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: 2402/15**	**DATA: 12/11/2015**	
LOCAL: Plenário 15 das Comissões	**INÍCIO: 10h37min**	**TÉRMINO: 11h44min**	**PÁGINAS: 25**

DEPOENTE/CONVIDADO - QUALIFICAÇÃO
DENNYS MARCELO ANTONIALLI - Diretor-Presidente do InternetLab e Representante do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas.

SUMÁRIO
Debate sobre o tema *Segurança de Sistemas*.

OBSERVAÇÕES
Houve intervenção fora do microfone. Ininteligível.

O SR. PRESIDENTE (Deputado Leo de Brito) - Bom dia! Declaro aberta a 30ª reunião ordinária da Comissão Parlamentar de Inquérito que investiga a prática de crimes cibernéticos — CPI-Ciber.

Expediente.

Comunico que a Comissão recebeu as seguintes correspondências: Ofício nº 1.303, de 2015, da Secretaria Municipal de Finanças e Desenvolvimento Econômico, do Município de São Paulo, encaminhando estudos técnicos referentes às informações relacionadas à ordem de convocação de servidores da Fazenda Municipal. O documento encontra-se disponível na Secretaria da Comissão.

Ordem do Dia.

Audiência pública. A reunião de hoje trata do tema Segurança de Sistemas e atende aos Requerimentos nº 17 e nº 35, de 2015, de autoria dos Deputados João Arruda e Leo de Brito. Convido para compor a Mesa o Sr. Pablo Cerdeira, Chefe do Big Data, da Prefeitura do Rio de Janeiro, e especialista em segurança e privacidade. *(Pausa.)* O Sr. Pablo Cerdeira justificou a sua ausência por estar doente. Caberá à Secretaria remarcar a audiência pública com o Sr. Pablo, que infelizmente não pôde estar presente. Convido também o Sr. Dennys Marcelo Antonialli, Diretor-Presidente do InternetLab e representante do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas, que se encontra aqui presente.

O convidado disporá de 20 minutos para a sua apresentação, após o que será passada a palavra ao Relator, aos Sub-Relatores, aos requerentes e aos senhores membros.

Concedo a palavra ao Sr. Dennys Marcelo Antonialli, Diretor-Presidente do InternetLab. S.Sa. dispõe de 20 minutos. Como nós temos apenas a fala de V.Sa., seremos complacentes em relação ao tempo, se o senhor quiser se estender um pouco.

O SR. DENNYS MARCELO ANTONIALLI - Obrigado, Deputado Leo de Brito. Bom dia a todos! Exmos. Srs. Deputados, todos aqui presentes, em primeiro lugar, eu gostaria de agradecer o convite para contribuir com os trabalhos desta Comissão e dizer que me sinto honrado em poder falar nesta Casa sobre um tema tão

importante quanto o da regulação da Internet e a prevenção dos crimes que podem decorrer do seu uso.

Gostaria de esclarecer também que falo aqui na condição de acadêmico, estudioso que sou dos temas referentes ao direito à privacidade e à regulação na Internet, temas que estudei na Alemanha e nos Estados Unidos, na Universidade de Stanford. Agora, desenvolvo a minha pesquisa de doutorado na Universidade de São Paulo, onde eu também coordeno o Núcleo de Direito, Internet e Sociedade, que é vinculado à Faculdade de Direito.

Além disso, falo na condição de Diretor-Presidente do InternetLab, que é um centro independente de pesquisa em direito e tecnologia sediado também em São Paulo. A nossa missão é produzir pesquisas, dados e diagnósticos da realidade brasileira que possam ajudar na formulação de políticas públicas de Internet.

Eu organizei a minha apresentação da seguinte forma. Inicialmente, eu vou fazer breves comentários sobre as garantias e os limites que a legislação brasileira e a Constituição Federal colocam em relação aos poderes de vigilância do Estado. Em seguida, vou comentar brevemente sobre como se dá o processo de investigação dos crimes que acontecem na Internet, sobretudo a identificação dos terminais responsáveis por eventuais atos tidos como ilícitos. Vou comentar sobre a diferença entre alguns tipos desses dados, a prerrogativa de acesso que se tem a eles, e encerrar falando sobre os princípios internacionais que norteiam e garantem a proteção aos direitos humanos na vigilância estatal.

Queria dizer também que muito desta apresentação se baseia em um relatório de pesquisa que o InternetLab elaborou em pareceria com a Electronic Frontier Foundation, organização da sociedade civil dos Estados Unidos que, desde 1990, atua na promoção dos direitos digitais e é muito reconhecida internacionalmente pela sua expertise técnica e jurídica nestes temas.

Começarei a falar sobre garantias e limites. Em primeiro lugar, eu gostaria de salientar que os crimes cibernéticos e os temas que têm sido tratados nesta Comissão são de extrema importância, e, em nenhum momento, as garantias e os limites que eu vou trazer aqui devem ser confundidos com a tentativa de proteger ou defender esses tipos de crime.

Crimes nefastos, como, por exemplo, abuso sexual infantil, têm que ser combatidos com rigor, e é importante que se pense em mecanismos e num modelo regulatório que possam coibir essas práticas. Ao mesmo tempo, eu acho importante que essas prerrogativas venham acompanhadas de algumas preocupações, até para depois não serem alvo de questionamentos, em decorrência do que prevê o nosso ordenamento jurídico.

Lembrando que a Constituição Federal traz a liberdade de expressão como direito, quaisquer modelos regulatórios em que nós venhamos a pensar têm que necessariamente privilegiar a garantia da liberdade de expressão; a intimidade e a vida privada; o sigilo das comunicações, sobre o qual eu vou falar um pouco mais à frente; a garantia do devido processo legal; o contraditório, a ampla defesa e a presunção de inocência. Todos esses são parâmetros e direitos que a Constituição Federal coloca e que devem ser observados quando pensarmos em procedimentos e modelos regulatórios para se coibirem os crimes na Internet.

Além disso, lembro que o Código de Processo Penal ordena que o juiz observe os princípios de adequação, necessidade e proporcionalidade ao ordenar a produção de provas. Essas premissas devem ser observadas em todas as ordens judiciais que forem emanadas. O mesmo vale para a apreciação de pedidos de medidas cautelares de produção de provas, procedimento que o Marco Civil também estabelece especificamente no caso da Internet.

A intimação do atingido deve sempre ocorrer, ressalvados os casos de urgência e de perigo de ineficácia. Assim, a regra é que sejam notificados os atingidos, a menos que isso possa trazer eventuais problemas para a investigação.

Pela Constituição Federal e pelo Código de Processo Penal, são inadmissíveis também as provas obtidas por meios ilícitos, contrariando a Constituição e a lei.

Parte dessas considerações que faço agora visa a impedir que mecanismos sejam usados para reunir eventuais provas que combatam esses crimes e depois sejam tidos como ilícitos, e as provas tenham que ser excluídas do processo e não ser apreciadas. Portanto, é importante que, ao se pensar nesses mecanismos tecnológicos, nessas formas de investigação, eles partam dos pressupostos que eu acabei de mencionar.

Em terceiro lugar, eu queria dizer que essas garantias e princípios também estão consagrados no Marco Civil da Internet. O art. 7º trata da inviolabilidade, do sigilo do fluxo das comunicações na Internet, salvo por ordem judicial; da inviolabilidade e do sigilo das comunicações privadas armazenadas. O Marco Civil já traz também um regramento que privilegia o sigilo dessas comunicações, ressalvados os casos em que o sigilo é quebrado por ordem judicial.

Adentrando um pouco mais o tema dos crimes cibernéticos, eu gostaria de fazer uma recapitulação de quais são as principais etapas, ou fases básicas de identificação de quem partiram os atos ilícitos que estão sendo investigados.

Basicamente, há dois atores principais quando se tenta identificar alguém ou algum terminal, como eu vou explicar daqui a pouco, de onde partiram esses atos tidos como ilícitos. Esses atores são o provedor de aplicações e o provedor de conexão. Os provedores de aplicações de Internet, como os senhores devem saber, são as plataformas, serviços e aplicativos que os usuários usam todos os dias: Google, Facebook, Twitter, Instagram. Quaisquer plataformas como estas são provedores de aplicações, ou seja, estão oferecendo uma aplicação para o usuário.

Nesse sentido, os provedores de aplicações são a primeira peça-chave na tentativa de se identificar de onde partiu determinada conexão ou postagem. Supondo, por exemplo, que se queira investigar de onde surgiu um vídeo que contém imagens ilícitas, a primeira coisa que deve fazer é se dirigir à plataforma, ao provedor de aplicações, porque é esse provedor de aplicações que vai ter condições de dizer qual a conexão a partir da qual aquele vídeo foi colocado na Internet, na plataforma. A mesma coisa ocorre com uma foto, com uma postagem de texto ou com o envio de um *e-mail.*

Então, o primeiro passo para identificar de onde partiu a postagem, a foto ou o vídeo é ir ao provedor de aplicações. O provedor de aplicações tem a obrigação, como eu vou falar mais à frente, de manter os registros de acesso a essas aplicações.

Uma pergunta como “de onde surgiu a conexão?” pode ser respondida pelo provedor de aplicações. Como é que o provedor de aplicações responde a essa pergunta? Geralmente com o número de endereço IP, uma data e uma hora, esclarecendo, por exemplo, em relação a um vídeo que se queira investigar, a partir

de onde ele foi colocado na Internet, a partir do número de IP “x”, na data e hora “y”. Isso possibilita acessar o segundo grande ator responsável neste processo, que é o provedor de conexão.

Os provedores de conexão são aqueles que administram esses IPs e os alocam aos usuários. Portanto, são responsáveis pelo oferecimento do serviço de Internet aos usuários. São eles que podem identificar, a partir daquela conexão numa determinada data e hora, que terminal estava usando aquele endereço de IP naquela data e naquela hora.

Sem esse endereço de IP que foi fornecido pelo provedor de aplicações, não há como acessar o provedor de conexão e somente com o endereço de IP do provedor de aplicações também não há como identificar o terminal. Então, são duas peças-chave na identificação do terminal de onde partiu a postagem, o vídeo, a foto etc. que encontram regramentos um pouquinho diferentes no Marco Civil, mas o Marco Civil já determina que esses dados e registros sejam guardados.

A partir do momento em que o provedor de conexão tem acesso ao endereço de IP, à data e à hora, ele é capaz de dizer que terminal estava tendo acesso àquela aplicação, ligado geralmente a uma conta. É importante dizer que o provedor de conexão consegue identificar o terminal de onde partiu e, eventualmente, a conta a partir da qual aquele serviço de Internet foi contratado. Mas isso não garante, necessariamente, que se identifique a pessoa exata. Sabemos que podem existir técnicas em que computadores são hackeados, sistemas são utilizados para que, a partir de uma mesma conexão de um terminal, uma pessoa com acesso remoto possa cometer um crime. Então, é importante saber e pensar nesta distinção de que há o terminal, o aparelho, o dispositivo, o computador que é identificado, e não necessariamente o usuário, embora se tenha muito mais condições de identificá-lo, muito mais indícios que permitam chegar ao eventual culpado, a partir desta cadeia de ligações entre provedores de aplicações e provedores de conexão.

Como eu disse, acho importante salientar que o Marco Civil, pensando neste esquema e nesta cadeia de identificação, já determina que essas informações e registros sejam guardados. Hoje, o Marco Civil, por ter essas determinações, já possibilita ou já determina, coloca uma obrigação legal para que tanto os provedores

de aplicações quanto os provedores de conexão guardem esses registros e tornem possível o fechamento dessa cadeia que eu mencionei há pouco.

Começando pelos provedores de aplicações, que são esses primeiros atores que devem ser acessados, o Marco Civil, no art. 15, determina que sejam guardados por 6 meses os registros de acesso a aplicações da Internet. Então, num período de 6 meses, independentemente de qualquer pedido, os provedores de aplicações são obrigados a manter esses registros. É claro que eles podem manter por mais tempo, mas a obrigação prevista na lei é de 6 meses.

Outra importante obrigação, característica do Marco Civil da Internet, é que esses registros e informações podem ser guardados por mais tempo, por solicitação das autoridades investigativas competentes, por meio de medida cautelar. O prazo, em regra, é de 6 meses. Mas, caso alguma investigação que esteja em curso requeira, é possível que esse pedido seja feito e cautelarmente aceito, para que esses dados possam ser guardados por um tempo maior, preservando possíveis provas para uma investigação que dure mais tempo.

É importante ressaltar também que, por obrigação legal, por dispositivo do Marco Civil, a ordem judicial é fundamental para o acesso a esses registros. Então, essa primeira etapa de acesso aos provedores de aplicações depende de ordem judicial. Isso ocorre porque, no Poder Judiciário, o juiz é legitimamente mais bem posicionado para avaliar em que medida a quebra do sigilo e da privacidade se justifica, com base nos indícios e na intenção de se coibir algum crime. Dessa forma, é importante que o Judiciário tenha esse crivo final na hora de determinar o acesso a esses tipos de registros de aplicações.

O esquema é muito parecido em relação aos provedores de conexão, às empresas que proveem o acesso à Internet. O Marco Civil, no art. 13, determina que esses provedores guardem — a diferença fica no prazo — por 1 ano os registros de conexão, que vão, assim, permitir que seja identificado o terminal. Essa mesma característica em relação à possibilidade de se pedir que esse prazo seja prorrogado, que esses dados sejam guardados por mais tempo, existe também de maneira cautelar, como também existe a mesma obrigatoriedade de que se obtenha ordem judicial para que esse provedor de conexão forneça os dados.

Como eu já falei de alguns tipos de dados diferentes, eu acho importante fazer algumas distinções. As duas primeiras se referem aos tipos de dados que eu mencionei há pouco — elas estão previstas no Marco Civil. Os registros de conexão são o conjunto de informações referentes à data e à hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e o recebimento de pacotes de dados. Trata-se justamente daquela primeira peça do quebra-cabeça que eu mencionei há pouco, é justamente o provedor de aplicações, que vai identificar qual a conexão, o número de IP, com a data e a hora, que acessou, seja o Facebook, seja o Twitter, seja o Google, o que vai servir para que o provedor de conexão possa identificar.

Os registros de acesso a aplicações são estes que eu mencionei agora: o conjunto de informações referentes à data e à hora de uso de determinada aplicação de Internet, a partir de determinado endereço de IP.

Tanto os registros de conexão quanto os registros de acesso a aplicações são tipos de metadados. Metadados, basicamente, são o conjunto de dados sobre comunicações, com exceção do seu conteúdo. Quaisquer dados a respeito de uma comunicação ou de uma postagem são metadados. Os metadados podem dizer coisas muito importantes e significativas, independentemente do conteúdo de uma comunicação. Exemplos de metadados são relações entre destinatários, quem falou com quem a que hora, dados sobre geolocalização. São todos os dados que independem da leitura de *e-mails*, por exemplo, mas que dizem respeito a esses *e-mails* — entre quem eles foram trocados, quando foram lidos, eventualmente até qual é o assunto dos *e-mails.* São dados que dizem respeito a essas comunicações e a essas relações, mas não são, necessariamente, o conteúdo da comunicação. É importante dizer isso porque há uma diferença.

O conteúdo das comunicações pode ser alvo de pedido de remoção do conteúdo. Existe uma grande diferença entre o pedido que se faz para que um vídeo que eventualmente divulgue imagens ilícitas seja retirado da Internet — é plenamente possível se fazer um pedido como este. Trata-se, então, de uma remoção de conteúdo. O mesmo acontece quando, por exemplo, se fala no direito ao esquecimento, que nada mais é do que a remoção de alguns conteúdos da Internet, coisa que hoje já é possível mediante ordem judicial. Uma coisa é a

remoção do conteúdo, outra coisa é o acesso a esse conteúdo para efeitos de vigilância e fiscalização, ou seja, a leitura desse conteúdo, que é protegido pela Constituição Federal e pela legislação infraconstitucional. Outra coisa é a leitura e o tratamento desses metadados.

Eu falo isso e aproveito para dar um exemplo de como os metadados podem ser importantes. Há um projeto do MIT chamado Emerger. Seria interessante que os senhores tivessem a curiosidade de conhecê-lo. Os senhores podem acessá-lo na Internet. Por meio desse projeto, é possível se logar na conta do Gmail, por exemplo, e ele vai analisar todas as suas relações e seus *e-mails* trocados, sem olhar o conteúdo dos *e-mails*. A partir disso, ele vai traçar e trazer uma série de informações bastante sensíveis e interessantes a respeito do seu perfil de comunicações.

Aqui a gente pode ver um gráfico que categoriza quais são as pessoas com quem eu mais troquei *e-mails*, a quem elas se ligam, com que frequência, a quantidade e a intensidade das comunicações, os contatos que ficam mais isolados; cada pessoa em quem você pode clicar e ter acesso a quem essas pessoas também estão ligadas e ligadas a você. O mais interessante é que este projeto consegue identificar que pessoas foram apresentadas a você e por quem.

É interessante observar que, sem olhar os conteúdos dos *e-mails,* já se pode ter uma ideia bastante apurada do perfil das comunicações. Muitas vezes, o importante sobre os metadados é que eles podem revelar informações mais sensíveis até do que o conteúdo dos *e-mails*. Então, saber que eu falo muitas vezes com o Francisco, que é outro Diretor do InternetLab, independentemente do que eu fale com o Francisco, já é uma informação bastante relevante que pode, eventualmente, dar margem a uma interpretação incorreta.

É importante que existam balizas para a análise dos metadados e para o acesso a esses dados, para que não se usem essas relações e inferências de maneira equivocada ou abusiva, de modo a ferir a presunção de inocência e a descontextualizar eventuais dados e informações.

Por fim, eu vou trazer alguns princípios internacionais que devem nortear os sistemas de investigação de crimes cibernéticos que, de novo, não pretendem proteger aqueles que eventualmente praticaram atos ilícitos e nefastos, que devem

ser, sim, processados e penalizados. Mas estabelecem algumas balizas para que esta investigação aconteça dentro dos princípios constitucionais e dentro do contexto dos direitos humanos e possam conversar de maneira harmônica com a investigação e a persecução criminal.

São treze princípios. Eu vou passar por eles de maneira breve. O primeiro diz respeito à legalidade. Os limites do direito à privacidade devem ser definidos clara e precisamente em leis e devem ser regularmente revistos para garantir que as proteções à privacidade prossigam lado a lado com as rápidas mudanças tecnológicas. Esse é um princípio importante, sobretudo no momento em que se discute, tanto no Congresso quanto no Ministério da Justiça, o anteprojeto, no caso do Ministério da Justiça, de Lei para a Proteção de Dados Pessoais, um marco regulatório que o Brasil ainda precisa aprovar e estabelecer, para que se tenha regras claras sobre os limites e os momentos em que a quebra da privacidade pode ser decretada e em que circunstâncias. Essa previsão em lei é bastante importante, e dela advém esse princípio.

O segundo princípio é o fim legítimo. A vigilância das comunicações só deve ser permitida em busca dos objetivos mais importantes do Estado. Claro, o combate aos crimes cibernéticos é um deles, mas devem ser justificados os fins a partir dos quais se requer ingerência sobre as comunicações e acesso a esses dados.

Necessidade. O Estado tem obrigação de provar que as atividades de vigilância das comunicações são necessárias, para que se alcance um fim legítimo.

Adequação. Que esses mecanismos sejam adequados, permitindo que aquela persecução aconteça, e proporcionais.

A vigilância deve ser considerada como um ato altamente intrusivo, que interfere com os direitos da privacidade, e deve ser quebrada ou relativizada de forma proporcional; então, apenas na exata medida em que for necessária, para que aquele crime seja processado. Isso quer dizer que dados em excesso não devem ser requeridos, e devem se ater apenas àqueles dados estritamente necessários para a persecução criminal.

O princípio da autoridade judicial competente é um dos mais importantes. As determinações relativas à vigilância das comunicações devem ser expedidas por uma autoridade judicial competente, que seja imparcial e independente.

Vemos a obrigatoriedade da ordem judicial no Marco Civil da Internet e em outros diplomas legais brasileiros. Isso é uma coisa boa, que deve ser preservada. Como eu falei, o Poder Judiciário é aquele que legitimamente tem autoridade para estabelecer os momentos e os limites à quebra da privacidade.

O devido processo legal vai garantir uma série de prerrogativas àqueles que estão sendo processados, que devem ter direito a um processo justo e público.

Notificação do usuário. Os indivíduos devem ser notificados de uma decisão autorizando a vigilância de suas comunicações, exceto quando uma autoridade judicial competente conclua que um aviso prejudicaria a investigação. Os indivíduos devem ter oportunidade de questionar tal vigilância, antes que ela ocorra.

Então, é claro que existem circunstâncias em que a investigação pode ser prejudicada caso o investigado seja notificado de que aquela investigação vai ocorrer, mas existem outros casos em que é saudável que se dê ao atingido, ao investigado, a possibilidade, até pela ampla defesa e contraditório, de questionar essas atividades. Por exemplo, em casos de liberdade de expressão, em que se objetiva a remoção de conteúdo. Em eventual responsabilização de determinado indivíduo, é importante que se dê a ele a oportunidade de se defender em relação à publicação daquele conteúdo. Isso não impede que aquele conteúdo possa ser removido por ordem judicial ou que ele possa ser eventualmente responsabilizado por aquelas imagens ou postagens que veiculou.

Transparência. O Governo tem obrigação de tornar públicas as informações suficientes para que o público em geral possa entender o escopo e a natureza de suas atividades de vigilância. Então, deve ter um sistema claro e transparente, com as balizas legais, para que essas investigações aconteçam.

Escrutínio Público. Os Estados devem estabelecer mecanismos de fiscalização para garantir a transparência e a responsabilização da vigilância nas comunicações. Os mecanismos de fiscalização devem ter autoridade para acessar todas as informações relevantes a respeito das ações do Estado.

Integridade das comunicações e sistemas. É importantíssimo que todos esses dados que serão repassados e compartilhados com o poder público e com as autoridades investigativas fiquem armazenados de forma segura, não sejam

vazados, para eventualmente não serem descontextualizados, prejudicando a imagem e os direitos daqueles que estão sendo investigados.

Por fim, salvaguardas para cooperação internacional. Ocasionalmente, os Estados podem precisar de assistência de provedores de serviços estrangeiros para conduzir a vigilância. Isso deve ser governado por tratados claros e públicos, que garantem que os *standards* de maior proteção à privacidade devem ser aplicados.

Salvaguarda contra acesso ilegítimo. Devem existir penalidades na esfera civil e criminal, impostas a qualquer parte responsável pela vigilância ilegal. Aqueles que oferecem mecanismos de vigilância devem ter acesso a remédios jurídicos efetivos.

Lembro aqui que, em 2007, o Brasil sofreu uma condenação na Corte Interamericana de Diretos Humanos por ter ocorrido uma série de monitoramentos e interceptações telefônicas sem o processo legal adequado da autoridade competente que expedisse aqueles pedidos. É o Caso Escher. Certamente, é uma coisa que deve ser evitada, quando se pensar no modelo regulatório para coibir a prática de crimes cibernéticos.

Em relação à minha apresentação, esses eram os pontos que eu pretendia abordar. Fico à inteira disposição dos senhores para eventuais esclarecimentos e dúvidas.

Obrigado.

O SR. DEPUTADO SILAS FREIRE - Sr. Presidente, só uma questão de ordem, por favor. Eu queria fazer um registro na CPI de Crimes Cibernéticos de um fato — e já eu falo do tema debatido aqui — que aconteceu ontem em um portal nacional: o G1, da *TV Globo*. Eles veicularam a informação de uma colisão entre um metrô e um trem em Teresina, em que aconteceram duas mortes, a do maquinista — já, já V.Exa. vai entender — e a do seu auxiliar. O metrô de Teresina é um trem de superfície em que, em alguns momentos, na região central, adentra o subterrâneo. Houve esse acidente, essa tragédia, e o G1 divulgou a informação. Depois da divulgação dessa informação, começou um ataque maciço ao Estado do Piauí, por parte de internautas.

Eu vou ler aqui alguns. Paulo Ramos: *"Matou algum índio aí no Piauí?" "Menos dois votos dos nazistas do PT".* E aí vai: *"Teresina é uma cidade minúscula, insignificante. A carroça seria o melhor transporte para estes lugares".* São os

comentários que estão no G1. O G1 não teve nenhuma preocupação. Eles passaram a noite inteira lá, se ainda não estiverem.

O Nordeste tem esta urucubaca danada; é um *show* de preconceitos! Eu quero me limitar até a narrar os fatos. Mas estou dando entrada nesta Comissão em um requerimento, pedindo a V.Exa. que oficie a Polícia Federal que investigue os autores deste criminoso preconceito contra o meu Estado, contra a capital do meu Estado e do povo do meu Estado. Nós precisamos apenar estas pessoas. O meu requerimento também irá propor que essas ofensas permaneçam em *sites* nacionais por determinado tempo. Eu acredito que deve ter um filtro nestes *sites* e estes *sites* deixam estas ofensas em âmbito nacional.

Se não estiver na programação de terça-feira, eu vou pedir a assinatura dos colegas para que conste no extrapauta. Eu me orgulho de ser do Piauí, orgulho-me do povo da minha terra. E nenhum desses palhaços que escreveram aqui no G1, que fizeram comentário irão diminuir o meu Estado, de jeito nenhum. Eu não queria e não gostaria de nascer em um Estado do Brasil que não fosse o Piauí. Eu me orgulho do meu Estado.

O SR. PRESIDENTE (Deputado Leo de Brito) - Muito obrigado, Deputado Silas Freire. Também agradeço aqui ao Sr. Dennys Marcelo Antonialli pela apresentação.

Deputado Silas, aqui, se formos observar, quero me somar à preocupação de V.Exa. Sou um Deputado do Acre. Há Deputado do Estado de Rondônia. Está ali o Deputado Daniel também, que é do Estado de Pernambuco.

O SR. DEPUTADO SILAS FREIRE - Mas nós temos que punir essas pessoas!

O SR. PRESIDENTE (Deputado Leo de Brito) - Nós sabemos o quanto é o preconceito, muitas vezes, de pessoas de outros Estados do Brasil em relação ao Norte e ao Nordeste. É pertinente a preocupação de V.Exa.

Nós vamos passar agora às indagações. Iniciaremos com a palavra dos Sub-Relatores.

Concedo a palavra ao Deputado Daniel Coelho pelo prazo de até 5 minutos.

O SR. DEPUTADO DANIEL COELHO - Obrigado. Saúdo o Deputado Leo de Brito, a Deputada Mariana Carvalho. Solidarizo-me com o Deputado Silas Freire e

com todo o povo do Piauí que, com certeza, merece todo o nosso respeito. Também saúdo o Sr. Dennys.

Eu queria tocar em um ponto aqui que, talvez, seja o que me causa mais dificuldade, ao longo desta CPI, em discutir a questão dos crimes contra a honra e da liberdade de expressão. Não é fácil transitarmos no limite ou a na linha tênue entre a censura e, por outro lado, a possibilidade de nós não permitirmos que a Internet seja utilizada para destruir a imagem de alguém, para cometer atos de racismo, atos de machismo, de homofobia. Essa linha é muito tênue. Até onde podem ir essa proibição e essa punição de quem comete esses atos, sem que nós corramos o risco de interferir e de começar a censurar uma coisa que já é livre por natureza, que é a Internet?

Eu queria perguntar, de forma objetiva, na visão de V.Sa., se existe direito fundamental absoluto. Como a InternetLab se posiciona na questão da compatibilização entre o exercício do direito à liberdade de expressão e à privacidade e vedação do anonimato; além disso, ao direito fundamental: a honra e a imagem, que também estão insertas no art. 5º Constituição Federal? Por um lado, nós temos uma garantia do direito à honra e à imagem, mas, por outro, a liberdade de expressão precisa ser preservada.

Essa é uma preocupação que os Deputados desta Comissão têm tido. Não há interesse de nenhum Deputado, de nenhum partido, em fazer censura na Internet, mas também nós não queremos deixar uma frouxidão que permita um sentimento de impunidade para quem comete, eu reitero, atos de racismos, atos de crimes contra a honra, o que, com certeza, não contam com a simpatia da grande maioria da sociedade.

Eu gostaria que V.Sa. comente um pouco mais sobre essa dicotomia que tanto nos preocupa: de um lado a defesa da honra, mas, de outro, a necessidade de garantirmos a liberdade de expressão.

O SR. DENNYS MARCELO ANTONIALLI - Obrigado, Deputado. Compartilho completamente da preocupação de V.Exa. Acho a pergunta bastante oportuna, sobretudo diante do caso que acabou de ser relatado aqui.

De fato, a Constituição garante tanto a privacidade quanto a liberdade de expressão. Acho que quando pensamos no contexto da Internet, a primeira coisa

sobre esse tema que deve ser esclarecida, que deve ser pensada, é que — como eu explorei aqui brevemente, durante a apresentação — tudo o que se faz na Internet deixa rastros, deixa registros. Essa é a primeira característica da Internet. Essa é uma coisa importante a ser pensada.

Quando a Internet surgiu, existiu um movimento de achar que a Internet era uma terra sem lei, de que era um espaço em que as pessoas poderiam se ofender mutuamente, ou veicular coisas ilícitas sem serem responsabilizadas. Eu acho que precisamos combater essa ideia, porque todos esses registros, esse caminho que eu explorei durante a apresentação torna possível a identificação e a responsabilização de pessoas que tenham se excedido.

Direito à liberdade de expressão, como nenhum outro direito fundamental, é absoluto; ele se relativiza e deve ser ponderado com outros direitos. Então, a veiculação de conteúdos ofensivos decorrentes de preconceitos e a discriminação devem, sim, ser perseguidos. A arquitetura da Internet propicia isso, através da identificação desses usuários.

Em relação a como isso deve acontecer para que não se estabeleça um regime de censura, eu acho importante lembrar o importante papel do Poder Judiciário, que é aquela autoridade legitimamente competente para ter um crivo que vá justamente ver em que circunstâncias a liberdade de expressão deve ser relativizada, e pode ser responsabilizado determinado usuário. É dessa forma que prevê o Marco Civil da Internet. As plataformas só são responsabilizadas quando deixam de cumprir ordem judicial, mas, a rigor, o momento em que esses conteúdos passam a ser exigíveis de ser retirados é quando existe uma ordem judicial, que vai justamente determinar se ali houve ou não um abuso. Acho que a resposta para isso é confiar e deixar ao crivo do Poder Judiciário, que é quem melhor pode fazer essa avaliação. Lembro, novamente, que todas essas pessoas que ofenderam, ainda que usem pseudônimo etc., são plenamente identificáveis. Esses registros possibilitam isso. Então, se por um lado a Internet pode, às vezes, servir de espaço para esse tipo de prática, existe um lado bom, que é esse lado dos registros que ficam.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Com a palavra o Deputado Leo de Brito.

O SR. DEPUTADO LEO DE BRITO - Quero saudar a todos: a Sra. Presidenta, Deputada Mariana; a todos os Srs. Deputados e a todas as Deputadas; os consultores; a assessoria e a imprensa aqui presentes; e também o Sr. Dennys.

Quero primeiro falar da importância que o InternetLab teve na construção do Marco Civil. Então, é importante ressaltar isso aqui, o que talvez seja uma das grandes conquistas da Internet brasileira e também da Internet mundial. Nós estamos vendo hoje que o Marco Civil está sendo replicado — digamos assim — mundo afora, em países como Itália, Reino Unido, Jordânia; enfim, há vários outros países que têm se utilizado dessa lei importante, do ponto de vista dos direitos e liberdades civis na Internet. Nós estamos agora completando praticamente 1 ano de implementação dessa lei.

A primeira pergunta a V.Sa., como uma das pessoas que contribuiu para a construção dessa tão importante lei, é a seguinte: qual seria sua avaliação depois de 1 ano de implementação do Marco Civil? Essa é a primeira pergunta que tenho a fazer. A outra pergunta — não sei se tem relação com a sua atividade, mas certamente V.Sa. deve atuar nela — é relacionada à questão da segurança da informação: V.Sa. tem conhecimento específico, também, do ponto de vista acadêmico, sobre a questão da segurança da informação? Aqui, eu já fiz várias perguntas nesse sentido, e alguns especialistas deram respostas positivas e outros negativas. Eu queria ouvir a sua opinião, também, a respeito da utilização de *software* livre dentro do cenário de segurança da informação. V.Sa. considera que a utilização do *software* livre contribui para esses princípios que estão no Marco civil e também do ponto de vista da própria segurança da informação, que é uma das áreas mais atingidas pelos crimes cibernéticos, em larga escala? Temos visto, na imprensa, várias situações em que nós tivemos a violação da segurança da informação. Inclusive, tem uma lei específica — Lei Carolina Dieckmann —, que trata dessa situação.

Outra situação com a qual nos deparamos aqui na CPI diz respeito à utilização do IPv6. Durante a apresentação dos delegados da Polícia Federal, em uma audiência nesta CPI, discutiu-se sobre a questão da adoção do IPv6, que seria uma possível solução para a questão de segurança, porque no caso o usuário teria

um IP fixo e não mais dinâmico como é hoje. Eu queria também a opinião de V.Sa. a respeito da adoção do IPv6.

Por fim, tenho mais três perguntas. O Ministério da Justiça possui um anteprojeto de lei de proteção de dados pessoais, o qual passou por duas consultas públicas, e está em fase final de adaptações para ser enviado à Câmara. V.Sa. tem conhecimento disso? O InternetLab já foi consultado a respeito desse anteprojeto? Qual a sua opinião também sobre esse anteprojeto relacionado à proteção de dados pessoais? Outra pergunta também que acredito ter grande atualidade diz respeito aos projetos de lei que estão tramitando aqui nesta Casa, os quais certamente o InternetLab deve estar acompanhando, como fez no caso do Marco Civil. O PL 215, de 2015, em tramitação aqui na Casa, que está sendo inclusive duramente criticado por acadêmicos e pela sociedade civil organizada, entre outras coisas, pretende que a autoridade policial possa ter acesso aos registros de conexão e de aplicações sem ordem judicial prévia. V.Sa. citou um conjunto de princípios que devem reger a Internet. Como V.Sa. avalia este projeto?

Há ainda alguns outros projetos que estão tramitando na Comissão de Ciência e Tecnologia, Comunicação e Informática que estavam na pauta, nas últimas semanas, o PL 1.879, de 2015, e o PL 2.390, de 2015. O primeiro exige que todos os usuários da Internet forneçam seu CPF para navegar na Internet. O segundo pretende criar o Cadastro Nacional de Acesso à Internet, com a finalidade de proibir o acesso de crianças e adolescentes a sítios eletrônicos com conteúdo inadequados.

Este último PL exige um cadastro prévio de todos os internautas, bem como uma lista de todo o conteúdo tido como impróprio para crianças e adolescentes. O senhor entende que esses projetos, tais como estão redigidos, são benéficos para a sociedade? Ou, apesar de bem-intencionados, suas redações fogem completamente à realidade de como funciona a Internet, aos princípios que foram levantados aqui? E, neste caso, como poderíamos resguardar nossas crianças e adolescentes?

Por fim, há a última questão, que também vem sendo levantada aqui, nos vários debates, nas várias audiências que nós fizemos, a respeito da utilização de perfis *fakes* para a prática de crimes cibernéticos.

Então, seriam basicamente essas perguntas, cujas respostas serão respondidas em bloco, não né?

(Intervenção fora do microfone. Ininteligível.)

O SR. DEPUTADO LEO DE BRITO - O.k. tudo bem.

Então, são essas as perguntas.

O SR. DENNYS MARCELO ANTONIALLI - Muito obrigado, Deputado Leo de Brito. Excelentes as colocações e as perguntas, e eu vou tentar passar por todas, aqui.

Em relação ao Marco Civil da Internet, de fato, é muito importante. Foi uma lei muito importante, é uma lei ainda muito importante, exatamente porque estabelece princípios e direitos básicos aos usuários da Internet no Brasil.

Neste primeiro ano, o mais importante, acho, é avaliar a implementação do Marco Civil pelo Poder Judiciário, que é quem está criando as primeiras teses de interpretação e solidificando alguns conceitos que ficaram em aberto na lei. Temos acompanhado bastante de perto a atuação do Poder Judiciário e a aplicação dessa lei. Temos visto que vários dos dispositivos que colocam obrigações e direitos têm repercutido de maneira positiva na forma como as decisões têm sido tomadas. Eventualmente, alguns de seus dispositivos têm demorado um pouco mais para serem absorvidos ou para serem consagrados pela jurisprudência, de maneira que eu julgaria mais adequada. Mas, por exemplo, a questão das URLs, da retirada de conteúdo, que é uma questão que o Marco Civil traz explicitamente, que se achava que fosse ser menos controverso, mas ainda existiam várias decisões determinando que conteúdos fossem retirados, sem indicação do local onde o conteúdo estava sendo armazenado, que traz uma série de questões não só práticas, mas em relação à liberdade de expressão. Isso tem sido consagrado pela jurisprudência, até com julgado recente da STF de que a indicação das URLs é necessária.

Além disso, eu acho importante salientar que, apesar desse 1 ano positivo, o Marco Civil ainda deixou uma série de questões em aberto, por ser uma lei de caráter principiológico. E aí nós aguardamos, depois da consulta pública, organizada pelo Ministério da Justiça, que saia o texto do decreto que regulamente algumas dessas questões do Marco Civil da Internet, como, por exemplo, a questão da neutralidade da rede. Assim como algumas outras questões, uma delas é o acesso

aos dados cadastrais — artigo 10, § 3º — por autoridades investigativas sem ordem judicial.

Em relação à segurança da informação e ao *software* livre, eu de fato acredito piamente que a utilização do *software* livre contribui para a segurança da informação, na exata medida em que o *software* livre, por ter um código aberto e transparente, possibilita que as falhas sejam identificadas e controladas de maneira coletiva. Então, que se possa auditar o Código pra ver se de fato existem falhas ou vulnerabilidade de segurança. Isso torna, com certeza, esses *softwares* não só transparentes, mas também mais seguros. Na medida em que essas falhas e vulnerabilidades são identificadas, é possível corrigi-las e deixar a informação, que está ali guardada, mais segura; ou a que ali esteja transitando, de forma mais segura.

Chamo também a atenção não só para o *software* livre, mas para as tecnologias de criptografia, que são muito importantes nesse sentido para que essas informações sejam transmitidas de maneira segura, e revezamentos ou abusos ou a má-utilização dessas informações aconteçam.

Sobre o IPv6, digamos que essa é quase uma necessidade que se impõe ao mundo, sobretudo diante do aumento massivo da quantidade de dispositivos conectados. Então, numa realidade específica de Internet das coisas, em que todas as coisas, a maioria das coisas que estão na nossa casa, ou no nosso trabalho, vão estar conectados à Internet, então, desde as lâmpadas até a geladeira, que vai poder conectar-se ao supermercado, por exemplo, e fazer um pedido quando algum alimento estiver acabando, todos esses dispositivos conectados — todos eles — precisam de um IP, de um endereço para se conectar à Internet. O modelo que a gente tem hoje tem um número limitado, então, o IPv6 vai fazer com que isso mude. E você tem aí muitas possibilidades para que esses dispositivos se conectem.

Em relação ao IP ser fixo e não mais dinâmico, essa também é uma diferença que impactaria pouco, sob o ponto de vista das coisas que discuti aqui, já que, como eu disse, os registros de acesso a aplicações de Internet de conexão indicam, justamente, sempre o endereço de IP e uma data e hora, justamente porque esses endereços de IP, por serem dinâmicos, vão sendo alocados em diferentes terminais.

Mas daí a importância da data e hora; com a data e hora e o endereço de IP é possível identificar.

Em relação ao anteprojeto de lei, do Ministério da Justiça, de proteção de dados pessoais, eu acho que é um projeto bastante maduro, que passou por várias etapas de discussão, tendo a última acontecido de janeiro a julho deste ano. É uma lei extremamente moderna, da forma como ficou redigido o novo texto. E chamaria atenção para uma característica principal da lei que é a possibilidade da criação da autoridade de garantia. Então, ao contrário dos projetos que tramitam no Congresso, por uma questão de prerrogativa e competência privativa da Presidência da República para a criação de órgão, o anteprojeto de lei de dados pessoais elaborado pelo Ministério da Justiça teria essa vantagem: de ter a possibilidade de criar essa autoridade de garantia, como fez no texto, que seria responsável pela fiscalização e garantia do direito à privacidade de usuários da Internet no Brasil, seja através da fiscalização de aplicativos e *sites* de políticas de privacidade; seja promovendo campanhas de educação e conscientização; seja fiscalizando, impondo multas quando houver violações. Então, eu ressaltaria essa característica importante do anteprojeto de lei de dados pessoais, elaborado pelo Ministério da Justiça.

Em relação aos projetos de lei que tramitam aqui na Casa, de fato, o PL 215 recebeu muitas críticas da comunidade acadêmica e da comunidade da sociedade civil, críticas com as quais eu comungo, exatamente por todos os princípios que explorei aqui. O dispositivo e as tentativas de se fazer com que autoridades policiais, autoridades investigativas tenham acesso a dados cadastrais ou a metadados, às vezes, sem ordem judicial, fere de maneira flagrante a proteção constitucional, que é garantida a privacidade.

O Poder Judiciário, como eu disse, é o órgão competente para avaliar em que circunstâncias e sob que argumentos essa quebra pode ser conferida, e isso deve continuar assim. Esses dados cadastrais podem colocar em risco ou expor indevidamente usuários, e isso não deve acontecer. É muito importante que se preserve o crivo judicial nesses casos.

Em relação aos dois outros projetos de lei, o PL 1.879 e o PL 2.390, também ressalto aqui uma preocupação bastante grande em relação às tentativas de controle da atividade do usuário e da identificação prévia de todas as suas

atividades na Internet. Então, imaginem os senhores se uma grande base de dados se formaria a partir de toda a navegação de todos os cidadãos brasileiros — aqui teriam que se conectar por meio do CPF. Imaginem os senhores a sensibilidade desse banco de dados. Basta pensar em um tipo de aplicação na Internet que é muito utilizada por todos os cidadãos, que são os mecanismos de busca. Se tivermos todos os termos de busca procurados por um cidadão, dentro do seu CPF, isso, com certeza, dá margem a um perfil bastante complexo e sensível do que aquele cidadão lê, pelo que ele se interessa, quais são as coisas pelas quais ele tem curiosidade, gerando, certamente, situações de descontextualização e abuso. Então, existem vários exemplos da atuação abusiva e descontextualização desses tipos de informação.

Existe, por exemplo, um caso, nos Estados Unidos, em que um roteirista que fazia um roteiro para um seriado de televisão, um seriado criminal, que fez uma série de buscas sobre como matar a esposa, envenenamento, técnicas de envenenamento, técnicas que utilização de bombas caseiras, etc. acabou sendo investigado pelo FBI. E demorou bastante tempo para que ele conseguisse provar que aqueles termos de busca pelos quais ele estava procurando eram para subsidiar o roteiro da série de TV que estava escrevendo, e não, necessariamente, ligados a planos de ataques terroristas, ou coisas nesse sentido.

Então, a mesma coisa acontece com o Cadastro Nacional de Acesso à Internet que, embora tenha uma finalidade louvável, que é de garantir uma experiência de Internet mais adequada a crianças e adolescentes, talvez a medida seja não reprimir ou impedir esse acesso, que porventura poderia acontecer com um dispositivo de um amigo, de um colega, de um familiar, e que não necessariamente seria completamente eficaz. Eu acho que, nesses casos, a principal medida que deve vir é a medida de educação, da conscientização desses jovens de como usar a Internet de forma saudável, de quais são as possibilidades da tecnologia para a sua educação, para a sua formação, como cidadão, para que no futuro essa criança, esse adolescente, quando virar adulto, também use a Internet de forma responsável. Então mais do que proibir e repelir esses conteúdos, eu acho importante campanhas de conscientização e educação.

Além disso, estão à disposição — e isso é um dispositivo até do próprio Marco Civil — dos pais, educadores, *softwares* de controle parental que ajudam a conferir a experiência da Internet do jovem adolescente enquanto ele é educado etc. Até é uma experiência um pouco mais saudável, um pouco mais segura na internet. O Marco Civil, inclusive, ressalta, destaca que essa possibilidade, essa faculdade está à disposição para os pais.

Por último, em relação aos perfis *fakes*, como eu comentei aqui, esses perfis, em geral, partem do pressuposto, ou da ideia, um pouco do mito até de que, ao criar um perfil *fake* o cidadão estaria protegido, ou estaria menos identificável, e seria mais fácil, então, cometer aquele crime e ficar impune, mas, tal como descrevi aqui brevemente, isso não é verdade. Então, mesmo dos perfis *fakes* há a possibilidade de se requerer dos provedores de aplicações de Internet qual o endereço de IP e a data e a hora em que foi acessada, foi criada aquela conta. Então, se vai ao provedor de conexão para que se consiga identificar, efetivamente, qual foi o terminal, independentemente de a pessoa ter atuado em nome próprio ou em nome de um perfil *fake*.

Então, por mais que essa tenha sido uma prática que tem aumentado, eu acho que ela, ainda assim, não é uma prática eficaz, e que, de alguma maneira, não encontra respaldo jurídico ou técnico adequado para que seja proibida.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Com a palavra o Deputado Rodrigo Martins.

O SR. DEPUTADO RODRIGO MARTINS - Eu queria... Eu sou o Sub-Relator da área de Segurança, e queria questionar o Dennys. Pelo que eu entendi, ele não concorda com a liberação do número do IP da pessoa para que a polícia, por exemplo, possa fazer algum tipo de investigação — somente o número. E, talvez, com o número do IP, — pelo menos foi o que nós já ouvimos aqui, na CPI —...com aquele determinado número de IP talvez seja fácil, ou não tão difícil, descobrir por onde o usuário percorreu. Mas nisso, você não ter o acesso, você não facilitar o acesso ao número do IP, dificulta algumas investigações policiais. É lógico, é claro, a Justiça, às vezes, por uma série de razões, tem uma dificuldade de agilizar um despacho.

E eu fico me perguntando, no caso, por exemplo, de pedofilia, um caso de sequestro, um caso um caso mais complicado: qual seria a sugestão, então, que o senhor traria para esse tipo de alteração na legislação não acontecer, mas de uma forma que venha facilitar, ajudar a identificação de que aquele IP foi usado pelo cidadão tal, em tal lugar? Então, é esse o meu questionamento.

O SR. DENNYS MARCELO ANTONIALLI - Obrigado, Deputado. Comungo, certamente, da sua preocupação legítima em identificar e coibir esses casos, especialmente quando se trata de casos mais extremos, como esses exemplos que mencionou.

Minha resposta para esses casos é continuar acreditando que o crivo judicial é necessário para o acesso a esses tipos de informações. Nesses casos mais extremos, eu acho que o uso de medidas cautelares ou medidas de urgência perante o Poder Judiciário se justificam e poderiam garantir o acesso a essas informações de maneira mais agilizada.

Ressalto também que o fato de a ordem judicial ser necessária e de que, às vezes, tomar algum tempo não prejudica o acesso a essas informações justamente porque, como eu mencionei, o Marco Civil obriga tanto os provedores de aplicações quantos os provedores de conexão a guardar, por um tempo determinado — no caso dos de aplicações, por 6 meses, e no caso dos provedores de conexão, por 1 ano — essas informações. Então, elas vão ficar guardadas ali, e assim que uma ordem judicial der permissão para que as autoridades investigativas tenham acesso a essas informações, elas poderão fazê-lo. Inclusive podem, essas autoridades, requerer cautelarmente que elas sejam guardados por um tempo maior.

O SR. DEPUTADO RODRIGO MARTINS - No caso de uma investigação funciona, até porque o culpado pode ser identificado, mas, no caso de risco de vida, não adianta guardar aqueles dados se uma pessoa for morta, por exemplo. Vai identificar o assassino, mas a vida já se foi.

O SR. DENNYS MARCELO ANTONIALLI - Não, claro, mas...

O SR. DEPUTADO RODRIGO MARTINS - São esses casos que a gente fica... Eu, enquanto Sub-Relator, fico me questionando. Eu não tenho ainda uma posição fechada.

O SR. DENNYS MARCELO ANTONIALLI - Com certeza.

O SR. DEPUTADO RODRIGO MARTINS - Lógico que estamos escutando, estamos na fase de oitiva, vamos discutir com os outros Sub-Relatores e com a própria Presidente, mas realmente deixa... coloca-nos na dúvida.

O SR. DENNYS MARCELO ANTONIALLI - Hum, hum.

O SR. DEPUTADO RODRIGO MARTINS - Há necessidade urgente, o que se fazer... Hoje, todos nós temos um número.

O SR. DENNYS MARCELO ANTONIALLI - Hum, hum.

O SR. DEPUTADO RODRIGO MARTINS - É o CPF, é o RG. Talvez, se o IPv6 tivesse sido implantado já no Brasil, e cada máquina, cada ponto de Internet tivesse um IP fixo, esse IP poderia ser realmente fixo, assim como um CPF de um cidadão. Mas eu fico sempre me questionando: enquanto isso não chegar, como nós faremos?

O SR. DENNYS MARCELO ANTONIALLI - Nesses casos, eu defenderia novamente a utilização das medidas de urgência perante o Poder Judiciário. As cautelares e as medidas de urgência garantem que você tenha um acesso com ordem judicial. Pode chegar no mesmo dia, pode chegar em 2 dias, um despacho com um juiz para que, em casos de urgência, o acesso a essas informações seja concedido. Daí, de novo, eu ressalto a importância do crivo judicial para que a quebra do sigilo e da privacidade seja decretada.

O SR. DEPUTADO RODRIGO MARTINS - Então, o senhor é contrário à identificação de um IP por uma pessoa, por exemplo.

O SR. DENNYS MARCELO ANTONIALLI - Em que sentido?

O SR. DEPUTADO RODRIGO MARTINS - Uso exclusivo de um IP por uma determinada pessoa.

O SR. DENNYS MARCELO ANTONIALLI - Não, não sou contrário. Acho que isso levanta uma série de questões e desafios...

O SR. DEPUTADO RODRIGO MARTINS - Sim.

O SR. DENNYS MARCELO ANTONIALLI - ... no sentido de que será muito mais fácil você ter um perfil completo, sobretudo o que se fez na Internet. Então, toda a navegação daquela pessoa, se ficar sempre ligada a um número, seja um número de IP, seja o cadastro do CPF...

O SR. DEPUTADO RODRIGO MARTINS - Um número fixo.

O SR. DENNYS MARCELO ANTONIALLI - ... isso expõe, de uma forma muito mais severa, o usuário. E aí, sim, defenderia ainda com mais veemência a necessidade de ordem judicial para que fosse acessada qualquer tipo de atividade por esse número que fosse tido como único.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Eu, na verdade, queria só saber aqui, também, uma opinião em relação a tudo isso que foi discutido, se o senhor acha que hoje dá para se desvendarem e descobrirem todos os crimes cometidos pela Internet. Como o senhor enxerga isso? Porque, às vezes, a gente escuta pessoas que falam das dificuldades, veem as questões; outros dizem que não, que é possível. Então, eu gostaria de saber dessa opinião específica, principalmente do senhor. E da InternetLab também.

O SR. DENNYS MARCELO ANTONIALLI - Obrigado, Deputada.

De fato, como explorei aqui, eu acredito que no estado da técnica atual, da arquitetura da Internet, como está arquitetada, seja muito difícil praticar crimes que não deixem rastros. Então, em geral, é possível sim, a partir dos caminhos que identifiquei aqui brevemente, perseguir, condenar e responsabilizar pessoas que eventualmente cometeram crimes.

O que eu acho que é importante nesse momento salientar é a necessidade de uma atualização do corpo técnico para que sejam utilizados mecanismos pouco intrusivos à privacidade, mas também eficazes. E que esses caminhos e o acesso a esses dados que permitem a identificação sejam, como tenho repetido, objeto do crivo judicial, para que se tenha acesso a essas informações sem prejudicar a privacidade dos usuários.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Deputado Leo de Brito, alguma consideração? *(Pausa.)* Deputado Rodrigo Martins? *(Pausa.)*

Quero aqui, mais uma vez, aproveitar e agradecer a sua participação em ter aceitado o convite desta Comissão, o requerimento do nosso Deputado Leo de Brito, para nos ajudar aqui, sem dúvida, a construir relatórios positivos no final desta Comissão. O nosso Sub-Relator Deputado Rodrigo Martins, tenho certeza, vai cada vez mais poder ir a fundo nesse tema também.

Agradeço ao senhor, como Diretor-Presidente, e a todos que também estão ligados à InternetLab.

Nada mais havendo a tratar, declaro encerrada a presente reunião, antes convocando reunião ordinária da Comissão para a próxima terça-feira, dia 17 de novembro, às 15 horas. O tema será Secretarias de Finanças do Município e do Estado de São Paulo.

Bom dia a todos!

Está encerrada a reunião.