço divido às vezes por mil, 2 mil, 3 mil pessoas. Mas esse endereço não tem o conceito de portabilidade de endereço IP.

Quando você está viajando com o celular, o número do celular em São Paulo é o mesmo número do celular em Brasília, etc. O IP, não! Se eu estiver usando o meu celular aqui, quando eu for para o *cybercafé* para pegar *wi-fi*, ele vai ter outro número; quando eu estiver em casa, ele tem outro número. Porque o IP é muito mais associado ao CEP. Embora não geograficamente, ele está estabelecido com as redes. Quer dizer, um bloco de endereços IPs tem uma regra de formação na qual você precisa atribuir para uma entidade, que é o que é chamado de sistema autônomo, que pode ser uma empresa, pode ser um órgão de governo. E esse conjunto de IPs está associado àquele sistema, e você precisa rotear para lá. Então, ele não é um IP que vai ficar fixo para uma pessoa. Não vai mais haver esse compartilhamento em larga escala. Vamos voltar, na verdade, ao que era a Internet de uns 15 anos atrás, em que você tinha IPs para todos e não era necessário fazer

esse compartilhamento tão agressivo. Mas não necessariamente precisará ser fixo. Você pode ter tecnologias em que esse IP é compartilhado.

Eu acho que, sobre aquela pergunta sobre o que o Marco Civil pode ajudar na área de segurança, há posições muito favoráveis ou não, há todo aquele debate sobre a parte de armazenamento de *logs*. O que eu acho que é muito importante é que ele deixa claro: *"Olha, tem alguns logs que precisam existir"*. Como, por exemplo, ao mesmo tempo em que uma operadora sabe quem usou um celular e quem tem um número, assim como o banco precisa manter em sigilo os meus dados bancários, você precisa ter certa noção de poder chegar a quem estava usando um IP. Mas, ao mesmo tempo, deixa algumas regras de que também não é logar tudo sobre todos. Eu acho que tem que haver certo balanço, porque uma das missões da segurança é também proteger a confidencialidade, a privacidade do cidadão.

Então, eu acho que ele, ao mesmo tempo em que dá uma maior segurança, deixa claro quais são os registros que precisam ser armazenados — e isso ajuda muito. E também deixa claro quais são os registros que não são desejáveis sejam armazenados por alguns atores, porque eles podem levar a problemas de privacidade e a outras quebras.

Eu acho que essa seria uma discussão maior. Os projetos de lei de proteção de dados pessoas são muito importantes. Porque eu acho que é possível, sim, armazenar muita coisa, mas não se deveria armazenar tanta coisa. Eu acho que essa falta de clareza da importância dessas informações pode trazer um pouco de confusão, mas eu acho que sim.

Temos trabalhado muito em alguns grupos de trabalho, com operadoras, com provedores, para acelerar ainda mais a adoção de IPv6 no Brasil, para sairmos desse período em que está difícil chegar aos autores de alguns crimes, mais por conta dessas tecnologias que estão sendo implementadas para compartilhar os poucos endereços antigos que ainda existem.

Então, é um problema técnico complexo. O Brasil está muito bem já na adoção do IPv6. O mundo está adotando isso aos poucos, mas, como a Internet hoje é chave para muitas coisas, as redes estão sendo muito conscienciosas. O IPv4 e o IPv6 vão conviver na Internet por muitos anos ainda. As redes vão precisar da presença nos dois mundos por um bom tempo.

Eu queria também fazer um comentário. Houve a pergunta do Deputado Rafael sobre as estatísticas de *spam*. Hoje, entre as coisas que nós recebemos, até naqueles números que eu mostrei, não entram reclamações de *spam* porque não há um conceito muito firme sobre o que é exatamente *spam*. É um *e-mail* não desejado, um *e-mail* que eu não queria, é um *e-mail* de comércio. E o nosso foco tem sempre sido o seguinte: como fazer para que a infraestrutura da Internet brasileira não seja abusada para mandar *spam* para o mundo.

O Levy comentou antes todo aquele nosso trabalho de combate ao *spam*. O Brasil era abusado por terceiros. Parecia que o *spam* vinha do Brasil, mas não vinha. E nós levávamos uma culpa. Éramos realmente reconhecidos na mídia internacional como o rei do *spam*. No fundo, nós tínhamos muitas máquinas sendo abusadas, muitas máquinas de usuários em casa. Precisávamos reduzir isso...

Nessas reclamações que nós recebemos, até hoje não conseguimos identificar especificamente pedofilia. Que o *spam* poderia ter sido usado, com certeza poderia, porque, no fundo, o *spam* ou as técnicas de envio de *e-mail* em massa nada mais são do que você conseguir mandar para um volume muito grande de destinatários mensagens. E existem várias técnicas de se abusarem das infraestruturas para permanecer anônimo. Na verdade, isso é só dificultar. Você consegue fazer isso passando por diversos pontos, e eu sempre só consigo ver o último.

Por exemplo, aquele processo multissetorial que foi feito com a defesa do consumidor, com todas as áreas, para fazer a gerência da Porta 25, como foi chamado, era para que no Brasil não fosse mais tão fácil ter esse abuso das nossas redes para esconder terceiros.

Eu posso até tentar procurar, mas não tenho nenhum dado sobre os dados do SpamCop e Abusix que são mandados para nós. Essas são duas organizações internacionais que recebem reclamações de usuários finais de *spam*, e eles repassam para nós aqueles *spam*s que parece terem saído de endereços IPs do Brasil. O que nós fazemos é tentar contatar esses donos, dizendo: *"Olha, pode ser que tenha uma problema na sua rede e você esteja sendo abusado por spammers"*.

Especificamente sobre casos de pornografia envolvendo crianças, sempre recomendamos que não nos notifiquem. Isso pode ser notificado diretamente para a

Polícia Federal. Há um endereço de *e-mail* público, divulgado na nossa página. Esse é um assunto muito sério, muito rápido. Queremos evitar que nos coloquem no meio disso, porque o máximo que nós vamos poder é fazer com que demore mais a chegada dessa informação até à polícia ou às autoridades que vão investigar isso.

Então, sempre instruímos as pessoas sobre isso. Esse é um crime no qual a vítima não precisa fazer notificação. Qualquer um que tome conhecimento disso pode rapidamente ir até a polícia. Os próprios provedores de Internet já sabem disso e já têm os dados de contato e acordos, porque isso é muito sério nessa área.

E só queria fazer um complemento. Eu acho que, em relação à discussão sobre criptografia, lembrando o que o Renato Martini comentou, a criptografia bem implementada realmente é muito difícil de quebrar. Ela tem que ser bem implementada e forte para que todos possam se proteger.

Hoje a gente sabe que alguns governos — principalmente os da polícia americana e polícias da Inglaterra — têm esse conceito de que as polícias podem quebrar ou ter acesso, podem ter uma espécie de *backdoor*, uma criptografia. Ou a criptografia é forte para todos ou ela não o é para ninguém. No momento em que você coloca um ponto de entrada, uma quebra, um *backdoor* para que alguém tenha acesso, isto a torna fraca para todos.

Então, esse é um ponto que tem que ser levado muito em consideração. A criptografia é essencial para proteger dados do Estado, essencial para proteger o cidadão, para proteger a privacidade, mas não dá para ela ser implementada funcionando às vezes bem, às vezes não. Acho que esse é um conceito tecnicamente complexo, mas é importante levar em consideração que ela é muito importante, que ela protege os dados, sejam do Estado, sejam do cidadão, e que ela é muito boa. Então, acho que esse é o ponto principal a saber.

Também quero complementar na parte da importância do *software* livre. Hoje, no NIC.br, em todos os nossos serviços nós usamos *software* livre. Mas quero lembrar que o fato de ele ser *software* livre não quer dizer que ele não tenha vulnerabilidades, porque ele pode ter defeitos de programação, defeitos de código, que nem sempre a gente consegue ver. É por isso que o fato de ser livre não quer dizer que automaticamente ele é mais seguro, mas que ele é mais auditável, ele é mais fácil de poder implementar extensões, e tem mais gente olhando para ele. Eu

acho que essa é uma grande diferença que se tem entre um e outro nesse ponto. Mas só para não confundir e achar que magicamente basta ser *software* livre que é mais seguro. Acho que é mais difícil, realmente, de se colocar coisas ocultas que ninguém veja, porque tem gente demais olhando, mas claro que é preciso ter pessoas capacitadas olhando para o código, porque ele é complexo.

Eu espero ter tocado em todas as perguntas, mas me coloco à disposição, claro, para qualquer esclarecimento, não só hoje como também no futuro.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Nós agradecemos por ter aceito o convite. Agradeço também ao Dr. Renato e ao Dr. Marcos pela participação nesta CPI, colaborando com o desenvolvimento dos nossos trabalhos.

Deputado Alexandre Leite.

O SR. DEPUTADO ALEXANDRE LEITE - Sra. Presidente, gostaria de fazer mais uma pergunta ao Marcos Vinícius.

Existe algum cargo de provimento de indicação política no SERPRO? Qual seria esse cargo? Faço esta pergunta porque me causam estranheza os dois ataques advindos de funcionários do SERPRO terem sido contra integrantes de um mesmo partido político.

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - De indicação política só os dos diretores. Eu, no caso, sou uma indicação política. Nós somos nomeados por decreto presidencial. Os demais são todos cargos da empresa. As pessoas têm as suas preferências partidárias, naturalmente, mas não são cargos de indicação política, não; são cargos da estrutura da empresa.

O SR. DEPUTADO ALEXANDRE LEITE - Coincidência ou existe algum motivo razoável para isso?

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - Ou talvez haja outros tipos de ataques que as pessoas... Porque, muitas vezes, acontece sem que as pessoas façam a denúncia. Não sei responder objetivamente a V.Exa. Os cargos de indicação política somos nós. Eu basicamente estou em um cargo de indicação político-partidária, governamental-partidária.

O SR. DEPUTADO RAFAEL MOTTA - Sra. Presidente...

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

O SR. DEPUTADO RAFAEL MOTTA - Só quero comunicar, Sra. Presidente, que o Deputado Leo de Brito aqui me mostrou, e eu já tinha recebido a informação, que no meu Estado do Rio Grande do Norte, assim como nos Estados do Acre, Ceará, Minas Gerais, Pernambuco, Rondônia, Santa Catarina e Tocantins, a Polícia Federal deflagrou uma terceira grande operação de combate à pedofilia virtual. Foram feitos nove mandados de busca e apreensão e quatro prisões em flagrante.

A Diretoria de Investigação e Combate ao Crime Organizado — DICOR coordenou essa operação, e a Polícia Federal efetuou essas prisões por abuso sexual de menores na Internet. Esperamos que essas operações, com o exemplo dessa chamada Operação Gênesis, ocorram com mais frequência. Eu acho que a Polícia Federal, num momento tão coincidente com a nossa CPI, tem que se tornar mais frequente. Infelizmente, um dos acusados pagou fiança e já está na rua.

Acho que é o momento de esta CPI pensar realmente em como proceder em relação à legislação sobre pedofilia, não apenas na parte da Internet, mas também de uma forma geral em relação aos trabalhos legislativos.

Mais uma vez, agradeço a todos os convidados que nos brindaram com informações valiosas. Agradeço a todos pela presença.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Sr. Marcos.

O SR. MARCOS VINÍCIUS FERREIRA MAZONI - Deputado, só para contribuir, eu também tenho Twitter, e, durante o processo, fui atacado várias vezes; só não transformei isso em crime de opinião. As pessoas podem ter suas opiniões. Eu fui atacado; só não fiz nada com isso.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Aproveito as palavras do Deputado Rafael Motta, já entrando nesse assunto, para dizer que na próxima terça-feira, dia 8 de setembro, no período da tarde, vamos ter aqui, em reunião de audiência pública desta Comissão, a presença do Conselho Nacional dos Direitos da Criança e do Adolescente — CONANDA, da Secretaria Nacional de Promoção dos Direitos da Criança e do Adolescente, do Childhood Brasil e do Senador Magno Malta, dando sequência às sugestões dos requerimentos aprovados no plenário.

Aproveito, também, para agradecer a todos os presentes por terem nos cedido as apresentações. Já foi pedido à Secretaria desta CPI que as envie aos *e-mails* dos nossos Parlamentares e membros desta CPI.

Nada mais havendo a tratar, declaro encerrada a presente reunião, antes convocando reunião ordinária de audiência pública para a próxima terça-feira, dia 8 de setembro, em plenário a ser informado na página das Comissões e encaminhado aos *e-mails* institucionais dos gabinetes e Lideranças.

Está encerrada a presente reunião. E, desde já, um bom feriado a todos. Até a próxima terça-feira.