CÂMARA DOS DEPUTADOS

DEPUTADO FEDERAL RODRIGO MARTINS

RELATÓRIO PARCIAL DE SEGURANÇA CIBERNÉTICA NO BRASIL

Em relação à nossa Sub-Relatoria, afeta à questão da Segurança Cibernética no Brasil, temos a apresentar as seguintes sugestões.

1 – Melhor tipificação do tipo penal de invasão de dispositivo informático contido na Lei Carolina Dieckmann (Lei nº 12.737/12)

Os depoimentos de delegados e membros do Ministério Público alertaram para o fato de que a Lei Carolina Dieckmann (Lei nº 12.737/12), que alterou o Código Penal mediante a inclusão do artigo 154-A tipificando como crime a "Invasão de dispositivo informático", possui redação que dificulta sua aplicação pela justiça. Em depoimentos à CPI, essas autoridades informaram que o simples uso de dispositivos por terceiros, mesmo que sem autorização, não caracterizaria crime, na visão dos juízes. Ademais, a simples quebra de sistemas de segurança ou, ainda, a alteração de páginas de internet – a chamada pichação virtual – ou de perfis nas redes sociais não configurariam automaticamente crime, de acordo com a redação dada.

Por esses motivos, sugerimos a apresentação **de Projeto de Lei aperfeiçoando a redação do tipo penal em comento.**

2 – Guarda dos registros de conexão por todos os provedores de internet e migração para o IPv6

Em diversas audiências públicas os membros desta CPI foram alertados de que novas modalidades de conexão à internet se utilizam de tecnologias que permitem o compartilhamento de endereços IPs, isto é,

compartilham o mesmo número que identificaria de maneira única o dispositivo conectado à internet, o que impediria a correta identificação dos internautas. Nesse sentido, o Serviço de Repressão a Crimes Cibernéticos da Polícia Federal salienta a necessidade da guarda não apenas dos endereços IPs, mas também das portas utilizadas por cada usuário[1].

Dentre as tecnologias, incluem-se o popular NAT 44, muito utilizado em conexões sem fio, do tipo *wi-fi* em pontos de acessos compartilhados, os chamados *hot spots*. Esse problema decorre, na verdade, da escassez na quantidade de IPs disponíveis em sua versão 4, o qual seria solucionado com a adoção da versão 6, o chamado IPv6.

No entanto, devido ao atual estágio de desenvolvimento e outras limitações, tais como de adaptação de conteúdos e de equipamentos, como relatado por especialistas e operadoras de telecomunicações em Audiência Pública nesta CPI, não é possível tecnicamente a adoção imediata da nova versão. Todavia, entendemos que a Anatel não tem tratado a questão da migração para o IPv6 com a prioridade necessária. Entendemos que a agência deveria incentivar mais enfaticamente a sua adoção por parte da indústria e das empresas do setor.

No aprofundamento da análise do tema, esta Sub-Relatoria pondera que a falha na identificação dos internautas não decorre naturalmente do uso da tecnologia e sim, de falha na regulamentação.

Notadamente, a definição, pelo Marco Civil da Internet (MCI, Lei nº 12.965/14), do que constitua provedor de internet e suas obrigações deixa um vazio legal para determinados tipos de provedores de conexão. O MCI dispõe que apenas os administradores que possuem endereços IP diretamente alocados pela autoridade de registro da internet no Brasil, o Cgi.br, possuem a necessidade de guardar registros de conexão de

---

[1] Ofício nº 2/2016-CGPFAZ/DICOR/DPF.

seus usuários. Para esclarecimento, chamaremos esses provedores de primários. Normalmente provedores primários são grandes empresas e entidades governamentais, que gerenciam grande quantidade de usuários e de conexões. Dentre elas, as companhias telefônicas, do cabo e entidades Estaduais e Federais.

Assim, de acordo com a Lei, provedores de conexão não primários, que por sua vez são usuários daqueles provedores, estão isentos da obrigação da guarda de registros de usuários. Como consequência, indivíduos podem acometer toda sorte de crimes cibernéticos quando conectados a esses provedores não primários com a certeza da impunidade, uma vez que seus registros de conexão não serão guardados.

De maneira acertada, e afortunada para esta CPI, essa incorreção no MCI já foi objeto de proposição, na forma do PL 3.237/15. Por esses motivos, concluímos por:

1. **manifestar nosso apoio ao PL 3.237/15 que determina a guarda unívoca dos registros de conexão por todos os provedores de conexão; e**

2. **oferecer Indicação ao Sr. Ministro de Estado das Comunicações sugerindo à Agência Nacional de Telecomunicações a adoção das medidas necessárias para a implantação do IPV6 no país**.

3 – Elaboração de Termo de Cooperação com os principais agentes na internet para a promoção da educação práticas seguras de navegação

Assim como no caso dos crimes contra crianças e adolescentes, em que se verificou a necessidade de educação específica para

o uso seguro da internet, existe a mesma necessidade para usuários adultos. Nas investigações, nos relatos das operações policiais e nos testemunhos oferecidos à CPI, ficou patente a desatenção dos internautas brasileiros com a questão da segurança. Falta de uso de programas antivírus, firewalls e fornecimento de informações sigilosas sensíveis são algumas das práticas que sabidamente facilitam o acometimento de crimes cibernéticos. Fraudes bancárias, estelionatos e até roubos e assaltos são facilitados pela quantidade de informações doadas de maneira desavisada por parcela significativa de internautas, assim como pelo não uso de ferramentas de proteção.

Por esses motivos, os integrantes desta CPI entendem que a segurança da internet passa pela educação dos internautas. Nesse sentido, concluímos pela necessidade de **elaboração de Termo de Cooperação a ser celebrado entre as operadoras de telefonia e principais provedores de acesso à internet, principais provedores de aplicações de computador e de internet e o Ministério Público Federal, no sentido de promover ações educativas continuadas para o uso seguro da internet por adultos.**

4 – Alocação de recursos do Fistel – Fundo de Fiscalização das Telecomunicações – para manutenção das polícias especializadas

As investigações desta CPI evidenciaram que o combate aos crimes digitais possui maiores chances de sucesso quando as polícias judiciárias possuem equipes especializadas para tratar do assunto. Na verdade, a constituição de órgãos específicos pelas polícias judiciárias já está prevista na Lei nº 12.735/12, conhecida como Lei Azeredo, oriunda do PL 84/99, de autoria do Deputado Luiz Piauhylino. No entanto, as investigações demonstraram a falta de estruturas constituídas para esse fim nas polícias estaduais, salvo raras exceções (esta CPI, inclusive, encaminhou ofício para

todos os Estados da Federação questionando a existência ou não de delegacias especializadas, mas as respostas não chegaram antes da conclusão do presente Relatório). Ademais, ficou evidente a falta de materiais humano e de equipamentos e de infraestrutura. A razão mais óbvia é a reconhecida falta de recursos perenes para o setor.

Esta Sub-Relatoria identificou que o Fistel (Fundo de Fiscalização das Telecomunicações), instituído pela Lei nº 5.070/66, com a finalidade de custear os custos regulamentares devidos ao exercício do poder de polícia por parte do Estado sobre os serviços de radiodifusão, é a fonte acertada para esse financiamento.

É sabido que os recursos arrecadados pelo Fistel (Fundo de Fiscalização das Telecomunicações), instituído pela Lei nº 5.070/66, e não repassados à Anatel perfazem a maioria das receitas do fundo e que tais recursos tem sido sistematicamente derivados para o Tesouro para fortalecimento de caixa e combate ao déficit fiscal. Entretanto, acreditamos que, em se tratando de fundos arrecadados em função do poder de polícia do Estado, uma parte desses recursos contingenciados poderia voltar ao sistema fortalecendo as polícias judiciárias no combate ao mau uso das telecomunicações.

Ressaltamos que o crime cibernético no País drena recursos da ordem de R$ 1 bilhão anuais, segundo estimativas, portanto, o retorno de parcela do Fistel para a estrutura de combate ao crime tem o potencial de diminuir essas perdas, grande parte das quais se concentra em entidades públicas. Assim, o descontingenciamento de recursos voltaria ao caixa da Administração na forma de maior eficiência em suas instituições.

Por esses motivos, sugerimos:

1. **Oferecer Projeto de Lei autorizando a aplicação de até 10% das receitas do Fistel transferidas para o Tesouro Nacional para o financiamento das**

estruturas de combate a crimes cibernéticos, previstas na Lei nº 12.735/12; e

2. **Oferecer Indicação ao Ministério da Justiça, sugerindo o estabelecimento de convênios entre as polícias federal e civis dos estados para aplicação de receitas do Fistel, transferidas para o Tesouro Nacional, no financiamento das estruturas de combate a crimes cibernéticos.**

5 – Fiscalização por parte do TCU das ações da Anatel no que diz respeito ao cadastro dos acessos pré-pagos à internet

A perpetuação de todo crime cibernético inicia-se pelo acesso à internet. Assim, em se fiscalizando as formas de acesso à internet e identificando corretamente os usuários da grande rede é possível reduzir a ocorrência de crimes digitais.

O avanço da tecnologia e a massificação do uso, no entanto, estabelecem uma corrida ininterrupta entre malfeitores e órgãos de fiscalização e controle, onde os primeiros iniciam sempre em vantagem. Dentre os avanços tecnológicos e de mercado uma das ferramentas mais utilizadas para o acometimento de crimes pela internet é a utilização do pré-pago.

Incialmente, os pré-pagos eram utilizados para práticas de extorsão para a compra de créditos. Atualmente, com o advento dos smartphones e das redes sem fio, esses telefones oferecem suporte completo para o acometimento dos mais variados crimes. Os trabalhos desta CPI verificaram que a compra de chips pré-pagos são extremamente facilitados pelas práticas das operadoras. Basta cadastrar um CPF fictício e é possível habilitar uma linha celular, adquirir um mínimo de créditos para tornar a linha operacional e navegar pela internet utilizando-se de redes wi-fi gratuitas

apontadas para as unidades prisionais. Cabe salientar, ainda, que o acesso a número de celular é fundamental para a criação de contas e perfis nos principais aplicativos de internet, tais como Google e Facebook. Portanto, a correta identificação dos usuários é imperativa no combate aos crimes cibernéticos.

Ocorre, no entanto, que esse cadastramento extremamente liberal por parte das operadoras é, na verdade, ilegal. A Lei 10.703/03 que dispõe sobre o cadastro de usuários de telefones pré-pagos, determina que, além do CPF, deverão constar do cadastro nome e endereço completos. Logicamente, para que o cadastro faça sentido deve haver uma conferência pelos estabelecimentos que comercializam esses chips, ou em última instância, pelas operadoras, para garantir a integridade do cadastro. Em outras palavras, se a prática comercial permite o uso de CPFs descasados do nome e da prova do endereço residencial, o procedimento equivale, na prática, ao descumprimento da Lei. Nesse caso cabe à Anatel agir e fiscalizar os procedimentos que estão sendo tomados pelas empresas em sua órbita de regulação. Em Audiência Pública nesta CPI, as operadoras foram unânimes em admitir a existência de falhas nesses cadastros de usuários do pré-pago.

Por esses motivos, **sugerimos a apresentação de Proposta de Fiscalização e Controle para que, com auxílio do Tribunal de Contas da União, seja verificado quais procedimentos são tomados pela Anatel para a garantia da integridade dos dados constantes nos cadastros das operadoras de telefonia dos usuários da telefonia pré-paga, de que trata a Lei nº 10.703/03**.

6 – Projeto de Lei para permitir a identificação automática de usuários da internet em casos de iminente risco à vida.

A prática do *cyberbullying*, o estupro virtual e as mais variadas formas de ameaças e extorsões pelas redes de comunicação são casos recorrentes no Brasil e no mundo. Foram relatados a esta CPI diversos casos em que vítimas dessas práticas funestas estiveram sob iminente risco de vida e em que as autoridades policiais estavam impedidas de agir de modo a cessar as ameaças. O entendimento das autoridades ouvidas nesta CPI é de que o procedimento de quebra do sigilo das comunicações para estes casos de iminente risco à vida deveria ser invertido. Apenas para esses casos, a autoridade policial deveria poder solicitar os dados do assinante diretamente à operadora telefônica e esta deveria estar obrigada a fornecer essas informações. De forma a coibir abusos, a sugestão é de que a autoridade policial notifique o juiz a cada caso de quebra e este, ao analisar os casos, irá verificar se houve excesso, determinando as penas cabíveis, caso necessário.

Esse entendimento, com o qual também concordamos, é análogo ao contido no Substitutivo aprovado ao PL 6.726/10, na CCTCI, apresentado pela relatora na Comissão, Deputada Margarida Salomão, e que atualmente encontra-se na Comissão de Finanças e Tributação. No entanto, o PL em questão trata exclusivamente da quebra do sigilo de localização de aparelhos celulares, em casos de iminente risco de vida dos usuários. O projeto foi uma resposta aos reiterados casos em que as autoridades policiais se viam impedidas de obter a localização de pessoas sequestradas, pois o sigilo compreenderia também a localização.

Isto posto, somos do entendimento que o PL 6.726/10 deveria ser ampliado o escopo, para permitir a quebra das comunicações e não apenas da localização. Entretanto, como a proposta ainda se encontra em análise por outras Comissões não temos a garantia de que tal inclusão seja feita. Por esse motivo, temos a compreensão de que a melhor forma de contribuir para a mitigação desses tipos de crimes digitais que atentam contra a vida seja pelo **oferecimento de novo Projeto de Lei determinando a possibilidade da quebra do sigilo de comunicação de usuários em risco**

iminente de vida por parte de autoridades de investigação, com notificação ao juiz, para atuação em caso de abuso.

7 – Indicação para implantação de Plano de Boas Práticas em Segurança da Informação na Administração.

Na questão da segurança das redes do governo, dentre as variadas Audiências Públicas realizadas, chamou a atenção aos membros desta CPI o depoimento dado por representante do Gabinete de Segurança Institucional da Presidência da República – GSIPR. O representante indicou a existência inúmeros ataques cibernéticos diários, muitos dos quais são encaminhados (60, em média, por dia) ao Centro de Tratamento de Incidentes de Redes da Administração Pública Federal. A vastidão dos ataques inclui, em ordem decrescente, abuso de sítio (23%), existência de páginas falsas (21%) e golpes *phising* (16%). Em Audiência Pública, os responsáveis pela segurança na área de TI do governo, apresentaram como uma das principais ações para o fortalecimento da segurança das redes do governo, a elaboração do documento "Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal", de 2015.[2] O documento, oferecido pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, deve ser considerado como o ponto de partida para o planejamento e o melhoramento da segurança e da resiliência das infraestruturas críticas dos serviços de TI da Administração. Nos próprios termos publicados no documento, a estratégia servirá para elevar a segurança da informação e comunicações e a segurança cibernética pública a níveis de excelência.

---

[2] Documento disponível em http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrategia_de_SIC.pdf, acessado em 23/11/15.

Na verdade, o basilar documento é uma resposta à recomendação contida no Acórdão 3.051/14 do Tribunal de Contas da União, que realizou auditoria de governança e gestão de TI em 30 entidades da Administração em que encontrou, especificamente no quesito segurança da informação:

> *"Planejamento inadequado e inexistência de análises de risco consistentes que respaldem as ações de segurança da informação. Falhas recorrentes no estabelecimento de processos como: gestão de continuidade de negócio, controle de acesso, gestão de riscos de segurança da informação e gestão de incidentes."*[3]

A falha apontada pelo Tribunal indicou à Sub-relatoria a necessidade de aprofundamento da investigação do assunto. Nessa análise, a CPI se deparou com farto material produzido pelo TCU.

O citado Acórdão 3.051/14, apresenta o índice iGovTI – Índice de Governança de TI – que mede a qualidade na gestão dos recursos de TI das instituições. Dando continuidade a esses levantamentos, o órgão publicou o Acórdão 3.117/14, "Levantamento de Governança de TI 2014",[4] que realizou aprofundado questionário em 372 organizações dos três poderes da União. Esta CPI se debruçou sobre os dados levantados por esses procedimentos e solicitou aos técnicos daquele órgão que elaborassem um índice específico que avaliasse a segurança das informações para aquele universo de entidades federais. O iGov-TI-SegInfo é o resultado dessa solicitação.

---

[3] "Governança e Gestão de TI em 30 Auditorias", TCU. Disponível em file:///C:/Users/P_6706/Downloads/2688968.PDF, acessado em 23/11/15.

[4] Informativo disponível em file:///C:/Users/P_6706/Downloads/Levantamento%20de%20governan%C3%A7a%20de%20TI%202014.pdf, acessado em 05/01/16.

O iGov-TI-SegInfo gerado pelo TCU busca aferir a qualidade do tratamento dado à segurança das informações pelas instituições federais. A figura abaixo apresenta o índice apurado do total de 372 instituições públicas federais investigadas pelo TCU.

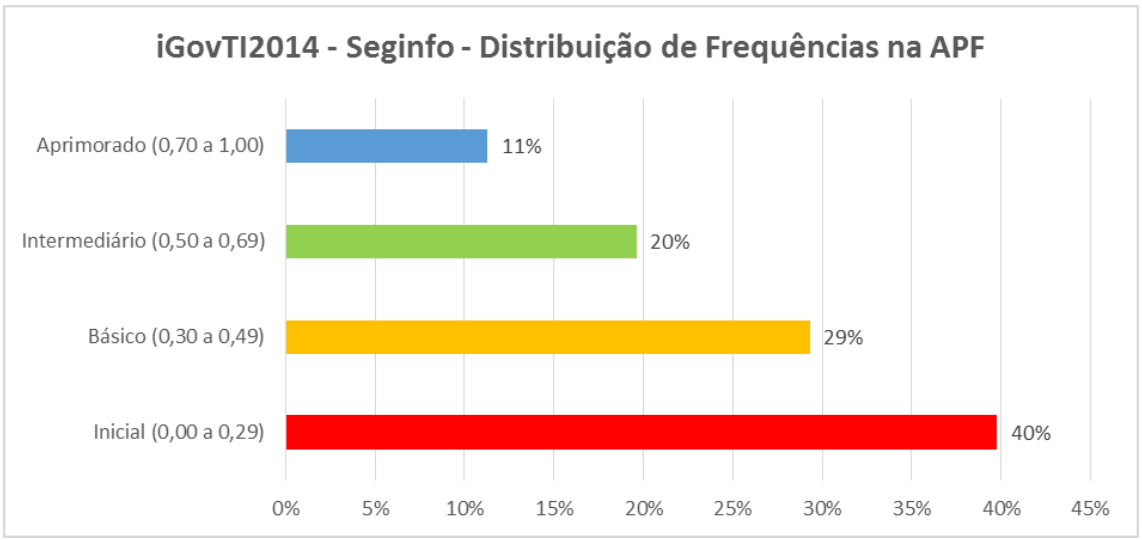


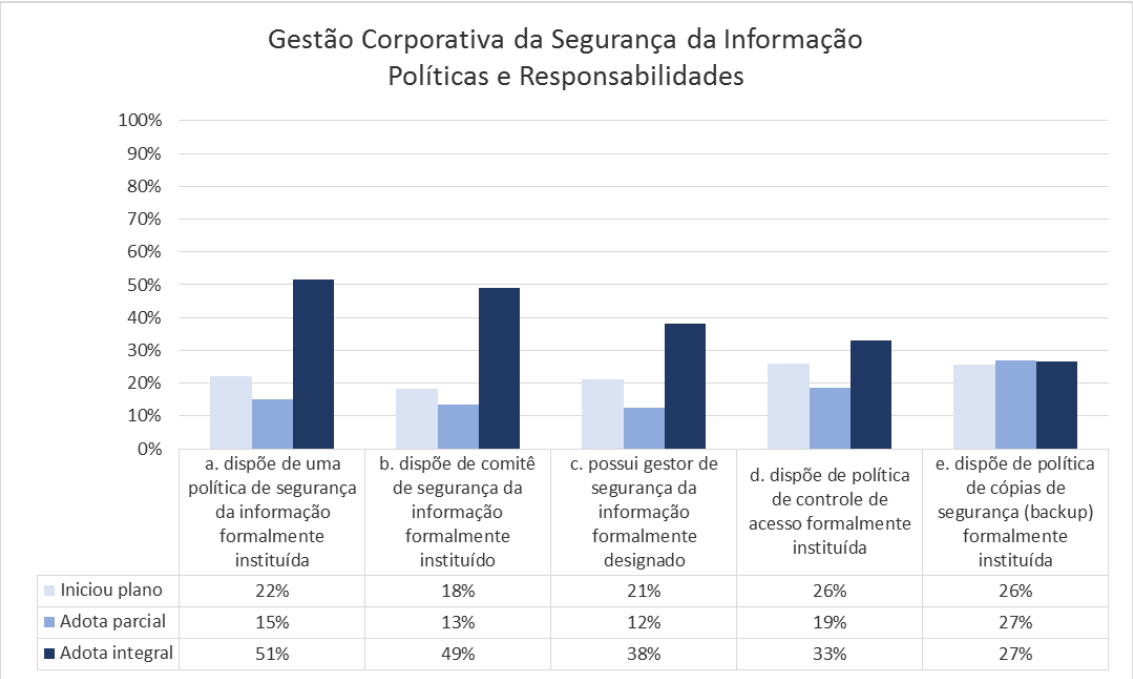
Figura – Índice SegInfo

Fonte: Elaborado com base em dados fornecidos pelo TCU coletados no âmbito do iGovTI2014

Como pode se ver da figura anterior, a Administração Pública Federal possui poucas instituições com aprimorada gestão da segurança de suas informações, apenas 11% das instituições (correspondente a 42 entidades). Em contrapartida, 40% (148 entidades) possuem controle classificado como “inicial”. Isto é, um expressivo conjunto de instituições não implementa uma série de procedimentos que permitiriam diminuir a incidência de quebra de segurança das informações, tais como acesso indevido, ataques e pichações virtuais, roubo de dados ou outros sinistros na área de informática.

As figuras a seguir detalham os diversos fatores que geraram o índice geral em segurança das informações das instituições

públicas.[5]



	a. dispõe de uma política de segurança da informação formalmente instituída	b. dispõe de comitê de segurança da informação formalmente instituído	c. possui gestor de segurança da informação formalmente designado	d. dispõe de política de controle de acesso formalmente instituída	e. dispõe de política de cópias de segurança (backup) formalmente instituída
Iniciou plano	22%	18%	21%	26%	26%
Adota parcial	15%	13%	12%	19%	27%
Adota integral	51%	49%	38%	33%	27%

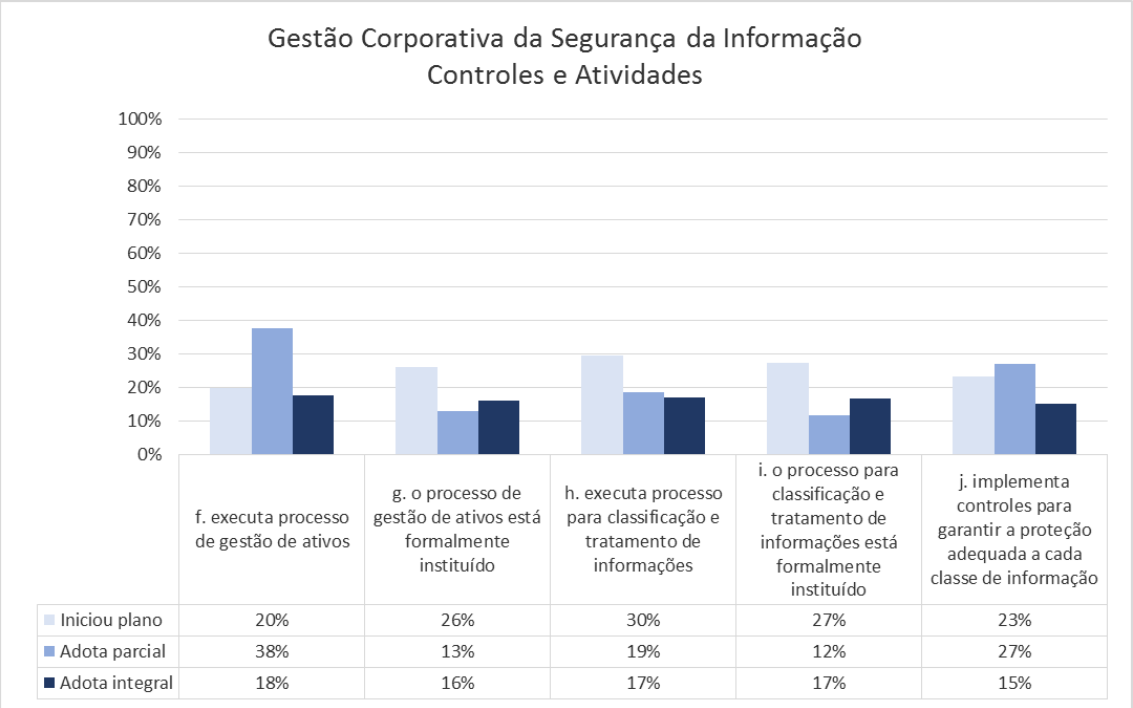
Figura – Políticas e Responsabilidades

A figura anterior - Políticas e Responsabilidades - indica que apesar de metade das instituições adotarem uma política de segurança para seus dados, apenas metade destas realiza regularmente back-ups de suas informações. Ademais, apenas um terço das empresas controla integralmente quem possui acesso às informações.

Além do estabelecimento de uma política formal para a gestão dos ativos e a responsabilização de equipes para a sua gerência, essas equipes formalmente estruturadas devem efetivamente gerir/monitorar os

[5] Fonte: Elaborado com base em dados fornecidos pelo TCU coletados no âmbito do iGovTI2014

ativos. A figura próxima detalha as ações nesse sentido.

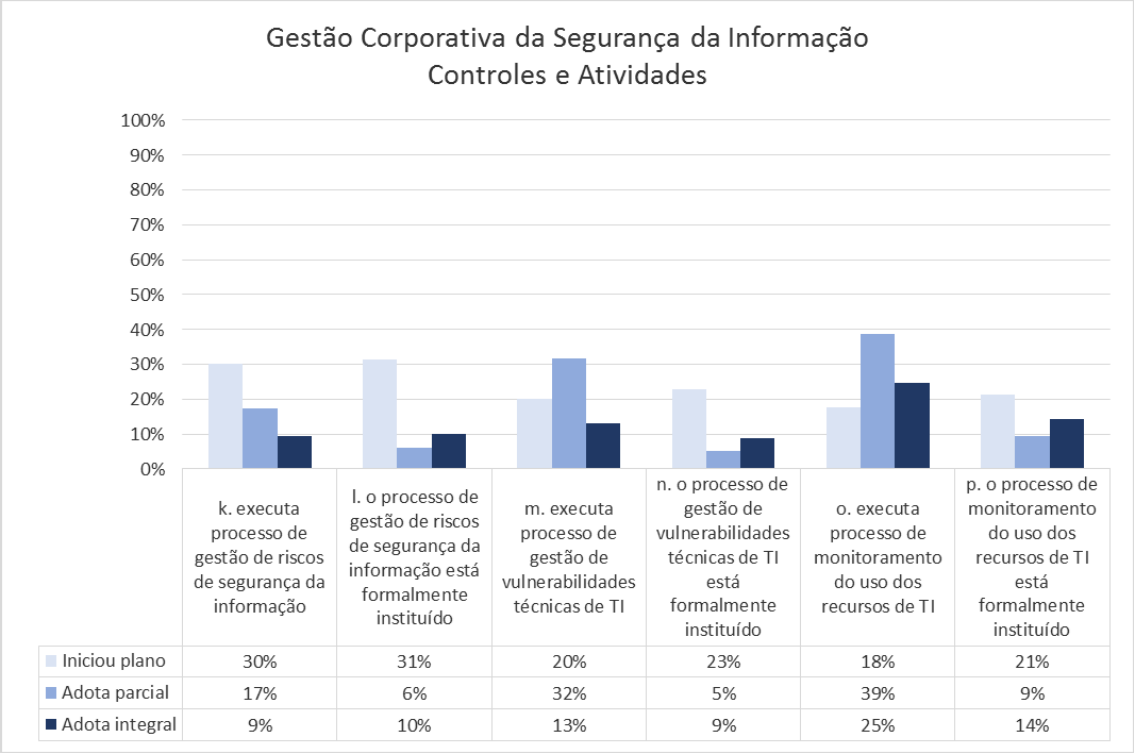


	f. executa processo de gestão de ativos	g. o processo de gestão de ativos está formalmente instituído	h. executa processo para classificação e tratamento de informações	i. o processo para classificação e tratamento de informações está formalmente instituído	j. implementa controles para garantir a proteção adequada a cada classe de informação
Iniciou plano	20%	26%	30%	27%	23%
Adota parcial	38%	13%	19%	12%	27%
Adota integral	18%	16%	17%	17%	15%

Figura – Controles e Atividades

A figura anterior – Controles e Atividades -, focada no processo de gestão dos ativos de informática, indica práticas ainda mais frágeis. Quase um terço das instituições não executam nenhum tipo de gestão de ativos de informática e apenas 15% do universo auditado implementam controles para garantir proteções especificas para cada tipo de dados.

Dando prosseguimento à gestão de ativos e dos dados das corporações, a próxima figura detalha a existência da previsão de procedimentos a serem seguidos em caso de ocorrência de contingências na área de TI.



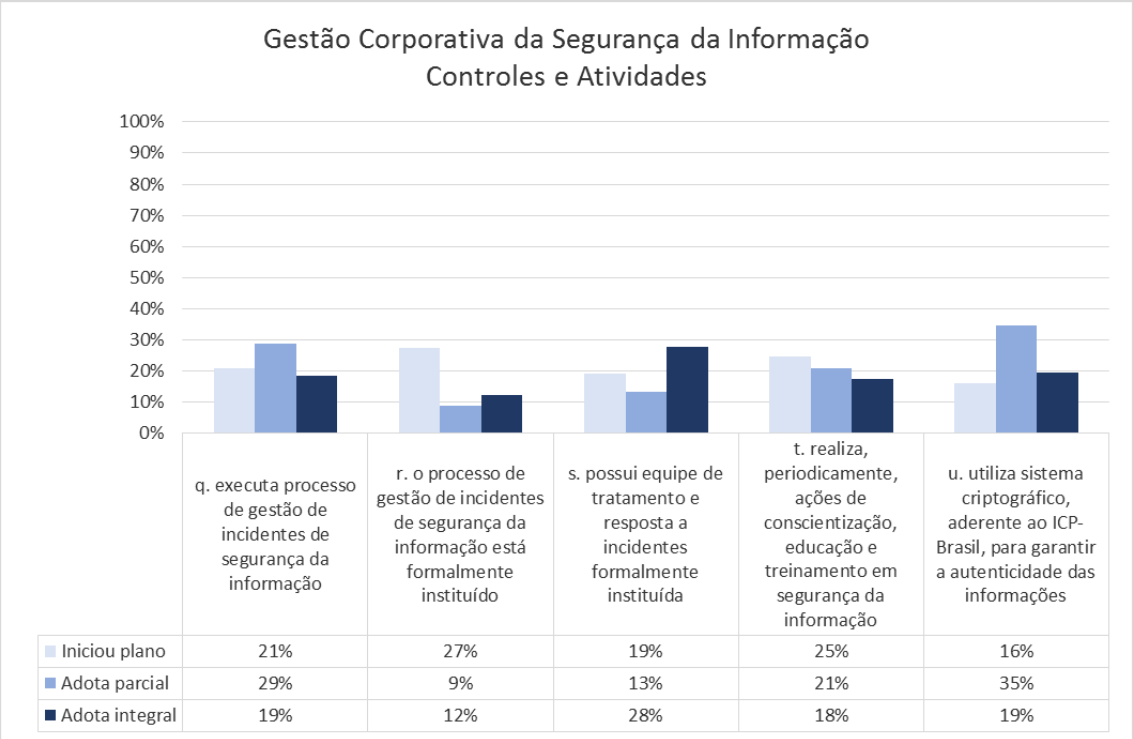
	k. executa processo de gestão de riscos de segurança da informação	l. o processo de gestão de riscos de segurança da informação está formalmente instituído	m. executa processo de gestão de vulnerabilidades técnicas de TI	n. o processo de gestão de vulnerabilidades técnicas de TI está formalmente instituído	o. executa processo de monitoramento do uso dos recursos de TI	p. o processo de monitoramento do uso dos recursos de TI está formalmente instituído
Iniciou plano	30%	31%	20%	23%	18%	21%
Adota parcial	17%	6%	32%	5%	39%	9%
Adota integral	9%	10%	13%	9%	25%	14%

Figura – Controle de Riscos

A análise da figura anterior – Controle de Riscos – sugere que a maioria das empresas monitora o uso dos recursos de TI e procura identificar de maneira sistemática riscos e vulnerabilidades em suas infraestruturas. No entanto, a grande maioria das empresas (90%, item ‘l’ e ‘m’) não possui, ou adota apenas parcialmente, planos para mitigar as vulnerabilidades apontadas na área de TI.

Identificadas as vulnerabilidades na infraestrutura, o passo seguinte verificado pela auditoria foi a identificação da existência de procedimentos seguidos pelas entidades em caso de ocorrência de incidentes informáticos. A próxima figura apresenta o desempenho das instituições públicas nesse quesito.

Figura – Gestão de Incidentes



	q. executa processo de gestão de incidentes de segurança da informação	r. o processo de gestão de incidentes de segurança da informação está formalmente instituído	s. possui equipe de tratamento e resposta a incidentes formalmente instituída	t. realiza, periodicamente, ações de conscientização, educação e treinamento em segurança da informação	u. utiliza sistema criptográfico, aderente ao ICP-Brasil, para garantir a autenticidade das informações
Iniciou plano	21%	27%	19%	25%	16%
Adota parcial	29%	9%	13%	21%	35%
Adota integral	19%	12%	28%	18%	19%

Embora os dados coletados pela auditoria não identifiquem quantitativos ou a ocorrência de incidentes na área de TI nas instituições, as respostas indicam que esse assunto não possui grande relevância. Apenas um terço das instituições já possuem equipes dedicadas para responder a incidentes (item ‘s’) e 12% possui procedimento integralmente implementado a ser seguido (‘r’). Proporção relativamente maior, aproximadamente a metade das instituições, adotou criptografia de chaves públicas para garantir a autenticidade das informações (‘u’). Em que pese o estágio incipiente na gestão de incidentes, o aspecto positivo na gestão desse quesito é que a maioria das instituições está atuando na prevenção, com ações de conscientização e de educação em seguranças das informações.

Em síntese, os documentos indicam que práticas de governança de tecnologias da informação, embora em uso crescente, ainda são distantes de um cenário satisfatório na Administração Pública Federal.

Entendemos que essa situação é extremamente preocupante quando as ameaças cibernéticas são praticadas por delinquentes, mas também por corporações privadas em busca de lucro e, até, por agências de inteligência de diversos países.

A espionagem eletrônica por meio das novas redes digitais, que interligam dados diversos e sistemas de suma importância para a vida das pessoas e para o setor produtivo, tem o potencial de subtrair recursos, assim como de paralisar o país em casos extremos.

Essas potencialidades são bem sabidas e documentadas e o fato mais concreto foi evidenciado com o episódio *Snowden*, tantas vezes mencionado ao longo desta CPI. A descoberta de que as Leis americanas, Calea e Patriota, obrigam a instalação de *backdoors* em sistemas de informática de empresas daquele país e que agências americanas podem levantar informações dentro e fora do país, são uma clara indicação de que o país deve agir com mais vigor.

Em que pese esta CPI não pôde investigar essas questões com maior detalhamento devido ao seu pronto encerramento, a curta análise indicou que o Brasil precisa ancorar sua infraestrutura de TI com maior ênfase em sua indústria nacional. Nesse sentido, julgamos pertinente que a infraestrutura seja auditada, com o auxílio de instituições brasileiras, contra a existência de *backdoors* e outros artifícios que porventura existam em seus equipamentos e softwares de TI.

Ademais, as entidades aqui mencionadas encarregadas da segurança deveriam auditar a segurança, a padronização de procedimentos e verificar as vulnerabilidades operacionais das principais redes de comunicação do país e, classificar, a exemplo do trabalho do TCU, as instituições.

Outro ponto salientado por esta CPI, no âmbito da Sub-Relatoria de Crimes Financeiros, foi a expertise do sistema financeiro em coibir crimes cibernéticos de maneira geral. Em que pese o tema ser atinente à outra Sub-Relatoria, julgamos conveniente que esse conhecimento seja incorporado pelas forças de defesa cibernética na forma de inciativas de cooperação tecnológica para o intercâmbio de informações, visando tornar o ambiente da internet no País, como um todo, mais seguro. Esta ação de compartilhamento de informações visa também ao crescimento do conhecimento da Administração em ferramentas de segurança de TI.

Entendemos que, em tempos de inúmeros ataques diários e de contingentes cada vez maiores de dados pessoais e de serviços prestados mediante o uso de ferramentas de TI, a adoção do conjunto de medidas discutidas neste tópico representaria uma ação mais incisiva por parte do Estado na proteção de sua infraestrutura de TI.

Pelos motivos expostos, julgo oportuno o **oferecimento de Indicação determinando à Administração Pública Federal, direta e indireta, a adoção, no âmbito de cada entidade, de: i) guia de boas práticas em segurança da informação; ii) medidas concretas de auditoria em sua infraestrutura pública de TI, e; iii) celebração de instrumentos de cooperação técnica entre autoridades públicas de segurança cibernética e entidades privadas.** (Parte III, 3.1)

8 – Melhor enquadramento das empresas estrangeiras às disposições legais brasileiras.

Durante a CPI diversas autoridades policiais, federais e estaduais, relataram a dificuldade de se fazer cumprir medidas judiciais que solicitam a identificação de usuários de aplicativos, assim como os dados referentes às suas comunicações. Alegou-se também ser Igualmente

dificultosa e morosa a retirada de conteúdos por ordem judicial, em alguns casos, de empresas globais. Neste ponto é preciso esclarecer que as depoentes restringiram esses problemas às principais empresas da internet global e excetuaram as operadoras de telefonia, uma vez que estas já possuem protocolos padronizados de atendimento às notificações e possuem mais pessoas em atividade no país para o fornecimento das informações.

Dentre as razões alegadas pelas empresas internacionais com presença no Brasil está o fato de que os dados não são armazenados no País e, portanto, as ordens judiciais não poderiam ser cumpridas. Nesse sentido, delegados apresentaram cópias de documentos de autoridades judiciais dos EUA exigindo, de maneira logica, até, que as requisições atendam aos requisitos legais e processuais daquele país, incluindo a tradução para o inglês.

O ápice deste imbróglio talvez possa ser ilustrado pelo episódio da determinação judicial de bloqueio nacional, por 48 horas, do Whatsapp, ocorrida em 17/12/15, por decisão da 1ª Vara Criminal de São Bernardo do Campo, do Estado de São Paulo. A medida, que causou uma certa comoção social no país, não chegou a perdurar pelo tempo determinado, tendo sido cassada pela justiça de segunda instância. Em sua decisão o desembargador considerou que "*não se mostra razoável que milhões de usuários sejam afetados em decorrência da inércia da empresa*"[6].

Esta CPI ouviu relatos das autoridades de investigação envolvidas com a causa e verificou que durante o processo foram aplicadas medidas gradativas de coerção, como multas. O pedido original das

---

[6] Trecho da decisão publicada no portal G1, em 17/12/15, "WhatsApp: Justiça concede liminar para restabelecer aplicativo no Brasil", disponível em http://g1.globo.com/tecnologia/noticia/2015/12/whatsapp-justica-concede-liminar-para-restabelecer-aplicativo-no-brasil.html, acessado em 23/02/16.

autoridades, que gerou a recusa no atendimento por parte do *Facebook* no Brasil ("Facebook Serviços Online do Brasil Ltda.), era para que o Whatsapp "espelhasse" em um computador da polícia, através do seu aplicativo para a internet, as mensagens trocadas pelos investigados via aplicativo telefônico.

Nesse processo, a filial do *Facebook* alegou que a empresa não possui gestão sobre a empresa responsável pelo aplicativo de mensagens, sendo que ambas são operadas de forma independente. Entretanto, a relatoria obteve acesso ao documento LAB-E 24/2015-MTMAP, do Laboratório de Análise de Crimes Eletrônicos da Polícia Civil do Estado de São Paulo, onde se conclui:

> *"'Facebook Serviços Online do Brasil Ltda.' é legítima subsidiária, controlada de fato e de direito pela empresa Facebook Inc., que adquiriu e tem plena gestão sobre Whatsapp Inc., sua subsidiária, e portanto, responsável por atender, nos termos de nossa legislação pátria, as autoridades brasileiras nas questões que envolvam os participantes desse mesmo grupo econômico."*

Assim, como as empresas, na verdade, pertencem ao mesmo grupo empresarial, a filial brasileira estaria obstaculizando e impedindo o andamento das investigações.

No aprofundamento do estudo acerca do assunto a CPI convidou representante dos EUA do Whatsapp. Em 01/12/15, Mark Kahn, Vice-Coordenador Jurídico Geral do aplicativo de mensagens, explicou que o sistema se utiliza de criptografia do tipo ponta-a-ponta e que as mensagens não são armazenadas em nenhum servidor da companhia e que portanto não há forma de acessar as informações dos usuários. Essa afirmação contradiz os termos do relatório da polícia do Estado de São Paulo, aqui relatado anteriormente, quando o investigador da corporação afirma que com a técnica do "espelhamento" seria possível monitorar as conversas de investigados.

Em reunião de trabalho com funcionários da Embaixada dos EUA, em 23/2/16, esta Sub-Relatoria solicitou informações acerca dos procedimentos realizados naquele país para obtenção dos registros de

usuários de aplicativos de mensagerias. Na ocasião foram confirmadas duas questões. Em primeiro lugar, foi reafirmada a questão do uso de criptografia ponta-a-ponta, porém não houve posicionamento claro acerca da possibilidade de utilização do "espelhamento". Em segundo lugar, os representantes daquele governo informaram que, as principais empresas de internet, e em especial o Facebook, possuem formulários on-line para denúncias por parte de usuários para retirada de conteúdos infringentes. No entanto, ressaltou que muitas vezes os pedidos são negados por não atenderem à legislação local (no caso a do Estado da Califórnia), especialmente quando as ordens não são chanceladas por uma segunda autoridade de investigação. Assim sendo, solicitações diretas de policiais envolvidos em investigações são sumariamente negadas.

Apesar da controvérsia com relação ao "espelhamento" do aplicativo, os diversos depoimentos deram conta de que há certa relutância em atender demandas judiciais por parte das subsidiárias brasileiras das empresas globais de internet. E aqui cabe ressaltar que estamos utilizando o termo genérico de subsidiárias sem entrar em maiores detalhes com respeito a direito comercial de registro de sociedades. O argumento das empresas "*ponto com"* passa invariavelmente pela afirmação de que os dados não são armazenados no país ou de que sua filial não possui mandato para representar determinadas atividades ou empresas coligadas. Assim, na falta de atendimento às demandas judiciais por parte das aplicações de internet, as autoridades recorrem a medidas coercitivas extremas que penalizam a toda a população.

A conclusão desta análise nos leva a crer que o Marco Civil da Internet (MCI, Lei nº 12.965/14) pode ser melhorado em sua redação de modo a melhor enquadrar as filiais nacionais de empresas estrangeiras do setor. Por isso, sugerimos a apresentação de **Projeto de Lei incluindo novo parágrafo ao artigo 22 do MCI, para determinar que filial, sucursal, escritório ou estabelecimento situado no País responde solidariamente**

pelo fornecimento de dados requisitados judicialmente de empresas com atuação no país e cuja matriz esteja situada no exterior.

9 – Visitas técnicas realizadas

Esta Sub-Relatoria realizou, ainda, visitas técnicas ao SERPRO, ao TSE e à DATAPREV, para verificar, *in loco*, como tais entes estão instrumentalizados para prevenirem-se contra ataques cibernéticos. Em todas as visitas, os entes aparentaram estar preparados para essa espécie de ataque, mas apontaram que, ultimamente, os investimentos na área de segurança estão sendo reduzidos, por conta de questões orçamentárias.

Essas são, em suma as nossas contribuições, que submetemos à apreciação do nobre Relator, com os respectivos anexos.

Sala das Sessões, em 30 de março de 2016.

Deputado RODRIGO MARTINS

ANEXOS

PROJETO DE LEI PARA ALTERAR A REDAÇÃO DO ART. 154-A DO DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940, PARA AMPLIAR A ABRANGÊNCIA DO CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO.

PROJETO DE LEI Nº , DE 2016

(Da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país)

Altera a redação do art. 154-A do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para ampliar a abrangência do crime de invasão de dispositivo informático.

O Congresso Nacional decreta:

Art. 1º Esta lei altera a redação do art. 154-A do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para ampliar a abrangência do crime de invasão de dispositivo informático.

Art. 2º O artigo 154-A do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, passa a vigorar com a seguinte redação:

"**Acesso indevido a sistema informatizado**

Art. 154-A. Acessar, indevidamente e por qualquer meio, sistema informatizado, ou nele permanecer contra a vontade expressa ou tácita de quem de direito:

Pena - detenção, de seis meses a dois anos, e multa.

§ 1º Na mesma pena incorre quem, sem autorização ou indevidamente, produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta descrita no *caput*.

§ 2º Se do acesso resultar:

I - prejuízo econômico;

II - destruição, danificação, inutilização, adulteração ou supressão de dados informatizados, ainda que parcialmente;

III - instalação de vulnerabilidade informática no dispositivo acessado;

IV - obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, arquivos, senhas, informações ou outros documentos ou dados privados;

V - controle remoto não autorizado do dispositivo acessado:

Pena - reclusão, de um a quatro anos, e multa, se a conduta não constitui crime mais grave.

§ 3º Se o crime é cometido contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal;

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal;

V - a Administração Pública direta ou indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos:

Pena - reclusão, de dois a quatro anos, e multa.

§ 4º Nas hipóteses dos §§ 2º e 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados, arquivos, senhas ou informações obtidas, ou se o acesso se dá mediante violação de mecanismo de segurança.

§ 5º Para os fins deste artigo, considera-se:

I - “sistema informatizado”: o computador ou qualquer dispositivo ou conjunto de dispositivos, interligados ou associados, em que um ou mais de um entre eles desenvolve o tratamento automatizado de dados informatizados através da execução de programas de computador, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informatizados armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos;

II - “dados informatizados”: qualquer representação de fatos, informações ou conceitos sob a forma suscetível de processamento em um sistema informatizado, incluindo programas de computador;

III - “mecanismo de segurança”: qualquer mecanismo que tem como finalidade evitar o acesso de terceiro não legítimo a um sistema informatizado e garantir autenticidade do detentor legítimo de acesso.” (NR)

Art. 3º Esta lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

Conforme apurado por esta Comissão Parlamentar de Inquérito, a legislação brasileira ainda é muito incipiente no que diz respeito aos crimes cibernéticos.

De fato, um dos únicos crimes que pode ser chamado de “*crime cibernético próprio*” previstos em nosso ordenamento jurídico é aquele

inserido no art. 154-A do Código Penal pela Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckmann), comumente chamado de "*invasão de dispositivo informático*".

Todavia, tal dispositivo foi elaborado de tal forma que diversas condutas que deveriam ser penalizadas não se encontram abrangidas pelo tipo penal. Para se ter uma ideia do absurdo, conforme afirmou a Dra. Fernanda Teixeira Souza Domingos, Procuradora do Ministério Público Federal, perante esta CPI, "*a lei chama-se Lei Carolina Dieckmann, **mas não abarcou a própria situação que a atriz sofreu**, que foi a obtenção e exposição de dados pessoais privados*".

Dessa forma, não há dúvida que a legislação precisa ser aprimorada neste particular.

É com esse intuito que apresentamos o presente projeto de lei, em grande parte inspirado na Convenção de Budapeste, na Lei nº 109/2009, de Portugal (legislação elogiada nesta Comissão por especialistas em crimes cibernéticos) e no projeto do novo Código Penal brasileiro, ainda em trâmite no Senado Federal.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

PROJETO DE LEI VISANDO À ALTERAÇÃO DA LEI Nº 5.070, DE 7 DE JULHO DE 1966, PARA AUTORIZAR O USO DOS RECURSOS DO FISTEL POR ÓRGÃOS DA POLÍCIA JUDICIÁRIA.

PROJETO DE LEI Nº , DE 2016

(Da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país)

Altera a Lei nº 5.070, de 7 de julho de 1966, autorizando o uso dos recursos do Fistel por órgãos da polícia judiciária.

O Congresso Nacional decreta:

Art. 1º Esta Lei altera a Lei nº 5.070, de 7 de julho de 1966, que cria o Fundo de Fiscalização das Telecomunicações – FISTEL – e dá outras providências, autorizando o uso dos recursos do fundo por órgãos da polícia judiciária.

Art. 2º O artigo 3º da Lei nº 5.070, de 7 de julho de 1966, passa a vigorar acrescido do seguinte parágrafo:

"Art. 3º .....

.....

Parágrafo único. Até 10 % (dez por cento) das transferências para o Tesouro Nacional poderão ser utilizados pelos órgãos da polícia judiciária de que trata o

artigo 4º da Lei nº 12.735, de 30 de novembro de 2012." (NR)

Art. 3º Esta lei entra em vigor um ano após sua publicação oficial.

JUSTIFICAÇÃO

A chamada Lei Azeredo, Lei nº 12.735/12, foi aprovada após longa tramitação no Congresso Nacional, na esteira do caso do vazamento das fotos da atriz Carolina Dieckmann, que por sua vez resultaram na aprovação da Lei nº 12.737/12. A Lei Azeredo, na verdade, é o resultado da tramitação do PL 84/99, do Deputado Luiz Piauhylino, que dispunha sobre diversos crimes na área de informática. A Lei resultante foi bastante simplificada com relação às propostas originais, tendo inclusive parte de seus dispositivos revogados. Apenas dois dispositivos restaram. O primeiro dispõe sobre práticas de discriminação racial nos meios de comunicação e o segundo determina que as polícias judiciárias estruturarão:

> "[Art. 4º]... setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado"

Em que pese essa disposição legal, os trabalhos da Comissão Parlamentar de Inquérito dos Crimes Cibernéticos evidenciaram a falta de estrutura dos Estados no combate a esses tipos de crimes. Tal como exposto por autoridades em Audiências Públicas na CPI, muitas unidades da federação não contam com delegacias especializadas ou setores específicos para cuidar com os diversos tipos de males acometidos mediante o uso de equipamentos eletrônicos, informáticos ou pela rede mundial de computadores.

Os diversos delegados ouvidos pelo colegiado foram unânimes em afirmar que a maior responsável pela desestruturação e pelo não

cumprimento da Lei 12.737/12 é a falta de recursos. Assim, a CPI dos Crimes Cibernéticos decidiu por propor o presente projeto de lei identificando uma fonte perene de recursos para essas atividades.

O Fistel – Fundo de Fiscalização das Telecomunicações - , instituído pela Lei nº 5.070/66, foi criado para, dentre outras finalidades, o "aperfeiçoamento da fiscalização dos serviços de telecomunicações existentes no País". Assim, entendemos que a estruturação das polícias judiciárias para o combate aos crimes cibernéticos guarda total aderência com o principal objetivo do fundo, quer seja a fiscalização no uso dos sistemas de telecomunicações, aí inserida, logicamente, a rede mundial de computadores.

Ademais, cabe salientar que o fundo arrecada aproximadamente R$ 2 bilhões anuais e já possui a previsão na Lei que o instituiu de que parte de seus recursos podem ser transferidos para o Tesouro Nacional. Como é amplamente noticiado na imprensa, os recursos do fundo são sistematicamente repassados ao Tesouro, principalmente para fins de superávit fiscal. O que se quer com este projeto é que apenas 10% dos recursos repassados ao caixa central da União possam ser destinados no combate a crimes cibernéticos. Como o projeto autoriza o uso de recursos e, portanto, não determina o uso peremptório dos mesmos, entendemos que todos os preceitos constitucionais e legais, como os constantes na Lei de Responsabilidade Fiscal, Lei Complementar nº 101/00, foram atendidos.

Assim, certos de que a aprovação desta Lei norteará as ações do Governo Federal no sentido de estruturar as polícias judiciárias estaduais no combate ao crime cibernético, contamos com o apoio dos nobres pares para a aprovação da matéria.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

PROJETO DE LEI QUE DISPÕE SOBRE O ACESSO DE AUTORIDADES ÀS INFORMAÇÕES RELATIVAS À INTERCEPTAÇÃO DE COMUNICAÇÕES DE DADOS DE USUÁRIO DE INTERNET.

PROJETO DE LEI Nº , DE 2016

(Da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país)

Dispõe sobre o acesso de autoridades às informações relativas à interceptação de comunicações de dados de usuário de internet.

O Congresso Nacional decreta:

Art. 1º Esta Lei disciplina o acesso de autoridades às informações relativas à interceptação de comunicações de dados de usuário de internet, para fins de investigação criminal e instrução processual penal.

§ 1º Para os fins desta Lei, considera-se:

I – provedor de conexão à internet, provedor de aplicação de internet, registro de conexão e registro de acesso a aplicações de internet: aqueles assim definidos pela Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil;

II – dados cadastrais: qualificação pessoal, filiação e endereço do usuário de internet.

§ 2º O acesso aos dados de que trata esta Lei aplica-se somente a partir da data da requisição de que trata o artigo 2º.

§ 3º O órgão regulador das telecomunicações regulamentará os critérios técnicos e operacionais para o fornecimento das informações de que trata o artigo 2º.

Art. 2º Delegado de polícia poderá requisitar, verbalmente ou por mensagem eletrônica, diretamente a provedor de conexão à internet e provedor de aplicação de internet, os dados cadastrais, de registro de conexão e de acesso a aplicações de internet de usuário de internet, apenas nos seguintes casos:

I – restrição da liberdade ou iminente risco para a vida de alguém;

II – desaparecimento de pessoa;

III – investigação criminal em que a comprovação da materialidade ou autoria de infração penal em andamento dependa do imediato conhecimento da localização do infrator ou coisa afim.

§ 1º No ato de requisição deverá ser informada a natureza do fato investigado e o número do inquérito policial ou, nos casos de urgência, do registro de ocorrência policial.

§ 2º A requisitada colocará à disposição do delegado de polícia as informações solicitadas, no prazo de duas horas.

§ 3º Cabe à corregedoria de polícia indicar às entidades de que trata o *caput* quais delegados de polícia habilitados para solicitar verbalmente e receber as informações de que trata o *caput*, com os respectivos meios de contato, bem como estabelecer as normas de procedimento para controle das requisições.

§ 4º As entidades de que trata o *caput* deverão manter canais técnicos para recebimento de requisições verbais e fornecimento das informações aos delegados de polícia habilitados.

§ 5º As entidades de que trata o *caput* que tiverem sido solicitadas as informações de que trata o *caput* encaminharão, quinzenalmente, à corregedoria de polícia e ao Ministério Público, extrato das requisições recebidas, indicando a pessoa objeto de solicitação, seus dados cadastrais, nome do delegado de polícia requisitante, número do inquérito policial ou da ocorrência policial e, se for o caso, a razão do não atendimento.

Art. 3º A requisição formulada verbalmente ou por mensagem eletrônica, pelo delegado de polícia deverá ser por ele comunicada à respectiva corregedoria e ao juiz em vinte e quatro horas, por escrito, instruído com cópia da portaria de instauração do inquérito policial ou do auto de prisão em flagrante, contendo:

I – descrição precisa dos fatos investigados;

II – indicação da existência de indícios suficientes da prática do crime objeto da investigação;

III – qualificação do investigado ou esclarecimentos pelos quais se possa 35dentifica-lo, salvo impossibilidade manifesta devidamente justificada;

IV – demonstração de serem os dados solicitados estritamente necessários e o tempo decorrido para resposta à requisição;

V – designação do código de identificação do sistema de comunicação e de sua relação com os fatos investigados.

§ 1º Na hipótese dos incisos I e II do artigo 2º, as informações prestadas pelo delegado de polícia resumir-se-ão àquelas conhecidas.

§ 2º Se a diligência ultrapassar o período definido no *caput*, a comunicação ao juiz deverá ser feita em até vinte e quatro horas de seu término.

§ 3º Para fins do disposto no artigo 10, inciso III, o juiz, antes de homologar a requisição, dará vista ao Ministério Público, da documentação encaminhada.

§ 4º Nos casos dos incisos I e II do artigo 2º, as entidades de que trata o *caput* daquele artigo deverão informar ao delegado de polícia que solicitou os dados o endereço do usuário para que este seja oficialmente comunicado do ocorrido pelo delegado e pela entidade, no prazo máximo de sete dias, devendo constar do comunicado as mesmas informações a que faz menção este artigo.

Art. 4º O juiz poderá determinar, no interesse da persecução criminal, o fornecimento, pelas entidades requisitadas nos termos do *caput* do artigo 2º, do histórico de comunicação de dados do usuário.

§ 1º O pedido será formulado, durante a investigação criminal, mediante representação do delegado de polícia ou, durante a instrução processual, mediante requerimento do Ministério Público.

§ 2º O pedido deve conter dados que indiquem a relevância da medida à prova do fato ou da autoria, o período considerado e a identificação do usuário de internet.

§ 3º Na hipótese de representação do delegado de polícia, o Ministério Público será ouvido no prazo de quarenta e oito horas.

§ 4º O pedido será distribuído e autuado em separado, sob segredo de justiça, devendo o juiz decidir no prazo de setenta e duas horas.

Art. 5º Contra decisão que indeferir o pedido dos dados de comunicação caberá recurso em sentido estrito do Ministério Público e pedido de reconsideração do delegado de polícia.

§ 1º O recurso em sentido estrito e o pedido de reconsideração tramitarão em segredo de justiça e serão processados sem a oitiva do investigado ou acusado, a fim de resguardar a eficácia da investigação.

§ 2º O mandado judicial será expedido no número de vias indicado pela autoridade de investigação e poderá ser encaminhado por qualquer meio idôneo, inclusive o eletrônico ou similar, desde que comprovada sua autenticidade.

Art. 6º As informações requisitadas deverão ser fornecidas pelas entidades de que trata o *caput* do artigo 2º por período não superior a quinze dias e:

I – em se tratando das situações previstas no art. 2º, de forma a obter a localização do usuário em tempo real;

II – em se tratando de histórico de comunicação de dados do usuário, em periodicidade não inferior a vinte e quatro horas, se outra superior não for assinada pela autoridade requisitante.

Parágrafo único. Dispensada a prestação das informações, disso noticiará ao juiz a autoridade requisitante e, sendo esta o delegado de polícia, também à corregedoria.

Art. 7º Os funcionários das entidades de que trata o *caput* do artigo 2º e os servidores envolvidos com a investigação que tiverem acesso às informações requisitadas deverão ser identificados e autenticados por mecanismo a ser regulamentado pelo órgão regulador das telecomunicações, mantendo sob sigilo a identidade dos funcionários das entidades.

Art. 8º Para os procedimentos de obtenção dos dados de comunicação de que trata o *caput* do artigo 2º, o delegado de polícia poderá requisitar serviços e técnicos especializados às entidades requisitadas e de pessoas físicas e jurídicas por elas contratadas, em caráter não oneroso.

Parágrafo único. Os órgãos de segurança deverão viabilizar, a suas expensas, o acesso às informações de que trata esta Lei, no âmbito de suas instalações.

Art. 9º As entidades de que trata o *caput* do artigo 2º manterão, para os efeitos desta lei, pelo prazo de um ano, os registros dos dados fornecidos aos delegados de polícia em virtude das requisições de que trata esta Lei.

Parágrafo único. Os registros deverão ser mantidos pelas entidades em ambiente controlado e de segurança, e a responsabilidade por sua guarda não poderá ser transferida a terceiros.

Art. 10. O descumprimento injustificado do disposto nesta lei sujeitará o infrator às seguintes penalidades, por infração, sem prejuízo de responsabilização civil e criminal, assegurado o devido processo administrativo:

I – não prestar informação solicitada, prestá-la parcialmente ou sustar a prestação antes de a autoridade requisitante dispensá-la: multa de R$ 50.000,00 (cinquenta mil reais);

II – descumprir prazo, prestar informação não autorizada ou prestar informação a terceiro não legitimado: multa de R$ 20.000,00 (vinte mil reais);

III – requisitar informação de comunicações de dados de usuário indevidamente: multa de R$ 10.000,00 (dez mil reais).

§ 1º As penalidades previstas no *caput* serão aplicadas pelo dobro da última aplicada, no caso de reincidência.

§ 2º As penalidades previstas nos incisos I e II serão aplicadas pelo órgão regulador das telecomunicações, mediante comunicação da infração pelo juiz ou pela corregedoria de polícia, e os valores arrecadados reverterão em favor do Fundo de Fiscalização das Telecomunicações (Fistel), de que trata a Lei nº 5.070, de 7 de julho de 1966.

§ 3º A penalidade prevista no inciso III será aplicada pelo juiz e reverterá a fundo de reequipamento das forças de segurança pública, ou equivalente, e na falta deste, ao Fundo de Fiscalização das Telecomunicações (Fistel).

§ 4º Para efeito da aferição do prazo previsto no inciso II, será levada em consideração a comunicação formal por escrito, ou por meio eletrônico, nos termos estabelecidos pela regulamentação do órgão regulador das telecomunicações.

§ 5º A requisição indevida de comunicações de dados, a prestação de informação não autorizada e a prestação de informação a terceiro não legitimado são consideradas violação de telecomunicações e de comunicação telefônica, e os infratores estarão sujeitos, também, às penalidades previstas no art. 58 do Código Brasileiro de Telecomunicações, instituído pela Lei nº 4.117, de 27 de agosto de 1962, e no art. 151 do Código Penal.

Art. 11. As pesquisas para o desenvolvimento de métodos ou soluções técnicas para a obtenção das informações de comunicações de dados de que trata esta Lei poderão ser financiadas com recursos do Fundo para o Desenvolvimento Tecnológico das Telecomunicações – FUNTTEL, instituído pela Lei nº 10.052, de 28 de novembro de 2000.

Art. 12. Esta lei entra em vigor após noventa dias de sua publicação oficial.

JUSTIFICAÇÃO

A Comissão Parlamentar de Inquérito dos Crimes Cibernéticos se debruçou no segundo semestre de 2015 sobre variados aspectos da internet e as diversas modalidades de crimes praticados na grande rede. Para a consecução dos trabalhos a CPI foi dividida em quatro Sub-Relatorias: Instituições Financeiras e Comércio Virtual, Crimes Contra a Criança e o Adolescente, Violações a Direitos Fundamentais e Crimes Contra a Honra, e; Segurança Cibernética no Brasil. Em diversas Audiências Públicas, foram elencados diversos tipos de crimes praticados com o auxílio da internet. Dentre muitos, destacamos: pedofilia, extorsão, fraudes bancárias e invasão de sítios. Em muitos desses casos, as vítimas correm risco iminente de vida. Quer seja pelo sequestro da pessoa ou por vítima de assédio virtual. A sofisticação das práticas virtuais, em muitos casos passa não só pela extorsão de valores, mas por práticas muito mais danosas, como a vingança pornô ou o estupro virtual, onde a vítima se sujeita a satisfazer pedidos sexuais virtuais, apenas para citar alguns exemplos escabrosos. Em muitas das vezes em que esses crimes são praticados, as vítimas pensam em se infligir mal físico e até em cometer suicídio. Não raramente precisam mudar de endereço, cidade, trocar de escola ou de emprego.

No mundo virtual, as consequências da prática de crimes virtuais contra a pessoa são diretamente proporcionais à duração da prática delitiva. Nesse sentido, o dano cresce de maneira exponencial, como no caso de vídeos ou fotografias que viralizam nas redes sociais. Por isso, a ação das autoridades de investigação deve se dar de maneira célere.

No entanto, conforme relatado por diversos delegados, autoridades do Ministério Público e entidades tais como de defesa da criança e do adolescente, a sistemática atual para realização da quebra do sigilo de comunicações de usuário de internet é extremamente morosa. Desafortunadamente, com a entrada em vigência do Marco Civil da Internet (Lei nº 12.965/14), a obtenção dos dados do usuário, quer seja os dados cadastrais, a identificação de um usuário de redes sociais praticante de

bullying, ou ainda o endereço IP de onde partiu um golpe bancário, foi extremamente dificultado. Pelo procedimento atual, a vítima notifica a autoridade policial, esta solicita a um juiz a quebra de sigilo para identificar o usuário de provedor de conexão, e, identificado o provedor, é necessário novo pedido judicial para aceder aos dados para aplicação de internet. Ademais, pela sistemática atual, para cada aplicação de internet é necessário um pedido distinto. Essa dupla decisão judicial, conforme relatado à CPI, e amplamente divulgado pela imprensa em casos notórios, dura vários dias, semanas até. Em muitas vezes, esse tempo pode custar a vida e, em vários deles, de crianças.

Por esses motivos, a CPI de Crimes Cibernéticos resolveu apoiar a sistemática proposta no Substitutivo aprovado ao PL 6.726/10, na CCTCI, apresentado pela relatora na Comissão, Deputada Margarida Salomão. A iniciativa, que trata somente da quebra do sigilo da localização de telefones celulares, inverteu essa lógica e propõe que a autoridade judicial tenha acesso imediato à localização e aos dados do assinante em casos de iminente risco à vida. Como forma de coibir abusos, o Substitutivo também determina que a autoridade deverá notificar o juiz que deverá analisar o caso e aplicar penas cabíveis, caso necessário. É exatamente essa a metodologia que estamos propondo. Na verdade, tomamos a liberdade de utilizar-nos da mesma estrutura do mencionado Substitutivo ao PL 6.726/10, apenas adaptando-o para permitir a obtenção não apenas dos dados de localização, mas dos dados cadastrais, de conexão e de navegação em qualquer aplicativo. Porém, assim como no Substitutivo mencionado, apenas para casos de iminente risco à vida, como sequestros relâmpagos ou práticas de *bullying* contra menores ou outros atentados à pessoa humana.

Entendemos que os dispositivos de coerção ao mau uso da futura Lei, previstos neste projeto, afastarão sobremaneira a possibilidade de que o instrumento seja utilizado para ferir as garantias constitucionais à privacidade, à intimidade e à vida privada. No entanto, a celeridade que a nova sistemática trará possui o potencial real de salvar vidas.

Pelos motivos expostos, contamos com o apoio dos nobres pares.

Sala das Sessões, em 30 de março de 2016.

CPI – Crimes Cibernéticos

PROJETO DE LEI PARA DETERMINAR QUE FILIAL, SUCURSAL, ESCRITÓRIO OU ESTABELECIMENTO SITUADO NO PAÍS RESPONDE SOLIDARIAMENTE PELO FORNECIMENTO DE DADOS REQUISITADOS JUDICIALMENTE DE EMPRESAS COM ATUAÇÃO NO PAÍS E CUJA MATRIZ ESTEJA SITUADA NO EXTERIOR.

PROJETO DE LEI Nº , DE 2016

(Da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país)

Altera o Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, determinando que filial, sucursal, escritório ou estabelecimento situado no País responda solidariamente pelo fornecimento de dados requisitados judicialmente de empresas com atuação no país e cuja matriz esteja situada no exterior.

O Congresso Nacional decreta:

Art. 1º Esta Lei modifica o Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, determinando que filial, sucursal, escritório ou estabelecimento situado no País responda solidariamente pelo fornecimento de dados requisitados judicialmente de empresas com atuação no país e cuja matriz esteja situada no exterior.

Art. 2º O art. 22 da Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet, passa a vigorar acrescido do seguinte § 2º:

"Art. 22 .....

.....

§ 2º No caso em que as operações de que trata o artigo 11 sejam realizadas no exterior, desde que o serviço seja ofertado ao

público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil, responde solidariamente pelo fornecimento sua filial, sucursal, escritório ou estabelecimento situado no País.” (NR)

Art. 3º Esta lei entra em vigor na data da sua publicação.

JUSTIFICAÇÃO

De acordo com autoridades policiais ouvidas pela CPI, algumas empresas da internet impõem obstáculos ao cumprimento de decisões judiciais, alegando que os conteúdos são armazenados no exterior e que não possuem condições técnicas para proceder às remoções. Nosso projeto deixa claro que, caso a empresa seja integrante do mesmo grupo comercial ou que aquela possua representação no país, a obrigação e as penalidades pelo não atendimento de eventuais decisões recairá sobre a personalidade jurídica que a representa no País.

Estamos certos de que com essa alteração ao Marco Civil da Internet, as dificuldades pelas quais estão passando as autoridades de investigação, o Poder Judiciário e, principalmente, as vítimas de crimes cibernéticos serão mitigadas.

Pelos motivos elencados, os membros da CPI dos Crimes Cibernéticos solicitam a aprovação do presente Projeto de Lei.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

PROPÕE QUE A COMISSÃO DE CIÊNCIA E TECNOLOGIA, COMUNICAÇÃO E INFORMÁTICA, FISCALIZE, COM AUXÍLIO DO TRIBUNAL DE CONTAS DA UNIÃO – TCU, AS AÇÕES DE ACOMPANHAMENTO E CONTROLE DA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL ACERCA DA CORRETA IMPLEMENTAÇÃO E UTILIZAÇÃO DOS CADASTROS DE USUÁRIOS DE TELEFONES PRÉ-PAGOS.

PROPOSTA DE FISCALIZAÇÃO E CONTROLE Nº , DE 2016

(Da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país)

Propõe que a Comissão de Ciência e Tecnologia, Comunicação e Informática, fiscalize, com auxílio do Tribunal de Contas da União – TCU, as ações de acompanhamento e controle da Agência Nacional de Telecomunicações – Anatel acerca da correta implementação e utilização dos cadastros de usuários de telefones pré-pagos.

Senhor Presidente:

Com base no art. 100, §1º, combinado com os arts. 60, inciso II, e 61 do Regimento Interno, proponho a V. Exª que, ouvido o Plenário desta Comissão, se digne a adotar as medidas necessárias para realizar, com auxílio do Tribunal de Contas da União – TCU, ato de fiscalização na Anatel – Agência Nacional de Telecomunicações – com respeito ações de acompanhamento e controle daquela Agência acerca da correta implementação e utilização dos cadastros de usuários de telefones pré-pagos, para elucidar as seguintes questões:

1. Verificar quais foram os procedimentos de fiscalização realizados pela Agência com o intuito de verificar o total cumprimento do disposto na Lei nº 10.703, de 2003, que *"Dispõe sobre o cadastramento de usuários de telefones celulares pré-*

pagos e dá outras providências" e quais os resultados dessas fiscalizações;

2. Verificar quantas e quais foram as multas aplicadas pela Anatel, em consonância com a citada lei, destacando os agravantes de natureza, gravidade e prejuízo previstos no artigo 5º daquele diploma legal;

3. Verificar a realização da campanha institucional prevista no artigo 6º da Lei nº 10.703, de 2003, bem como a avaliação dos objetivos alcançados e ações decorrentes desta avaliação;

4. Verificar quantos foram os processos de utilização dos dados cadastrais dos usuários de telefones pré-pagos, por autoridades autorizadas, por unidade da federação;

5. Verificar se a fiscalização da Anatel junto às prestadoras de serviços de telefonia móvel afere a veracidade das informações prestadas pelos usuários dos serviços pré-pagos, ainda que por amostragem, e os procedimentos de coleta das informações definidas na legislação.

JUSTIFICAÇÃO

Há muito a sociedade brasileira tem-se deparado com a prática de crimes que são perpetrados por meio de ou se apoiam nos serviços de telecomunicações, especialmente os serviços de telefonia celular. Com o avanço da tecnologia e a escalada de utilização de *smartphones*, o cenário vem se agravando a largos passos.

O Congresso Nacional aprovou, ainda no ano de 2003, a Lei nº 10.703, com o objetivo de cadastrar todos os usuários de telefones

móveis no País, de sorte a que eventuais utilizações inadequadas destes aparelhos pudessem ser atribuídas, ou questionadas, a seus proprietários. De acordo com a legislação aprovada, os cadastros devem ser realizados pelas prestadoras dos serviços e fiscalizados pela Anatel.

Com a massificação dos serviços pré-pagos, que correspondem a cerca de 80% de toda a rede de telefonia celular no Brasil, os procedimentos de cadastramento foram sendo simplificados, com a possibilidade, inclusive, de serem realizados por meio de *call centers*. Com este cenário, o objetivo da Lei nº 10.703, de 2003, vem sendo comprometido a cada dia, uma vez que nem sempre a veracidade das informações coletadas pode ser atestada.

Este ambiente de pouca confiabilidade tem sido explorado, em escala crescente, por criminosos que informam falsos dados e têm seus aparelhos habilitados sem nenhuma dificuldade. Não é à toa que os dados da criminalidade com a utilização de celulares pré-pagos tem sido alarmantes.

Outra questão que facilita a ação criminosa é a conjunção da utilização de terminais pré-pagos em *smartphones* com acesso à internet gratuita por meio de *wifi*. Neste tipo de utilização, o criminoso se esconde duplamente, porque muitos acessos gratuitos não exigem qualquer tipo de cadastro de seus utilizadores.

Este é, certamente, um campo em que esta Comissão Parlamentar de Inquérito precisa se debruçar. Por esta razão, apresentamos a presente Proposta de Fiscalização e Controle para que, com o apoio do Tribunal de Contas da União, possamos verificar o que tem sido feito no órgão público a quem compete a fiscalização das telecomunicações, ou seja, a Anatel. A partir dos dados da fiscalização proposta, poderemos direcionar nossas políticas públicas para atingirmos de maneira mais eficaz os objetivos de coibir a prática de ações criminosas que são conduzidas com a utilização das tecnologias de comunicação e de informação.

Dessa forma, considerando a importância de garantirmos a correta utilização dos serviços de telecomunicações para a fruição de ligações e conexões seguras e livres da criminalidade, insto os nobres Pares para a aprovação desta Proposta de Fiscalização e Controle.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

INDICAÇÃO AO PODER EXECUTIVO, SUGERINDO A ADOÇÃO DE MEDIDAS PARA MELHORAR A SEGURANÇA DA INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO DA ADMINISTRAÇÃO PÚBLICA E OUTRAS PROVIDÊNCIAS.

REQUERIMENTO Nº , DE 2016

(Da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país)

Requer o envio de Indicação ao Poder Executivo, sugerindo a adoção de medidas para melhorar a segurança da infraestrutura de tecnologia da informação da Administração Pública e outras providências.

Senhor Presidente:

Nos termos do art. 113, inciso I e § 1º, do Regimento Interno da Câmara dos Deputados, requeiro a V. Exª. seja encaminhada ao Poder Executivo a Indicação em anexo, sugerindo a adoção de medidas para melhorar a segurança da infraestrutura de tecnologia da informação da Administração Pública e outras providências.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

INDICAÇÃO Nº , DE 2016

(Da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país)

Sugere a adoção de medidas para melhorar a segurança da infraestrutura de tecnologia da informação da Administração Pública e outras providências.

Excelentíssimo Senhor Ministro-Chefe da Secretaria de Governo da Presidência da República:

A Comissão Parlamentar de Inquérito dos Crimes Cibernéticos foi criada em 17/07/15, para investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país, tendo em vista (i) que a Polícia Federal realizou em 2014 a operação batizada de IB2K para desarticular uma quadrilha suspeita de desviar pela Internet mais de R$ 2 milhões de correntistas de vários bancos, quadrilha esta que usava parte do dinheiro desviado para comprar armas e drogas; (ii) o último relatório da Central Nacional de Denúncias de Crimes Cibernéticos que aponta um crescimento, entre 2013 e 2014, de 192,93% nas denúncias envolvendo páginas na Internet suspeitas de tráfico de pessoas, e (iii) os gastos de US$ 15,3 bilhões com crimes cibernéticos no Brasil em 2010.

Os trabalhos da CPI foram divididos em quatro Sub-Relatorias, uma delas a de Segurança Cibernética no Brasil, a cargo do Sub-Relator Deputado Rodrigo Martins. Em sua análise, essa Sub-Relatoria considerou que os esforços empreendidos pelo extinto Gabinete de Segurança

Institucional no ano de 2015 foram extremamente profícuos e contribuíram sobremaneira para a elevação da segurança cibernética da infraestrutura de tecnologia da informação (TI) do País. Ademais, a Sub-Relatoria analisou as recomendações contidas nos Acórdãos 3.051 e 3.117, ambos de 2014, do Tribunal de Contas da União, em que o referido órgão manifesta sua preocupação por falhas no planejamento, análise de risco e gestão da segurança da informação, dentre outros problemas elencados.

Além da análise desses documentos oficiais, esta CPI ouviu em diversas Audiências Públicas, para tratar sobre o tema da segurança na internet, a posição de especialistas, autoridades do Poder Executivo e do Poder Judiciário, assim como de membros do Ministério Público Federal e Estaduais. Todos foram unânimes em ressaltar que a gestão da segurança dos recursos de TI precisa melhorar e precisa de ações mais incisivas de governo. Por esses motivos e tendo se debruçado sobre a matéria, este colegiado vem oferecer a presente Indicação sugerindo a aplicação pela Administração Pública Federal, e pelos fundos especiais, autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, das seguintes medidas:

i) **Elaboração de Guia de Boas Práticas em Segurança da Informação a ser adotado de maneira peremptória pelos órgãos da Administração Pública Federal;**

ii) **Realização de auditoria em sua infraestrutura pública de TI, incluindo equipamentos (hardware), programas (software) e sistemas desenvolvidos, para fins de verificação da existência de *backdoors* e outras fragilidades em termos de segurança cibernética e de soberania nacional;**

iii) **Celebração de instrumentos de cooperação técnica entre autoridades públicas de segurança**

cibernética e entidades privadas, em especial com aquelas ligadas ao setor financeiro e bancário.

Certos de contar com a compreensão e o engajamento do Senhor Ministro-Chefe para dar consecução às medidas, esperamos vê-las implementadas, para que todo o ambiente cibernético brasileiro seja provido de maior segurança, evitando a prática de crimes.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

INDICAÇÃO AO MINISTÉRIO DA JUSTIÇA, SUGERINDO O ESTABELECIMENTO DE CONVÊNIOS ENTRE AS POLÍCIAS FEDERAL E CIVIS DOS ESTADOS PARA APLICAÇÃO DE RECEITAS DO FISTEL, TRANSFERIDAS PARA O TESOURO NACIONAL, NO FINANCIAMENTO DAS ESTRUTURAS DE COMBATE A CRIMES CIBERNÉTICOS.

REQUERIMENTO

(Da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país)

Requer o envio de Indicação ao Ministério da Justiça, sugerindo o estabelecimento de convênios entre as polícias federal e civis dos estados para aplicação de receitas do Fistel, transferidas para o Tesouro Nacional, no financiamento das estruturas de combate a crimes cibernéticos.

Senhor Presidente:

Nos termos do art. 113, inciso I e § 1º, do Regimento Interno da Câmara dos Deputados, requeiro a V. Exª. seja encaminhada ao Ministério da Justiça a Indicação em anexo, sugerindo o estabelecimento de convênios com as polícias federal e civis dos estados para aplicação de receitas do Fistel (Fundo de Fiscalização das Telecomunicações), instituído pela Lei nº 5.070/66, transferidas para o Tesouro Nacional no financiamento das estruturas de combate a crimes cibernéticos.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

INDICAÇÃO Nº , DE 2016

(Da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país)

Sugere o estabelecimento de convênios entre as polícias federal e civis dos estados para aplicação de receitas do Fistel, transferidas para o Tesouro Nacional, no financiamento das estruturas de combate a crimes cibernéticos.

Excelentíssimo Senhor Ministro de Estado da Justiça:

A Comissão Parlamentar de Inquérito dos Crimes Cibernéticos foi criada em 17/07/15, para investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país, tendo em vista (i) que a Polícia Federal realizou em 2014 a operação batizada de IB2K para desarticular uma quadrilha suspeita de desviar pela Internet mais de R$ 2 milhões de correntistas de vários bancos, quadrilha esta que usava parte do dinheiro desviado para comprar armas e drogas; (ii) o último relatório da Central Nacional de Denúncias de Crimes Cibernéticos que aponta um crescimento, entre 2013 e 2014, de 192,93% nas denúncias envolvendo páginas na Internet suspeitas de tráfico de pessoas, e (iii) os gastos de US$ 15,3 bilhões com crimes cibernéticos no Brasil em 2010.

Os trabalhos da CPI foram divididos em quatro Sub-Relatorias, uma delas a de Segurança Cibernética no Brasil, a cargo do Sub-Relator Deputado Rodrigo Martins. Em sua análise, essa Sub-Relatoria considerou que o combate aos crimes digitais possui maiores chances de sucesso quando as polícias judiciárias possuem equipes especializadas para tratar do assunto. No entanto, as investigações demonstraram a falta de estruturas constituídas para esse fim na grande maioria das polícias estaduais. Ademais, ficou evidente a falta de material humano, de equipamentos e de infraestrutura. A razão mais óbvia é a reconhecida falta de recursos perenes para o setor.

Por esses motivos, a CPI vem oferecer esta Indicação, sugerindo ao Ministério da Justiça o estabelecimento de convênios entre as polícias federal e civis dos estados para aplicação de parte das receitas do Fistel, transferidas para o Tesouro Nacional, no financiamento das estruturas de combate a crimes digitais, notadamente as delegacias especializadas em crimes cibernéticos.

É sabido que os recursos arrecadados pelo Fistel (Fundo de Fiscalização das Telecomunicações), instituído pela Lei nº 5.070/66, e não repassados à Anatel perfazem a maioria das receitas do fundo e que tais recursos tem sido sistematicamente derivados para o Tesouro para fortalecimento de caixa e combate ao déficit fiscal. Entretanto, acreditamos que, em se tratando de fundos arrecadados em função do poder de polícia do Estado, uma parte desses recursos contingenciados poderia voltar ao sistema na forma indicada, isto é, fortalecendo as polícias judiciárias no combate ao mau uso das telecomunicações. Ressaltamos que o crime cibernético no País drena recursos da ordem de R$ 1 bilhão anuais, segundo estimativas, portanto, o retorno de parcela do Fistel para a estrutura de combate ao crime tem o potencial de diminuir essas perdas, grande parte das quais se concentra em entidades públicas. Assim, o descontingenciamento de recursos voltaria ao caixa da Administração na forma de maior eficiência em suas instituições.

Certos de contar com a compreensão e o

comprometimento do Senhor Ministro para a formação dos convênios, acreditamos que o fortalecimento das delegacias especializadas servirá sobremaneira para a diminuição de crimes cibernéticos em território nacional.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

INDICAÇÃO À AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, SUGERINDO A ADOÇÃO DAS MEDIDAS NECESSÁRIAS PARA A IMPLANTAÇÃO DO IPV6 NO PAÍS.

REQUERIMENTO Nº , DE 2016

(Da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país)

Requer o envio de Indicação ao Sr. Ministro de Estado das Comunicações sugerindo à Agência Nacional de Telecomunicações a adoção das medidas necessárias para a implantação do IPV6 no país.

Senhor Presidente:

Nos termos do art. 113, inciso I e § 1º, do Regimento Interno da Câmara dos Deputados, requeiro a V. Exª. seja encaminhado ao Sr. Ministro de Estado das Comunicações Indicação para que a Agência Nacional de Telecomunicações adote as medidas necessárias para a implantação do IPV6 no país.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

INDICAÇÃO Nº , DE 2016

(Da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país)

Sugere a adoção das medidas necessárias para a implantação do IPV6 no país.

Excelentíssimo Senhor Ministro das Comunicações:

A Comissão Parlamentar de Inquérito dos Crimes Cibernéticos foi criada em 17/07/15, para investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país, tendo em vista (i) que a Polícia Federal realizou em 2014 a operação batizada de IB2K para desarticular uma quadrilha suspeita de desviar pela Internet mais de R$ 2 milhões de correntistas de vários bancos, quadrilha esta que usava parte do dinheiro desviado para comprar armas e drogas; (ii) o último relatório da Central Nacional de Denúncias de Crimes Cibernéticos que aponta um crescimento, entre 2013 e 2014, de 192,93% nas denúncias envolvendo páginas na Internet suspeitas de tráfico de pessoas, e (iii) os gastos de US$ 15,3 bilhões com crimes cibernéticos no Brasil em 2010.

Os trabalhos da CPI foram divididos em quatro Sub-Relatorias, uma delas a de Segurança Cibernética no Brasil, a cargo do Sub-

Relator Deputado Rodrigo Martins. Em sua análise, essa Sub-Relatoria considerou que a adoção do padrão IPv6 e seu uso por parte dos provedores de acesso a internet é de fundamental importância no combate aos crimes cibernéticos.

No protocolo atualmente em uso, o IPv4, existe uma escassez severa de números IP para identificação dos usuários da internet. Essa limitação é consequência da própria definição do IPV4 e da enorme expansão verificadas na última década no número de dispositivos conectados à rede mundial de computadores. Algumas tecnologias, como a NAT 44, que compartilham o mesmo número IP entre vários usuários, são capazes de contornar essa limitação, sendo por isso amplamente empregadas no país. Entretanto, esse compartilhamento do mesmo número IP entre diversos internautas dificulta sensivelmente o rastreamento dos registros de acesso até o seu usuário final. Assim, a identificação do internauta porventura praticante de determinado crime na internet se torna bastante desafiadora, o que aumenta a impunidade e estimula a criminalidade.

A nova versão do protocolo de endereçamento resolve definitivamente o problema da escassez de endereços na internet, o que permitirá aos provedores atribuir um identificador único para cada usuário, sem necessidade de compartilhamento. Desta forma, o rastreamento dos registros de acesso de qualquer investigado será mais simples, facilitando sobremaneira o trabalho da autoridade policial no combate aos crimes cibernéticos.

Por esses motivos, a CPI vem oferecer esta Indicação, sugerindo à Anatel, por intermédio do Ministério das Comunicações, que adote as medidas necessárias para viabilizar a implantação do IPV6 no país da forma mais célere possível.

Certos de contar com a compreensão e o engajamento do Senhor Ministro para dar consecução às medidas, esperamos vê-las implementadas, para que todo o ambiente cibernético brasileiro seja provido de maior segurança, evitando a prática de crimes.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos