CÂMARA DOS DEPUTADOS

CPI – CRIMES CIBERNÉTICOS

COMISSÃO PARLAMENTAR DE INQUÉRITO DESTINADA A INVESTIGAR A PRÁTICA DE CRIMES CIBERNÉTICOS E SEUS EFEITOS DELETÉRIOS PERANTE A ECONOMIA E A SOCIEDADE NESTE PAÍS.

RELATÓRIO FINAL

Presidente: Deputada Mariana Carvalho

Relator: Deputado Esperidião Amin

Sub-Relatores: Deputados Sandro Alex, Rafael Motta,

Daniel Coelho e Rodrigo Martins

Brasília, _____ de _____

SUMÁRIO

PARTE I – TRABALHOS DA COMISSÃO PARLAMENTAR DE INQUÉRITO

1 – DA CRIAÇÃO DA CPI

Esta Comissão Parlamentar de Inquérito foi criada por Ato da Presidência da Câmara dos Deputados, de 17 de julho de 2015, com o seguinte teor:

ATO DA PRESIDÊNCIA

Satisfeitos os requisitos do art. 35, caput, e § 4º, do Regimento Interno, para o Requerimento de Instituição de CPI nº 10, de 2015, do Sr. Sibá Machado e outros, esta Presidência dá conhecimento ao Plenário da criação da **Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos** e seus efeitos deletérios perante a econômica e a sociedade neste país, tendo em vista: (i) que a Polícia Federal realizou em 2014 a operação IB2K para desarticular uma quadrilha suspeita de desviar pela Internet mais de R$ 2 milhões de correntistas de vários bancos, quadrilha que usava parte do dinheiro desviado para comprar armas e drogas; (ii) o último relatório da Central 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.

A Comissão será composta de 26 (vinte e seis) membros titulares e de igual número de suplentes, mais um titular e um suplente, atendendo ao rodízio entre as bancadas não contempladas, designados de acordo com os §§ 1º e 2º do art. 33, combinado com o § 5º do art. 35, todos do Regimento Interno.

Brasília, 17 de julho de 2015

EDUARDO CUNHA
Presidente da Câmara dos Deputados

O Requerimento para a criação desta CPI (RCP nº 10/2015),

de autoria do Deputado Sibá Machado e outros, foi formulado nos seguintes termos:

REQUERIMENTO Nº 10, DE 2015.
(Do Sr. Sibá Machado - PT/AC)

Requeremos a criação de Comissão Parlamentar de Inquérito, com a finalidade de 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.

Senhor Presidente:

Requeremos a Vossa Excelência, nos termos do § 3o do art. 58 da Constituição Federal e dos arts. 35, 36 e 37 do Regimento Interno da Câmara dos Deputados, a criação de Comissão Parlamentar de Inquérito, composta por 25 membros titulares e igual número de suplentes, obedecendo-se o princípio da proporcionalidade partidária, para investigar, no prazo de até 120 dias, a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste paiís.

As despesas decorrentes do funcionamento da Comissão de que trata este requerimento correrão à conta dos recursos orçamentários da Câmara dos Deputados.

Os recursos administrativos e o assessoramento necessários ao funcionamento da Comissão serão providos pelo Departamento de Comissões e pela Consultoria Legislativa, respectivamente.

JUSTIFICATIVA

Faz-se necessária a instalação da Comissão Parlamentar de Inquérito proposta neste requerimento, com a possibilidade de ser ampliada em vista de fatos novos conexos aos aqui mencionados.

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, o número de fraudes na Internet no Brasil aumentou 6.513% entre 2004 e 2009.

A SaferNet Brasil, associação civil de direito privado, especializada no enfrentamento aos crimes e violações aos Direitos Humanos na Internet, nos últimos 09 (nove) anos recebeu e processou 3.606.419 denúncias anônimas, por meio da Central Nacional de Denúncias de Crimes Cibernéticos, envolvendo 585.778 páginas (URLs) distintas – das quais 163.269 foram removidas – conectados à Internet através de 41.354 números IPs distintos.

Entre os 1.225 pedidos de ajuda e orientação psicológica atendidos pela SaferNet, em 2014, 222 foram vazamentos de fotos íntimas, situação chamada de sexting. Isso significa um aumento de 119,8% em relação a 2013. Mais da metade das vítimas tinha até 25 anos, das quais 25% tinham entre 12 e 17 anos.3

De acordo com a SaferNet, houve crescimento de 192,93% nas denúncias envolvendo páginas suspeitas de tráfico de pessoas na comparação entre 2014 e 2013. ‘O objetivo era recrutar pessoas, principalmente mulheres, inclusive adolescentes, para a prostituição em cidades-sedes da Copa do Mundo’, segundo Thiago Tavares, representante da entidade.

A Central Nacional de Denúncias de Crimes Cibernéticos recebe uma média de 2.500 denúncias por dia envolvendo páginas na Internet contendo evidências dos crimes de Pornografia Infantil ou Pedofilia, Racismo, Neonazismo, Intolerância Religiosa, Apologia e Incitação a crimes contra a vida, Homofobia e maus tratos contra os animais.

Ademais, diversas outas atividades no mercado negro da Internet são realizadas, em prejuízo considerável para o bem-estar social. Os ataques cibernéticos ocorrem por

diversas formas, incluindo:

- envio de e-mails de phishing para o maior número possível de endereços de e-mail.
- criação de sites maliciosos na Web que parecem ser o mais legítimo possível.
- agressores amadores, conhecidos como 'script kiddies', que coletam computadores das vítimas (chamados de 'root'), que podem ser usados para hospedar um site de phishing ou um retransmissor de spam. Em alguns casos, os exploradores violam diretamente os bancos de dados de cartões de crédito, não necessitando da etapa de phishing.
- retirada de fundos de um cartão de crédito ou de uma conta bancária comprometidos.
- recebimento de mercadorias compradas com informações roubadas de cartões de créditos em um local de entrega que não pode ser rastreado.

Uma grande variedade de artigos é comercializada por phishers e impostores, tais como:

- números de cartões de crédito: normalmente, para que esses números tenham algum valor, é necessário ter também os números CVV2 (3 ou 4 dígitos presentes na parte de trás do cartão).
- acesso administrativo ou à raiz de servidores: servidores violados por crackers que os impostores podem acessar como desejam são comumente usados para hospedar sites de phishing, e são normalmente chamados de 'roots'.
- listas de endereços de e-mail: usadas para propagandas de spam ou como alvos de golpes de phishing.
- contas bancárias on-line.
- contas de serviços de pagamento on-line, como e-gold, que é bastante popular entre os impostores, pois os fundos podem ser enviados instantaneamente e, em geral, sem que possam ser rastreados.
- moedas falsificadas: o dinheiro falsificado é impresso e enviado pelo correio.

De acordo com a Symantec, empresa especializada em segurança digital, os gastos com crimes cibernéticos no Brasil em 2010 foi de US$ 15,3 bilhões. Segundo a empresa,

8 de cada 10 brasileiros conectados à internet já foram vítimas de algum crime cibernético.

Segundo o chefe da Unidade de Repressão a Crimes Cibernéticos da Polícia Federal, delegado Carlos Eduardo Miguel Sobral, os grupos de combate a fraudes eletrônicas foram transformados em delegacias de repressão a crimes cibernéticos. Além das fraudes eletrônicas bancárias, a Polícia Federal também investiga incidentes nas redes do Governo Federal por meio do Projeto Oráculo. A atuação é conjunta com o Departamento de Segurança da Informação e Comunicações (DSIC), órgão subordinado ao Gabinete de Segurança Institucional da Presidência da República. O DSIC é o responsável por planejar e coordenar a execução de atividades de segurança cibernética na administração pública federal.

O Governo Federal possui 320 redes para monitorar ataques cibernéticos. Esses ambientes sofrem de 6 a 7 milhões de incidentes por ano. Desse montante, o que de fato preocupa é 1% dos casos, que são as tentativas sérias de furtos de dados. Isso representa uma média de dois mil ataques graves por hora nessas 320 redes, que partem de organizações criminosas ou de grupos de crackers mal-intencionados.

Crackers invadiram a rede virtual da empresa Sony com 77 milhões de usuários do videogame Playstation. O ataque custará à empresa R$ 37,7 bilhões, segundo estimativa do Instituto Americano Ponemon.

A seguir listamos alguns casos reais de crimes cibernéticos ocorridos recentemente, apenas a título exemplificativo:

1. 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. São cumpridos 53 mandados – 8 de prisão preventiva, 10 de temporária e 35 de busca e apreensão – no Distrito Federal, Goiás e São Paulo. De acordo com a PF, a quadrilha enviava milhares de e-mails oferecendo serviços para pagamento com desconto de até 60% de boletos bancários e tributos como IPVA e IPTU. Ao acessar os links enviados no e-mail, o correntista entrava em páginas falsas e acabava fornecendo números de contas e senhas. Com isso, os golpistas conseguiram acessar a conta da pessoa e desviar dinheiro. A investigação aponta que a quadrilha usava parte do dinheiro desviado para fazer viagens, festas e comprar armas e drogas,

2. Racismo contra a cearense Melissa Gurgel, Miss Brasil 2014,

3. O Ministério Público Federal identificou e acusou, em 2014, internautas que postaram comentários considerados racistas contra os cearenses durante um acidente em Canindé, no interior do Ceará, que resultou na morte de 18 pessoas.

Diante de todo o exposto, e tendo em vista o aumento significativo do número de crimes cibernéticos, bem como seus efeitos deletérios perante a sociedade e a economia do 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, propomos a criação de uma CPI, para a qual contamos com o apoio de nossos nobres pares.

Sala das Sessões, em _____ de 2015.

Deputado Sibá Machado
(PT/AC)

Esta CPI, portanto, foi criada para investigar a a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade brasileiras.

2 – DA CONSTITUIÇÃO E COMPOSIÇÃO DA CPI

A constituição desta Comissão Parlamentar de Inquérito se deu em 05 de agosto de 2015, por Ato da Presidência, nos seguintes termos:

ATO DA PRESIDÊNCIA

Satisfeitos os requisitos do art. 35, caput, e § 4º, do Regimento Interno, para o Requerimento de Instituição de CPI nº 10, de 2015, do Sr. Sibá Machado e outros, esta Presidência constitui **Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a econômica e a sociedade neste país, tendo em vista: (i) que a Polícia Federal realizou em 2014 a operação IB2K para desarticular uma quadrilha suspeita de desviar pela Internet mais de R$ 2 milhões de correntistas de vários bancos, quadrilha que usava parte do dinheiro desviado para comprar armas e drogas; (ii) o último relatório da Central 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**, e

RESOLVE

I – designar para compô-la, na forma indicada pelas Lideranças, os Deputados constantes da relação anexa;

II – convocar os membros ora designados para a reunião de instalação e eleição, a realizar-se no dia 06 de agosto, quinta-feira, às 09h30, no Plenário 03 do Anexo II.

Brasília, 05 de agosto de 2015

EDUARDO CUNHA
Presidente da Câmara dos Deputados

A composição atual desta CPI é a seguinte:

PMDB/PP/PTB/DEM/PRB/SD/PSC/PHS/PTN/PMN/PRP/PSDC/PEN/PRTB
TITULARES
ALEXANDRE LEITE (DEM/SP)
ALUÍSIO MENDES (PSDC/MA)
CABUÇU BORGES (PMDB/AP)
ESPERIDIÃO AMIN (PP/SC)
JOÃO ARRUDA (PMDB/PR)
ODELMO LEÃO (PP/MG)
PR. MARCO DELICIANO (PSC/SP)
ROGÉRIO PENINHA MENDONÇA (PMDB/SC)
RONALDO NOGUEIRA (PTB/RS)
SUPLENTES
ARNALDO FARIA DE SÁ (PTB/SP)
CELSO JACOB (PMDB/RJ)
CONCEIÇÃO SAMPAIO (PP/AM)
JOÃO MARCELO SOUZA (PMDB/MA)
JUSCELINO FILHO (PRP/MA)
LAURA CARNEIRO (PMDB/RJ)
MARCELO AGUIAR (DEM/SP)
VALTENIR PEREIRA (PMDB/MT)
PT/PSD/PR/PROS/PCdoB
TITULARES
ALICE PORTUGAL (PCdoB/BA)
DELEGADO ÉDER MAURO (PSD/PA)
EVANDRO ROMAN (PSD/PA)
LAERTE BESSA (PR/DF)
LEO DE BRITO (PT/AC)
ODORICO MONTEIRO (PT/CE)
SANDRO ALEX (PSD/PR)
SILAS FREIRE (PR/PI)
SUPLENTES
JÔ MORAES (PCdoB/MG)
MARGARIDA SALOMÃO (PT/MG)
PAULO PIMENTA (PT/RS)

PSDB/PSB/PPS/PV
TITULARES
ÁTILA LIRA (PSB/PI)
DANIEL COELHO (PSDB/PE)
FÁBIO SOUSA (PSDB/GO)
MARIANA CARVALHO (PSDB/RO)
RAFAEL MOTTA (PSB/RN)
RODRIGO MARTINS (PSB/PI)
SUPLENTES
ALEX MANENTE (PPS/SP)
BRUNA FURLAN (PSDB/SP)
BRUNO COVAS (PSDB/SP)
FLAVINHO (PSB/SP)
JHC (PSB/AL)
NELSON MARCHEZAN JUNIOR (PSDB/RS)
PDT
TITULAR
SUBTENENTE GONZAGA (PDT/MG)
REDE
TITULAR
ALESSANDRO MOLON (REDE/RJ)

3 – PLANO DE TRABALHO

No início dos trabalhos desta Comissão, foi apresentado o presente Roteiro de Trabalho, com o fim de planejar as ações e estabelecer critérios e prioridades das atividades da CPI:

ROTEIRO DE TRABALHO

Proposta do Relator Deputado ESPERIDIÃO AMIN

I. INTRODUÇÃO

Visando ao bom funcionamento da CPI, sugerimos aos Ilustres Membros da Comissão Parlamentar de Inquérito dos Crimes Cibernéticos o presente roteiro de trabalho, que, através das atividades investigatórias, permita a formação da convicção dos Nobres Parlamentares acerca do tema.

A efetividade dos trabalhos da CPI será obra de todos os seus integrantes. Todos os Nobres Deputados serão convidados a participar ativamente das atividades da Comissão, inclusive sob a forma de requerimentos. Por isso, serão necessárias reuniões administrativas, convocadas com antecedência e com pauta especifica, para discussão e votação de requerimentos.

II. MÉTODO DE TRABALHO

Para a consecução dos objetivos da CPI, este Plano de Trabalho prevê a realização de aprovação de requerimentos diversos; oitiva de testemunhas, de autoridades públicas e de especialistas; e realização de diligências, entre outras providências. A credibilidade de uma investigação parlamentar passa pela robustez das provas que sustentam as suas conclusões.

Além das previstas neste Plano de Trabalho, poderão ser realizadas outras diligências julgadas necessárias pela Presidência, Relatoria e Plenário desta Comissão Parlamentar.

III. RELATÓRIO FINAL

Do Relatório Final poderão constar recomendações,

providências, propostas legislativas e eventual encaminhamento das respectivas conclusões ao Congresso Nacional, ao Poder Executivo, ao Ministério Público, ao Tribunal de Contas e aos Conselhos Profissionais respectivos, e aos demais órgãos responsáveis pela tomada das providências apontadas pela CPI.

IV. ATIVIDADES A SEREM DESENVOLVIDAS

a) Realizar oitiva de convidados especialistas, servidores públicos e autoridades públicas que possam contribuir para a realização deste trabalho, inclusive membros do Poder Judiciário, do Ministério Público e parlamentares relatores de projetos ligados ao tema; operadores do Direito em geral; e representantes de Organizações especializadas na temática, dentre outros;

b) Realizar sessões de debates, nas quais os membros terão a oportunidade de expor suas experiências práticas e teóricas sobre o tema;

c) Realizar estudos sobre a legislação pátria e internacional relacionadas aos crimes cibernéticos;

d) Verificar junto ao Poder Judiciário, ao Ministério Público, às Defensorias Públicas e às Polícias Judiciárias as denúncias de crimes cujo escopo seja informático, a fim de se obter parâmetro geral sobre essa modalidade de criminalidade em nosso país;

e) Realizar o levantamento das proposições legislativas relacionadas ao tema da CPI que estão em andamento na Câmara dos Deputados;

f) Realizar diligências para averiguação de denúncias de crimes cibernéticos;

g) Verificar as ocorrências de violações a direitos humanos praticadas por meio da internet;

h) Classificar as modalidades de crimes considerados como cibernéticos, como as de vazamento de informações pessoais, pornografia infantil, pedofilia, racismo, homofobia, maus tratos com os animais, estelionatos e outras fraudes, entre outros;

i) Analisar o crime organizado para o cometimento de delitos cibernéticos;

j) Estudar casos de operações policiais, como o caso da operação denominada IB2K, com o intuito de compreender o *modus operandi* de crimes de natureza cibernética;

k) Realizar reuniões administrativas com a finalidade de avaliar os trabalhos desenvolvidos, a fim de assegurar a qualidade do relatório a ser produzido;

V. ORIENTAÇÃO PARA OS TRABALHOS

Orienta-se que sejam alternadas as atividades de diligência para averiguação da ocorrência de crimes cibernéticos com aquelas descritas nos demais itens, com o intuito de tornar as diligências mais eficazes.

VI. CONCLUSÃO

As atividades previstas neste Roteiro de Trabalho objetivam conferir efetividade à investigação parlamentar, respeitando os postulados previstos na Constituição Federal.

Pretende-se levar a efeito a consecução de um trabalho técnico, eficiente e capaz de identificar a verdade real, propondo eventuais modificações nos marcos legais que regulam a matéria *sub examine.*

Nessa senda, será concretizada uma das atividades mais nobres do Congresso Nacional, qual seja, a função fiscalizadora.

Sala das Comissões, em 13 de agosto de 2015.

Deputado ESPERIDIÃO AMIN (PP/SC)
Relator

Este Roteiro de Trabalho foi aprovado em reunião realizada no dia 13 de agosto de 2015 e, embora o esforço da Comissão, **diversos dos pontos apontados não puderam ser devidamente desenvolvidos, em razão do prazo exíguo para a conclusão dos trabalhos da CPI, levando-se em conta a abrangência da matéria a ela relacionada**.

4 – REQUERIMENTOS APROVADOS PELA CPI

Esta Comissão Parlamentar de Inquérito aprovou, durante os seus trabalhos, os seguintes requerimentos:

Nº	AUTORIA	EMENTA	SITUAÇÃO	RESPOSTA(S)
01	Deputada Mariana Carvalho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de REQUISIÇÃO, ao Grupo de Trabalho de Enfrentamento aos Crimes Cibernéticos do Ministério Público Federal, de cópia em inteiro teor, inclusive em meio magnético e arquivo pesquisável, de todos os relatórios e análises estatísticas produzidas com base nos dados fornecidos pelas diversas unidades do **Ministério Público Federal**, relacionados ao combate aos crimes cibernéticos no Brasil.	**APROVADO na 4ª Reunião, realizada em 18/08/15**	OFÍCIO GAB/PRR2/N.C.Nº 1952, em 08/09/15, encaminha relatório com estatísticas, obtidas no sistema informatizado da PGR denominado Único. (Power Point, apresentado pela Dra. Neide M.C. Cardoso de Oliveira, na reunião do dia 10/09/15).
02	Deputada Mariana Carvalho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de COMPARTILHAMENTO de todo o material probatório produzido pela **Comissão Parlamentar de Inquérito** criada, no âmbito do **Senado Federal**, com o objetivo de se investigar e apurar a utilização da Internet para a prática de crimes de 'pedofilia', bem como a relação desses crimes com o crime organizado, que conclui seus trabalhos no ano de 2010.	**APROVADO na 6ª Reunião, realizada em 25/08/15**	OF. Nº 1329/2015-SF – 16/09/15. Do Senador Renan Calheiros. Encaminha tabela de documentos recebidos pela CPI Crimes de Pedofilia do Senado, para que esta CPI indique os documentos que deseja acessar.
03	Deputada Mariana Carvalho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVOCAÇÃO, à Unidade de Repressão de Crimes Cibernéticos da **Polícia Federal**, de cópia em inteiro teor, inclusive em meio magnético e arquivo pesquisável, de todos os levantamentos de dados, estudos, pesquisas, relatórios e análises estatísticas produzidas pelo órgão, relacionados ao combate aos crimes cibernéticos no Brasil.	**APROVADO na 4ª Reunião, realizada em 18/08/15**	Of. 307/2015-GAB/DPF, de 10/09/15 do Diretor – Geral da Polícia Federal, Delegado Leandro Daiello Coimbra, solicitando decisão específica do plenário da CPI acerca da quebra de sigilo, para fornecimento dos documentos solicitados.
04	Deputada Mariana Carvalho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE ao SENADOR **MAGNO MALTA**, que presidiu a Comissão Parlamentar de Inquérito que investigou a utilização da Internet para a prática de crimes de "pedofilia", bem como a relação desses crimes com o crime organizado, para prestar depoimento.	**APROVADO na 6ª Reunião, realizada em 25/08/15**	Audiência realizada em 08/09/2015. **(Compareceu)**

05	Deputada Mariana Carvalho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE a **NEIDE MARA CAVALCANTI CARDOSO DE OLIVEIRA**, Procuradora da República que coordena o Grupo de Trabalho de Enfrentamento aos Crimes Cibernéticos do Ministério Público Federal, e a DRA. **FERNANDA TEIXEIRA SOUZA DOMINGUES**, Procuradora da República em São Paulo que coordena o Grupo de Combate a Crimes Cibernéticos para prestar informações.	**APROVADO COM ALTERAÇÃO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 10/09/2015. **(Compareceram)**
06	Deputada Mariana Carvalho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE a **CARLOS EDUARDO MIGUEL SOBRAL**, Delegado Federal que chefia a Unidade de repressão a Crimes Cibernéticos da Polícia Federal, para prestar informações.	**APROVADO COM ALTERAÇÃO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 20/08/2015. **(Compareceu)**
07	Deputada Mariana Carvalho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE a **THIAGO TAVARES NUNES DE OLIVEIRA**, representante da SaferNet Brasil, para prestar informações.	**APROVADO COM ALTERAÇÃO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 29/09/2015. (**Compareceu)**
08	Deputado Daniel Coelho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE aos senhores presidentes das companhias **Google Brasil Internet Ltda**., **Microsoft do Brasil, Facebook Serviços Online do Brasil Ltda. E Twitter Brasil Rede de Informação Ltda**, para prestarem depoimentos.	**APROVADO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 27/08/2015. **(Compareceram)**
09	Deputado Daniel Coelho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE à senhora **MIRIAM LEITÃO**, para prestar depoimento.	**APROVADO na 6ª Reunião, realizada em 25/08/15**	Carta s/nº de 16/09/15, da Sra. Mirian Leitão, informando que **não poderá comparecer** a esta CPI devido a compromissos profissionais já assumidos.
10	Deputado Daniel Coelho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE ao senhor **RENATO DA SILVEIRA MARTINI**, Diretor-presidente do Instituto Nacional de Tecnologia da Informação – ITI, para prestar depoimento.	**APROVADO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 03/09/2015. **(Compareceu)**
11	Deputado Daniel Coelho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE à senhora **CAROLINA DIECKMANN**, para prestar depoimento.	**APROVADO na 6ª Reunião, realizada em 25/08/15**	Carta s/nº de 14/09/15, da Sra. Carolina Dieckmann, informando que **não poderá comparecer** a esta CPI devido a compromissos profissionais já assumidos.

12	Deputado Daniel Coelho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE ao senhor **CARLOS ALBERTO SARDENBERG**, para prestar depoimento.	**APROVADO na 6ª Reunião, realizada em 25/08/15**	Carta s/nº de 16/09/15, da Sr. Carlos Alberto Sardenberg, informando que **não poderá comparecer** a esta CPI devido a compromissos profissionais já assumidos.
14	Deputado João Arruda	Requer seja realizada reunião de Audiência Pública para debater as medidas adotadas pelas empresas de telecomunicações e de aplicações de internet para contribuir no combate aos crimes cibernéticos, com a presença dos seguintes convidados: **Eduardo Levy**, Diretor-Executivo do Sindicato Nacional das Empresas de Telefonia e de Serviço Móves Celular e Pessoal – SindiTelebrasil; **Fábio Coelho**, Presidente do **Google** Brasil; Diego Dzodan, Vice-Presidente do **Facebook** para a América Latina e **Guilherme Ribenboim**, Vice-Presidente do **Twitter** para a América Latina.	**APROVADO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 03/09/2015, Eduardo Levy **(Compareceu)** Audiência realizada em 27/08/2015. **(Compareceram)**
15	Deputado João Arruda	Requer seja realizada reunião de Audiência Pública em conjunto com a Comissão de Constituição e Justiça e de Cidadania para debate acerca do Projeto de Lei nº 5.555, de 2013, que "Altera a Lei nº 11.340, de 7 de agosto de 2006 – Lei Maria da Penha – criando mecanismos para o combate a condutas ofensivas contra a mulher na Internet ou em outros meios de propagação da informação", com a presença do convidado, **Thiago Tavares Nunes de Oliveira,** Presidente da empresa SAFERNET BRASIL.	**APROVADO na 6ª Reunião, realizada em 25/08/15**	Audiência realizada em 29/09/2015. **(Compareceu)**
16	Deputado João Arruda	Requer seja realizada reunião de Audiência Pública para debater assuntos relacionados à utilização da internet como meio para a prática de crimes de pedofilia, com a presença dos seguintes convidados: **Carolina de Oliveira Brandão**, Coordenadora-Geral do Conselho Nacional dos Direitos da Criança e do Adolescente – Conanda; **Carlos Eduardo Miguel Sobral,** Delegado da Unidade de Repressão a Crimes Cibernéticos da Polícia Federal e **Thiago Tavares**, presidente da SaferNet Brasil.	**APROVADO na 6ª Reunião, realizada em 25/08/15**	Audiência realizada em 08/09/2015, Pedro Affonso Duarte Hartung Em substituição a sra. Carolina Brandão. **(Compareceu)** Audiência realizada em 20/08/2015, Carlos Eduardo Miguel Sobral **(Compareceu)** Audiência realizada em 29/09/2015, Thiago Tavares **(Compareceu)**

17	Deputado João Arruda Subscrito pelo Deputado Leo de Brito	Requer a realização de Audiência Pública para discutir as implicações de crimes digitais nos sistemas de informática do governo e nos bancos de dados que contenham informações privadas de cidadãos, com os seguintes convidados, **Marcos Mazoni**, Diretor-Presidente do Serviço Federal de Processamento de Dados (SERPRO); **Jorge Rachid**, Secretário da Receita Federal do Brasil; Sr. **Rodrigo Ortiz D'Avila Assumpção**, Presidente da Empresa de Tecnologia e informações da Previdência Social (DATAPREV), **Cristiano Rocha Heckert,** Secretário de Logística e tecnologia da Informação (SLTI) e **Fernando de Lima Santos**, Chefe de Gabinete de Segurança Institucional (GSI), **Juliana Pereira da Silva**, representante do Senacom/MJ; Sr. **Sérgio Amadeo** da Universidade Federal do ABC; **Dennys Marcelo Antoniall**i, representante do Internetlab e representante do Centro de Tecnologia e Sociedade da FGV.	**APROVADO COM ALTERAÇÃO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 03/09/2015, Marcos Vinicius Ferreira Mazoni **(Compareceu)** Audiência realizada em 29/09/2015, Juliana Pereira da Silva **(Compareceu)** Audiência realizada em 12/11/2015, Dennys Marcelo Antonialli **(Compareceu)**
18	Deputado João Arruda	Requer seja realizada reunião de Audiência Pública para discussão dos crimes cibernéticos praticados contra o sistema bancário e seus correntistas. Convidando as seguintes autoridades: **Eduardo Rodrigues de Souza Filho**; Advogado Sênior na Federação Brasileira de bancos – FEBRABAN; **Wilson Rodrigues de Souza Filho**, Delegado da Polícia Federal da divisão de repressão a crimes financeiros do órgão; **Antônio Gustavo Rodrigues,** Presidente do Conselho de Controle de Atividades Financeiras – COAF, do Ministério da Fazenda.	**APROVADO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 24/09/2015, Adriano Cabral Volpini da FEBRABAN Em substituição ao Sr. Eduardo R. de Souza Filho **(Compareceu)**
19	Deputado João Arruda Subscrito pelo Deputado Pr. Marco Feliciano	Requer a realização de Audiência Pública para discutir questões referentes à intimidade na internet, os crimes contra a honra praticados por meio de plataformas digitais e suas implicações em face do Direito e das normas vigentes. Requer sejam convidados **Renato Opice Blum**, advogado especialista em Direito Eletrônico e **Luiz Cláudio Silva Allend**, advogado e residente da Comissão Especial de Direito e Tecnologia e Informação da Ordem dos Advogados do Brasil (OAB) e José Antônio Milagre, Advogado e perito em informática.	**APROVADO COM ALTERAÇÃO na 6ª Reunião, realizada em 25/08/15**	Audiência realizada em 10/09/2015, Luiz Cláudio Silva Allemand **(Não compareceu)**
20	Deputado Alexandre Leite	Solicita convidar o Senhor **Carlos Eduardo Miguel Sobral,** Delegado da Polícia Federal e integrante da Diretoria da Associação Nacional dos Delegados de Polícia Federal (ADPF).	**APROVADO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 20/08/2015. **(Compareceu)**
21	Deputado Leo de Brito	Requer sejam convidados os Srs. ELEMER COELHO e STÊNIO SANTOS, **delegados da Polícia Federal**, para prestar informações perante esta Comissão Parlamentar de Inquérito.	**APROVADO COM ALTERAÇÃO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 20/08/2015. **(Compareceram)**

23	Deputada Ana Perugin Subscrito pela deputada Jô Moraes	Requer seja convidado o Sr**. Carlos Eduardo Miguel Sobral,** chefe da Unidade de Repressão a Crimes Cibernéticos.	**APROVADO COM ALTERAÇÃO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 20/08/2015. **(Compareceu)**
24	Deputado Jean Wyllys Subscrito pela deputada Jô Moraes	Requer a realização de oitivas de especialistas, representantes de núcleos acadêmicos, lideranças de entidades da sociedade civil e movimentos sociais ligados ao tema da Comissão, com os seguintes convidados: **Leandro Daiello Coimbra**, Diretor Geral da Polícia Federal; **Elmer Coelho Vicente**, Delegado Chefe do Serviço de Repressão a Crimes Cibernéticos da Polícia Federal**; Pablo Bergman,** delegado da Unidade de Repressão ao Crime de Ódio e Pornografia Infantil na Internet; **Thiago Tavares Nunes de Oliveira**, Representante da ONG SaferNet; **Raquel Recuero,** jornalista, professora e pesquisadora do Programa de Pós-Graduação em letras e do Curso de Comunicação Social da Universidade Católica de Pelotas, doutora em Comunidades em Redes Sociais na Internet; **David Miranda**, Coordenador da Campanha pelo Asilo a Edward Snowden no Brasil; **Sérgio Amadeu**, professor adjunto da Universidade Federal do ABC (UFABC) e autor dos livros "Exclusão Digital: a miséria na era da informação" e "Software Livre: a luta pela Liberdade do conhecimento"; **Bia Barbosa**, jornalista e representante do Coletivo Intervozes; **Maíra Kubick,** doutora em Ciências Sociais pela UNICAMP e professora da UFBA**; Leonardo Sakamoto,** Coordenador geral da ONG Repórter Brasil e, diretora executiva da ONG Artigo 19. Foi oficial de programas do alto comissariado para direitos Humanos da ONU.	**APROVADO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 20/08/2015, Elmer Coelho Vicente **(Compareceu)** Audiência realizada em 29/09/2015, Thiago Tavares Nunes de Oliveira **(Compareceu)**
25	Deputado Odorico Monteiro	Requer a convocação do Sr. **Thiago Tavares**, Diretor da SAFERNET, para prestar informações perante esta Comissão Parlamentar de Inquérito.	**APROVADO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 29/09/2015 **(Compareceu)**
26	Deputada Alice Portugal Subscrito pelos deputados, Pr. Marco Feliciano, Silas Freire, Rodrigo Martins, Odorico Monteiro.	Requer que seja realizada audiência pública, tendo como convidados representantes da Federação Brasileira dos Bancos - **Febraban**, dos Bancos Itaú, Bradesco, Caixa Econômica Federal e Banco do Brasil, para apresentar junto a esta CPI informações a respeito das fraudes aplicadas aos correntistas e as instituições, utilizando sistemas computacionais e a rede mundial de computadores, bem como as medidas adotadas, tanto em nível tecnológico, quanto jurídico para o combate ao crime cibernético.	**APROVADO na 6ª Reunião, realizada em 25/08/15**	Audiência realizada em 24/09/2015, Adriano Cabral Volpini, FEBRABAN **(Compareceu)**

27	Deputada Alice Portugal	Requer que seja realizada audiência pública com a presença do Chefe de Repressão a Crimes Cibernéticos da Polícia Federal para apresentar informações sobre os crimes e fraudes cometidos com o uso da internet, das ações e providências realizadas, a taxa de elucidação dos crimes, dentre outras informações relevantes à CPI. Da mesma forma apresentar uma visão crítica das dificuldades encontradas no processo de investigação, tendo como convidado **Elmer Coelho Vicente**, Chefe de Repressão a Crimes Cibernéticos da polícia Federal.	**APROVADO na 4ª Reunião, realizada em 18/08/15**	Audiência realizada em 20/08/2015. Elmer Coelho Vicente **(Compareceu)**
28	Deputada Alice Portugal	Requer que seja realizada audiência pública com a presença de representante da SaferNet Brasil e do Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda) para apresentar a esta CPI dados sobre denúncias, crimes e violações contra os direitos humanos, a exploração sexual de criança e adolescente, praticados no ambiente da internet, bem como trazer informações sobre as ações e os encaminhamentos promovidos para a solução e o enfrentamento dos crimes e das infrações. Solicita sejam convidados os Srs.: **Thiago Nunes de Oliveira,** Diretor-Presidente da SaferNet Brasil e **Carolina Brandão**, Secretária Executiva do Conselho Nacional dos Direitos da Criança e do Adolescente.	**APROVADO na 6ª Reunião, realizada em 25/08/15**	Audiência realizada em 08/09/2015, Pedro Affonso Duarte Hartung **(Compareceu)** Audiência realizada em 29/09/2015, Thiago Tavares Nunes de Oliveira **(Compareceu)**
29	Deputada Alice Portugal Subscrito pela deputada Jô Moraes	Requer que seja realizada audiência pública para que sejam apresentadas, perante esta CPI, informações sobre incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira e dados sobre invasões, ou tentativas de invasão, às redes de computadores da Administração Pública Federal. Solicita sejam convidados dos Srs.: **Marconi dos Reis Bezerra,** Diretor do Departamento de Segurança da Informação e Comunicações – DSIC do gabinete de Segurança Institucional da Presidência da República – GSI/PR e **Demi Getschko**, Diretor Presidente do Núcleo de Informação e Coordenação do Ponto BR - NIC.br, braço executivo do Comitê Gestor da Internet no Brasil – CGI.br, responsável pelo CERT.br – Centro de estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.	**APROVADO COM ALTERAÇÃO na 6ª Reunião, realizada em 25/08/15**	Audiência realizada em 17/09/2015, Marconi dos Reis Bezerra **(Compareceu)** Audiência realizada em 03/09/2015, **Cristine Hoepers** (representante do Sr. Demi Getschko) **(Compareceu)**

30	Deputado Jean Wyllys	Requer a realização de audiência pública para discutir o financiamento de crimes cibernéticos por meio de anúncios e propagandas em websites utilizados para o cometimento de crimes. **Edson Luiz Vismona**, Presidente do Fórum Nacional Contra a Pirataria e Ilegalidade; **Elmer Coelho Vicente**, Delegado Chefe do Serviço de Repressão a Crimes Cibernéticos da Polícia Federal; **Eduardo Ariente**, Doutor em Direito pela USP, Professor da Faculdade de Direito do Mackenzie e do Departamento de Ciências da Computação do IME/USP; **Pablo Ortellado**, Doutor em Filosofia pela Universidade de São Paulo, Professor de Gestão de Políticas Públicas. É coordenador do Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (Gpopai). Atualmente, desenvolve pesquisa sobre direitos autorais e políticas culturais; **Jorge Machado**, professor-doutor da Escola de Artes, Ciências e Humanidades (EACH) da Universidade de São Paulo. Possui graduação em Ciências Sociais pela Universidade de São Paulo (1996), doutorado em Sociologia pela Universidade de Granada (2001) e pós-doutorado na Universidade de Campinas (2004). Atua na área de Políticas Públicas, dedicando-se principalmente às temáticas associadas à tecnologia de informação e humanidades.	**APROVADO na 6ª Reunião, realizada em 25/08/15**	Audiência realizada em 20/08/2015, Elmer Coelho Vicente **(Compareceu)**
31	Deputado Rafael Motta	Requer a realização de Audiência Pública da Comissão Parlamentar de Inquérito - Crimes Cibernéticos, para tratar dos crimes virtuais praticados contra crianças e adolescentes, no início do mês de outubro do corrente ano, na cidade de Natal-RN, com a presença das seguintes pessoas: **Kandy Takashi**, Superintendente Regional da Polícia Federal no Rio Grande do Norte; **Kalina Leite**, Secretária de Estado de Segurança Pública do Rio Grande do Norte; **Rubens Alexandre de França**, Delegado da Polícia Federal no rio Grande do norte; **Wellington Guedes**, Delegado da polícia Civil do Estado do Rio Grande do Norte e **Dilma Felizardo**, Diretora Executiva do Instituto Brasileiro de Estudos, Pesquisas e Formação para a Inovação Social (Ibeps).	**APROVADO na 6ª Reunião, realizada em 25/08/15**	Audiência realizada em 05/10/2015, em Natal/RN Márcio Tenório Wanderley. Rubens Alexandre de França. Mário Azevedo Jambo. Maria Dilma Felizardo Bezerra. Ricardo Kleber Martins Galvão. **(Compareceram)** Kalina Leite Gonçalves **(Não compareceu)**
33	Deputado Leo de Brito	Requer que sejam convidados os senhores **Paulo Renâ** e **Cristiana Gonzalez.**	**APROVADO na 8ª Reunião, realizada em 01/09/15**	Audiência realizada em 22/09/2015, **Cristiana Gonzalez** **(Compareceu)**
34	Deputado Leo de Brito	Requer que sejam convidados os senhores **Pedro Rezende**, **Pedro Markun**, e **Pablo Ximenes**.	**APROVADO na 8ª Reunião, realizada em 01/09/15**	Audiência realizada em 13/10/2015, Pedro Rezende, Pedro Markun, e Pablo Ximenes **(Compareceram)**

35	Deputado Leo de Brito	Requer que sejam convidados os Senhores **Marcelo Branco** e **Pablo Cerdeira** para prestar informações nessa CPI.	**APROVADO na 8ª Reunião, realizada em 01/09/15**	Audiência realizada em 12/11/2015, Pablo Cerdeira **(Compareceu)**
36	Deputado Jean Wyllys	Requer que esta Comissão Parlamentar de Inquérito convide os(as) **representantes** dos **movimentos MBL** e **Revoltados On Line**; a senhora **Beatriz Kicis de Sordi** e o responsável pelo perfil **"Faca na Caveira"** para prestarem depoimento.	**APROVADO COM ALTERAÇÃO na 8ª Reunião, realizada em 01/09/15**	Audiência realizada em 27/10/2015, Beatriz kicis **(Compareceu)**
37	Deputado Jean Wyllys	Requer sejam convidados o representante do **Humaniza Redes** - Pacto Nacional de Enfrentamento às Violações de Direitos Humanos na internet e o Sr. **Thiago Tavares Nunes de Oliveira**, Representante da ONG SaferNet para prestarem informações a esta CPI.	**APROVADO na 8ª Reunião, realizada em 01/09/15**	Audiência realizada em 29/09/2015, Thiago Tavares Nunes de Oliveira **(Compareceu)**
38	Deputado João Arruda	Requer seja realizada reunião de Audiência Pública para debater as ações de instituições envolvidas no combate ao crime cibernético**. Centro de Comunicações e Guerra Eletrônica do Exército - CCOMGEX; Instituto Nacional de Criminalística - ABC e Associação Brasileira de Criminalística.**	**APROVADO na 8ª Reunião, realizada em 01/09/15**	Audiência realizada em 17/09/2015
39	Deputado Odorico Monteiro	Requer a convocação do Sr. **GABRIEL SAMPAIO**, representante da Secretaria de Assuntos Legislativos do Ministério da Justiça, para colaborar com o bom andamento desta Comissão Parlamentar de Inquérito. No texto, mudar de convocado para convidado.	**APROVADO COM ALTERAÇÃO na 8ª Reunião, realizada em 01/09/15**	
40	Deputado Odorico Monteiro	Requer o convite do Sr. **RICARDO BERZOINI** - Ministro de estado das Comunicações, para colaborar com o bom andamento desta Comissão Parlamentar de Inquérito.	**APROVADO COM ALTERAÇÃO na 8ª Reunião, realizada em 01/09/15**	
41	Deputado Odorico Monteiro	Requer o convite do Sr**. PAULO RENÁ** - Diretor do Instituto Beta para Internet e Democracia e Mestre em Direito pela UNB, para colaborar com o bom andamento desta Comissão Parlamentar de Inquérito.	**APROVADO COM ALTERAÇÃO na 8ª Reunião, realizada em 01/09/15**	
42	Deputado Odorico Monteiro	Requer o convite do Sr. **LUIZ MONCAU** - Representante do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas, para colaborar com o bom andamento desta Comissão Parlamentar de Inquérito.	**APROVADO COM ALTERAÇÃO na 8ª Reunião, realizada em 01/09/15**	

43	Deputado Juscelino Filho	Requer a realização de audiência pública para discutir a privacidade, intimidade, inviolabilidade, exclusividade, propriedade individual e particular dos dados pessoais e sobre o direito de esquecimento, com os senhores: **Carol Conway**, Diretora do Conselho de Estudos Jurídicos da Associação Brasileira de Internet (Abranet); **Virgilio Augusto Fernandes Almeida,** Representante Titular do Ministério da Ciência, Tecnologia e Inovação do Comitê Gestor da Internet (CGI); **Luiz Claudio Silva Allemand,** Presidente da Comissão Especial de Direito da Tecnologia e Informação e da Comissão Especial de Transparência e Acesso à Informação da Ordem dos Advogados do Brasil (OAB) e **Aurélio Veiga Rios**, Procurador Federal dos Direitos do Cidadão do Ministério Público Federal.	**APROVADO na 8ª Reunião, realizada em 01/09/15**	Audiência realizada em 10/09/2015, Luiz Cláudio Silva Allemand **(Não compareceu)**
44	Deputado Alexandre Leite	Solicita convidar o Senhor **Jeferson Monteiro**, criador do perfil "Dilma Bolada".	**APROVADO COM ALTERAÇÃO na 8ª Reunião, realizada em 01/09/15**	Audiência realizada em 29/10/2015, Jeferson Monteiro **(Compareceu)**
45	Deputado Alexandre Leite	Solicita convidar a Senhora **Danielle Fonteles**, proprietária da agencia Pepper Interativa.	**APROVADO COM ALTERAÇÃO na 8ª Reunião, realizada em 01/09/15**	
47	Deputado Alexandre Leite	Solicita convidar o Senhor **Sérgio Diniz**, proprietário da Sarkis Comunicação.	**APROVADO COM ALTERAÇÃO na 8ª Reunião, realizada em 01/09/15**	
49	Deputado Subtenente Gonzaga	Requer a realização de Convite para prestar informações sobre as manipulações ocorridas na enquete sobre o Estatuto da Família no site da Câmara dos Deputados. Convidados: representantes técnicos do Centro de Informática da Câmara dos Deputados– CENIN e da Secretaria de Comunicação Social da Câmara dos Deputados - SECOM, bem como o Deputado Cléber Verde Secretário de Comunicação Social e também o Deputado Diego Garcia, relator do PL 6.583/2013 e denunciante dos fatos.	**APROVADO na 8ª Reunião, realizada em 01/09/15**	

50	Deputado Fabio Sousa	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE à senhora ANGÉLICA MOURA GOULART, Secretária Nacional de Promoção do Direito da Criança e Adolescente, para apresentar a essa CPI dados sobre denúncias recebidas pelo DISQUE 100, relacionadas à violência sexual, contra a criança e o adolescente no ambiente virtual.	**APROVADO na 8ª Reunião, realizada em 01/09/15**	Audiência realizada em 08/09/2015, **Heloiza de Almeida Prado Botelho Egas** - Coordenadora - Geral de Enfrentamento da Violência Sexual Contra Criança e Adolescentes da Secretaria Nacional de Promoção dos Direitos da Criança e do Adolescente **(Compareceu)**
51	Deputado Rafael Motta	Requer que a Comissão Parlamentar de Inquérito dos Crimes Cibernéticos convide o senador **Magno Malta** (PR-ES), para colaborar com a sub-relatoria sobre os crimes praticados contra a criança e o adolescente no ambiente virtual.	**APROVADO na 8ª Reunião, realizada em 01/09/15**	Audiência realizada em 08/09/2015, **(Compareceu)**
52	Deputado Rafael Motta	Requer que a Comissão Parlamentar de Inquérito dos Crimes Cibernéticos convide servidores públicos da Polícia Federal e da Justiça Federal, para colaborarem com a sub-relatoria sobre os crimes praticados contra a criança e o adolescente no ambiente virtual. Chefe da Unidade de Repressão a Crimes Cibernéticos da Polícia Federal, senhor **Adalto Martins**, para tratar da Operação Carrossel; Delegado da Polícia Federal responsável pela Operação Tapete Persa, senhor **Marcelo Bórcio**; Delegado da Polícia Federal responsável pela Operação Moicano, senhor **Valdemar Latance Neto**; Juíza federal do estado de Minas Gerais, senhora **Simone dos Santos Lemos**, para tratar da atuação dos pedófilos na internet.	**APROVADO COM ALTERAÇÃO na 8ª Reunião, realizada em 01/09/15**	
53	Deputado Rafael Motta	Requer que a Comissão Parlamentar de Inquérito dos Crimes Cibernéticos convide representantes do Unicef, da Unesco e da **Childhood Brasil**, para colaborarem com a sub-relatoria sobre os crimes praticados contra a criança e o adolescente no ambiente virtual.	**APROVADO COM ALTERAÇÃO na 8ª Reunião, realizada em 01/09/15**	Audiência realizada em 29/09/2015, Itamar Batista Gonçalves - Gerente de Advocacy da Childhood Brasil e Adalto Soares - Representante da UNESCO **(Compareceram)**
55	Deputado Alexandre Leite	Solicita convidar a Senhora **Márcia Godoy**, professora universitária e ex-funcionária da Sarkis Comunicação, para prestar informação.	**APROVADO COM ALTERAÇÃO na 8ª Reunião, realizada em 01/09/15**	
56	Deputado Rogério Peninha Mendonça	Requer convidar palestrante para participar da Audiência Pública que discutirá os crimes cibernéticos no Brasil, com a senhora, **Patrícia Peck Pinheiro**, advogada especialista em Direito Digital e Profº **Pedro Mizukami**, Centro de tecnologia e Sociedade da Fundação Getúlio Vargas.	**APROVADO COM ALTERAÇÃO na 9ª Reunião, realizada em 08/09/15** (Sugestão da deputada Margarida Salomão)	Audiência realizada em 22/09/2015, Patricia Peck **(Compareceu)** Audiência realizada em 13/10/2015, Profº Pedro Mizukami **(Compareceu)**

57	Deputado Daniel Coelho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE à senhora MARIA JÚLIA COUTINHO, para prestar informações.	**APROVADO na 8ª Reunião, realizada em 01/09/15 (Extra Pauta)**	Carta s/nº de 14/09/15, da Sra. Maria Júlia dos Santos Coutinho Moura, informando que **não poderá comparecer** a esta CPI devido a compromissos profissionais já assumidos.
58	Deputado Odelmo Leão	Requer convite ao SR. RONALDO LEMOS - Advogado, Professor e Pesquisador em temas de tecnologia e um dos principais criadores do Marco Civil da Internet, para colaborar com o bom andamento desta Comissão Parlamentar de Inquérito.	**APROVADO na 9ª Reunião, realizada em 08/09/15**	Audiência Pública realizada em 06/10/2015, Ronaldo Lemos (**Compareceu**)
59	Deputado Fabio Sousa	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE aos senhores delegados da Polícia Federal **Pablo Bergmann** e **Luiz Augusto Pessoa Nogueira,** para abordarem sobre a Operação Darkode, realizada pela PF em parceria com a FBI.	**APROVADO na 17ª Reunião, realizada em 01/10/15**	
60	Deputado Odorico Monteiro	Requer que seja convidado o senhor **Pablo Ximenes**, para prestar informações que possam auxiliar os parlamentares membros dessa comissão, tendo em vista o objeto de investigação da mesma.	**APROVADO na 17ª Reunião, realizada em 01/10/15**	Audiência Pública realizada em 13/10/2015, Pablo Ximenes **(Compareceu)**
61	Deputado Jean Wyllys	Requer que esta Comissão Parlamentar de Inquérito convide os responsáveis pelo perfil **"Faca na Caveira"** para prestar depoimento.	**APROVADO na 9ª Reunião, realizada em 08/09/15**	
62	Deputado Alexandre Leite	Solicita que esta CPI requisite ao Superior Tribunal de Justiça **cópia do inteiro teor de todos os documentos** relativos ao inquérito da **"Operação Acrônimo".**	**APROVADO na 11ª Reunião, realizada em 10/09/15**	Aguardando
64	Deputado Léo de Brito	Requer seja convidado o Sr. **Fábio Morais de Paula**, delegado da Polícia Federal, para prestar informações perante esta Comissão Parlamentar de Inquérito	**APROVADO na 11ª Reunião, realizada em 10/09/15**	
65	Deputado Delegado Éder Mauro Subscrito pelo deputado Rodrigo Martins	Solicita realização de Audiência Pública tratar questões de crimes cibernéticos, no que diz respeito a operacionalização entre fato criminoso e investigação, dentre outros.	**APROVADO na 14ª Reunião, realizada em 22/09/15**	
67	Deputada Mariana Carvalho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE ANDRÉ ABREU MAGALHÃES, Perito Criminal da Polícia Federal, para prestar esclarecimentos, por ter atuado na equipe das Operações Proteja Brasil, Darknet (desdobramento) e Genesis, deflagradas para coibir a exploração sexual infantil na Internet.	**APROVADO na 11ª Reunião, realizada em 10/09/15**	Audiência realizada em 15/09/2015, André Abreu Magalhães **(Compareceu)**

68	Deputado Daniel Coelho	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE a JOAQUIM BENEDITO BARBOSA GOMES, para prestar depoimento.	**APROVADO na 17ª Reunião, realizada em 01/10/15**	
69	Deputado Leo de Brito	Requer seja convidada a Sra. **Joanna Maranhão**, Fundadora da ONG Infância Livre, para prestar informações perante esta Comissão Parlamentar de Inquérito	**APROVADO na 14ª Reunião, realizada em 22/09/15**	
71	Deputado Fabio Sousa	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE aos senhores **Diego de Freitas Aranha, Pedro Antônio Dourado de Rezende**, e à senhora **Maria Aparecida da Rocha Cortiz**, membros do Comitê Multidisciplinar Independente (CMind), para prestarem informações sobre possíveis crimes cibernéticos relacionados ao voto eletrônico.	**APROVADO na 17ª Reunião, realizada em 01/10/15**	Audiência realizada em 22/10/15, Maria Aparecida da Rocha Cortiz **(Compareceu)**
73	Deputado Sandro Alex	Requer sejam tomadas as providências necessárias para convidar os expositores elencados, a fim de prestarem esclarecimentos sobre publicidade e comércio virtual na Internet. Sr. **Edinho Silva**, Ministro da Comunicação; Sr. **Gilberto Leifert**, Presidente do CONAR - Conselho Nacional de Autorregulamentação Publicitária;	**APROVADO na 14ª Reunião, realizada em 22/09/15**	Audiência pública realizada em 08/10/2015, compareceram o Ministro Edinho Silva, representante da ABA e representante da ABAP.
76	Deputado Sandro Alex	Requer a convocação de representante do **Conar** para prestar esclarecimentos sobre publicidade na internet.	**APROVADO na 17ª Reunião, realizada em 01/10/15**	
77	Deputado Sandro Alex	Requer a convocação de Diretores do Departamento de Tributação e Julgamento da Prefeitura de São Paulo e do Chefe da Coordenadoria da Administração Tributária da Secretaria da Fazenda do Estado de São Paulo.	**APROVADO na 23ª Reunião, realizada em 20/10/15**	
83	Deputado Leo de Brito	Requer seja aprovada por esta Comissão Parlamentar de Inquérito a realização de VISITA TÉCNICA ao Sr. **Edward Snowden**, agente da CIA, que se encontra em asilo político na Rússia.	**APROVADO. na 24ª Reunião, realizada em 22/10/15 Com a sugestão dos deputados Fábio Sousa e Esperidião Amin de inclusão de visita ao ativista Julian Assange, na Embaixada do Equador, em Londres.**	

84	Deputado Silas Freire Subscrito pelo Deputado Pastor Marco Feliciano	Requer que esta Comissão Parlamentar de Inquérito convide o Senhor **Domingos Meireles** para prestar esclarecimentos aos seus membros.	**APROVADO. na 23ª Reunião, realizada em 20/10/15**	
85	Deputado Silas Freire	Requer que esta Comissão Parlamentar de Inquérito convide o Senhor **Danilo Baltieri** para prestar esclarecimentos aos seus membros.	**APROVADO na 22ª Reunião, realizada em 15/10/15**	
87	Deputada Mariana Carvalho	Requer seja submetido à deliberação desta Comissão Parlamentar de Inquérito o pedido ora formulado de COMPARTILHAMENTO, pelo Ministério Público Federal, de cópias em inteiro teor e arquivo pesquisável, de todos os procedimentos investigatórios criminais, em andamento ou concluídos, incluída a documentação sigilosa neles contida, que tenham por objeto a apuração de ilicitudes relacionadas à publicidade digital promovida pelo Governo Federal nos últimos dez anos.	**APROVADO na 22ª Reunião, realizada em 15/10/15 Com o acréscimo de compartilhamento de informações de investigações sobre sites com conteúdo audiovisual ilícito (Pirata)**	
88	Deputada Mariana Carvalho	Requer seja submetido à deliberação desta Comissão Parlamentar de Inquérito o pedido ora formulado de COMPARTILHAMENTO, pela Polícia Federal, de cópias em inteiro teor e arquivo pesquisável, de todos os inquéritos policiais, em andamento ou concluídos, incluída a documentação sigilosa neles contida, que tenham por objeto a apuração de ilicitudes relacionadas à publicidade digital promovida pelo Governo Federal nos últimos dez anos.	**APROVADO na 22ª Reunião, realizada em 15/10/15 Com o acréscimo de compartilhamento de informações de investigações sobre sites com conteúdo audiovisual ilícito (Pirata)**	
91	Deputado Sandro Alex Subscrito pelo Deputado Pastor Marco Feliciano	Solicita a convocação do Senhor **Anderson de Andrade**, presidente da Abradi, do Senhor **Guilherme Ribenboim**, Presidente da IAB-Brasil, e do Senhor **Fábio Coelho**, diretor geral do Google Brasil para prestarem depoimento nesta CPI.	**APROVADO. na 23ª Reunião, realizada em 20/10/15**	
92	Deputado Silas Freire	Requer que esta Comissão Parlamentar de Inquérito convide a Senhora **Juliana Cunha,** Coordenadora da Safernet, para prestar esclarecimentos aos seus membros.	**APROVADO. na 24ª Reunião, realizada em 22/10/15**	

93	Deputado Rodrigo Martins	Requer que seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE ao Delegado de Polícia **Gerson Pereira**, ao repórter **Alex Barbosa** e à empresária **Daniela Carvalho** para falarem sobre o crime de sequestro de dados pela internet.	**APROVADO. na 24ª Reunião, realizada em 22/10/15**	
94	Deputado Rodrigo Martins	Requer que seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE à Delegada de Polícia **Mayana Rezende**, ao Promotor de Justiça **Fabrício Paturi**, ao Delegado de Polícia **Silvio Huppies** e o analista de segurança de informação **Fernando Mercel** para falarem sobre os crimes cibernéticos.	**APROVADO. na 24ª Reunião, realizada em 22/10/15**	
95	Deputada Mariana Carvalho **Subscrito pelos deputados Esperidião Amin e Leo de Brito**	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de REALIZAÇÃO DE AUDIÊNCIA PÚBLICA E DILIGÊNCIAS no Estado de Rondônia, para acompanhar o andamento e os resultados da operação Gênesis, da Polícia Federal.	**APROVADO. na 24ª Reunião, realizada em 22/10/15 COM O ACRÉSCIMO DE REALIZAÇÃO DE AUDIÊNCIAS PÚBLICAS E DILIGÊNCIAS NOS ESTADOS ONDE OCORRE A OPERAÇÃO GÊNESES DA POLÍCIA FEDERAL (AC, CE, MG, PE, RN, RO, SC E TO).**	
96	Deputado Rodrigo Martins	Requer que seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE ao Senhor **Pedro Sérgio Murari Pace** - Diretor da empresa Apple Computer Brasil Ltda., para prestar esclarecimentos sobre o funcionamento do comércio de aplicativos, músicas e outros realizados via Apple Store e Itunes, bem como sobre a segurança dos aplicativos comercializados.	**APROVADO. na 24ª Reunião, realizada em 22/10/15**	
99	Deputado Rafael Motta	Requer que a Comissão Parlamentar de Inquérito (CPI) dos Crimes Cibernéticos convoque o especialista em Segurança da Informação **Arthur César Oreana**, para colaborar com a sub-relatoria sobre os crimes praticados contra a criança e o adolescente no ambiente virtual.	**APROVADO. na 28ª Reunião, realizada em 05/11/15**	
103	Deputado Aluisio Mendes	Requer a requisição à Polícia Federal de 2 (dois) policiais especializados em crimes cibernéticos.	**APROVADO. na 28ª Reunião, realizada em 05/11/15**	

104	Deputada Mariana Carvalho	Requer a **prorrogação do prazo de funcionamento da CPI** - CRIMES CIBERNÉTICOS, por 60 (sessenta) dias, a contar do prazo inicialmente estipulado para o término efetivo dos trabalhos (04/12/2015), e suspendendo-se o prazo durante o período de recesso parlamentar.	**APROVADO. na 28ª Reunião, realizada em 05/11/15**	
105	Deputado Bruno Covas	Requer que sejam convidados o representante da Delegacia de Repressão aos Crimes de Informática do Estado do Rio de Janeiro para apresentação dos trabalhos já realizados sobre crimes cibernéticos e a atriz **Taís Araújo** para discutir questões sobre racismo na Internet.	**APROVADO. na 28ª Reunião, realizada em 05/11/15**	
107	Deputado Daniel Coelho	Requer que seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE a Procuradora da República, **Priscila Costa Schreiner**, para falar dos graves fatos noticiados na mídia acerca do assédio sexual sofrido pela participante do MasterChef Júnior.	**APROVADO. na 28ª Reunião, realizada em 05/11/15**	
108	Deputado Daniel Coelho	Requer que seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE ao jogador, **Michel Bastos**, para falar acerca do *cyberbullying* - ofensa e discriminação que sofreu nas redes sociais.	**APROVADO. na 28ª Reunião, realizada em 05/11/15**	
109	Deputado Daniel Coelho **Subscrito pelo deputado Fábio Sousa.**	Requer que seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE a atriz, **Taís Araújo**, para falar acerca do *cyberbullying* - ofensa e discriminação que sofreu nas redes sociais.	**APROVADO. na 28ª Reunião, realizada em 05/11/15 Com a sugestão do deputado Fábio Sousa de inclusão de convite à jornalista Raquel Sherazade.**	
110	Deputado Daniel Coelho	Requer que seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE ao Delegado de Polícia, **Eli José de Oliveira**, para falar acerca do vazamento de cenas mórbidas na internet.	**APROVADO. na 28ª Reunião, realizada em 05/11/15**	Audiência Pública realizada em 10/11/2015, Eli José de Oliveira (**Compareceu**)
111	Deputado Sandro Alex	Requer a inclusão de convidados para a Audiência Pública destinada a discutir a criptografia de WhatsApp, objeto do Requerimento nº 65, de 2015.	**APROVADO. na 28ª Reunião, realizada em 05/11/15**	
112	Deputado Sandro Alex	Requer convidar representantes do Ministério Público a Sra. **Neide Mara Cavalcante**, Procuradora Regional da República no Estado do Rio de Janeiro e a Sra. **Fernanda Teixeira Souza Domingos**, Procuradora da República no Estado de São Paulo, para reunião de trabalho nesta CPI.	**APROVADO. na 34ª Reunião, realizada em 26/11/15**	

116	Deputado Bruno Covas	Requer que seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE ao Senhor RONALDO TOSSUNIAN, Delegado de Polícia do Estado de São Paulo e atualmente Delegado Titular da 4ª Delegacia de Investigações sobre Fraudes Patrimoniais praticadas por meios eletrônicos do Departamento de Investigações Criminais - DEIC, para prestar informações a esta comissão.	**APROVADO. na 34ª Reunião, realizada em 26/11/15**	
117	Deputado Fábio Sousa	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de REQUISIÇÃO DE INFORMAÇÕES E DOCUMENTOS abaixo discriminados à Ministra das Mulheres, da Igualdade Racial e dos Direitos Humanos da Presidência da República. (trata de denúncia da jornalista Sherazade contra postagens ofensivas do Jeferson Monteiro.	**APROVADO. na 34ª Reunião, realizada em 26/11/15**	
118	Deputado Rafael Motta	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE à senhora JULIANA DE FARIA, jornalista que lançou a hashtag no Twitter, #PrimeiroAssédio, com o objetivo de estimular mulheres a contarem os casos de assédio que viveram na infância e devido a comentários nas redes sociais de cunho sexual a respeito de uma das participantes do reality show MasterChef Júnior, para prestar esclarecimentos.	**APROVADO. na 34ª Reunião, realizada em 26/11/15**	
119	Deputado Rafael Motta	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE à senhora FABIANA DOS SANTOS KASPARY, Juíza de Direito na Comarca de Porto Alegre, para prestar esclarecimentos.	**APROVADO. na 34ª Reunião, realizada em 26/11/15**	
120	Deputado Rafael Motta	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE à senhora LAURA LOWENKRON, Antropóloga e autora do livro "O monstro contemporâneo: a construção social da pedofilia em múltiplos planos", para prestar esclarecimentos.	**APROVADO. na 34ª Reunião, realizada em 26/11/15**	
121	Deputado Rafael Motta	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE à senhora NADINE GASMAN, Representante da ONU Mulheres no Brasil, para prestar esclarecimentos.	**APROVADO. na 34ª Reunião, realizada em 26/11/15**	

122	Deputado Silas Freire	Requer que esta Comissão Parlamentar de Inquérito solicite de oficio à Policia Federal que identifique e investigue os responsáveis pelos comentários preconceituosos e maldosos contra os nordestinos, na reportagem do dia 11/11/2015 do Portal G1/Globo do Estado do Piauí, referente a colisão entre Metrô e Trem na cidade de Teresina.	**APROVADO. na 34ª Reunião, realizada em 26/11/15 Com a supressão de envio de ofício ao Portal G1.**	
123	Deputado Bruno Covas	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE ao Senhor MARCELO DIAS, Presidente da Comissão da igualdade Racial da OAB-RJ, para prestar informações a esta comissão.	**APROVADO. na 34ª Reunião, realizada em 26/11/15**	
124	Deputado Bruno Covas	Requer seja submetido à deliberação do Plenário desta Comissão Parlamentar de Inquérito o pedido ora formulado de CONVITE ao Senhor ALESSANDRO THIERS, delegado-titular da Delegacia de Repressão a Crimes de Informática (DRCI) da Polícia Civil do Estado do Rio de Janeiro, prestar informações a esta comissão.	**APROVADO. na 34ª Reunião, realizada em 26/11/15**	
125	Deputado Sandro Alex	Requer sejam tomadas as providências necessárias para CONVIDAR o Delegado da Polícia Federal, Dr. VALDEMAR LATANCE NETO, Delegado Federal de Sorocaba e Chefe do Setor de Inteligência da PF, para prestar esclarecimentos sobre a "Operação Barba Negra" deflagrada em 18 de novembro de 2015, na região de Sorocaba, no Estado de São Paulo, que desbaratou o maior site pirata da América Latina.	**APROVADO. na 34ª Reunião, realizada em 26/11/15**	
130	Deputado Paulo Henrique Lustosa	Requer autorização para que membros da CPI possam visitar os **"Data Centers"** das empresas de telefonia Claro/Embratel, Vivo/Telefônica, Tim e Oi no intuito de analisar e fiscalizar como é feita a segurança dos sistemas.	**APROVADO. na 34ª Reunião, realizada em 26/11/15**	
131	Deputado Paulo Henrique Lustosa	Requer a inclusão de convidados para Audiência Pública destinada a discutir questões de crimes cibernéticos no que diz respeito a criptografia, objeto do Requerimento nº 65 de 2015. **Pablo de Camargo Cerdeira**, FGV/RJ; **Klaus Steding-Jessen**, Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil; **Luiz Moncau**, Pesquisador e Cogestor do Centro de Tecnologia e Sociedade-FGV RJ e **Sergio Amadeu**, Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas – Universidade Federal do ABC. (Os dois últimos só convidar na ausência dos dois primeiros)	**APROVADO. na 34ª Reunião, realizada em 26/11/15**	

132	Deputado Delegado Éder Mauro	Requer o envio de Indicação ao Excelentíssimo Senhor Ministro das Comunicações sugerindo, por intermédio da Agência Nacional de Telecomunicações - ANATEL a implementação de sua legislação para regular e aumentar a segurança das operadoras de telefonia no que tange às práticas de crimes cibernéticos.	**APROVADO. na 36ª Reunião, realizada em 03/12/15**	
133	Deputado Jhc	Requer a convocação, pela CPI - Crimes Cibernéticos, do Diretor-Geral da Agência Brasileira de Inteligência, Sr. **Wilson Roberto Trezza**, o Diretor-Geral da Polícia Federal, Sr. **Leandro Daiello Coimbra**, e da Srª. **Ozana Rodrigues**, mãe do brasileiro recrutado pelo Estado islâmico através da internet, para esclarecimentos sobre a maneira com a qual extremistas religiosos têm se valido da internet como instrumento de cooptação de brasileiros, as medidas repressivas e eventuais carências legislativas no ordenamento brasileiro que impeçam uma profícua dos órgãos competentes pela prevenção e repressão de atos de terrorismo. No texto, mudar de convocado para convidado.	**APROVADO COM ALTERAÇÃO . na 36ª Reunião, realizada em 03/12/15**	
134	Deputado Rodrigo Martins	Solicita informações ao Ministério das Comunicações quanto aos procedimentos adotados pela Agência Nacional de Telecomunicações - Anatel no que diz respeito aos testes de homologação de equipamentos de interconexão à rede mundial de computadores, em especial quanto à vulnerabilidades de segurança.	**APROVADO na 40ª Reunião, realizada em 18/02/16**	
137	Deputado Jhc	Requer que seja realizada, no âmbito desta Comissão, audiência pública para que sejam discutidos o *Cyberbullying* e o *Cyberstalking* enquanto crimes cibernéticos.	**APROVADO na 40ª Reunião, realizada em 18/02/16**	Audiência Pública realizada em 03/03/2016, Gisele Truzzi e Maria Tereza Maldonado (**Compareceram**)
138	Deputado Silas Freire Subscrito pelo Deputado Esperidião Amin	Requer a realização de audiência pública para ouvir junto a Comissão Parlamentar de inquérito destinada a investigar a pratica de crimes Cibernéticos, do Sr. **Juiz Luiz Moura Correia** da Central de Inquéritos da Comarca de Teresina-PI.	**APROVADO na 40ª Reunião, realizada em 18/02/16**	
139	Deputado Esperidião Amin	Requer seja convidado o Dr. FABIANO FONSECA BARBEIRO, Delegado da Polícia Civil do Estado de São Paulo, para ser ouvido, em REUNIÃO RESERVADA, por esta Comissão Parlamentar de Inquérito.	**APROVADO na 40ª Reunião, realizada em 18/02/16**	Audiência realizada em 01/03/16, Fabiano Fonseca Barbeiro **(Compareceu)**
140	Deputado Delegado Éder Mauro	Requer a realização no âmbito desta Comissão, audiência pública para que sejam discutidas e apuradas denúncias de ameaças terroristas, principalmente pelo meio cibernético, tendo em vista a ocorrência das Olimpíadas de 2016.	**APROVADO na 40ª Reunião, realizada em 18/02/16**	Seminário realizado em 29/03/16.
141	Deputada Mariana Carvalho	Requer a prorrogação do prazo de funcionamento da CPI - CRIMES CIBERNÉTICOS, por 60 (sessenta) dias, a contar do prazo estipulado para o término dos trabalhos (14/03/2016).	**APROVADO na 42ª Reunião, realizada em 01/03/16**	Req. 4.092/2016 Em 09/03/16 Defirida a prorrogação do prazo por 30 dias, “ad referendum”

142	Deputado Silas Freire	Requer que esta Comissão Parlamentar de Inquérito convide o Senhor Jivago Castro Ramalho para prestar esclarecimentos aos seus membros.	**APROVADO na 42ª Reunião, realizada em 01/03/16**	Audiência Pública realizada em 15/03/2016, Jivago de Castro Ramalho (**Compareceu)**
143	Deputado Flavinho	Requer a realização e Audiência Pública com a finalidade de debater a venda de produtos abortivos com entrega no Brasil, por sítios virtuais.	**APROVADO na 43ª Reunião, realizada em 03/03/16**	Audiência Pública realizada em 17/03/2016, Antonio Carlos França Kruel; Nailton Alves de Oliveira; Marileide Almeida Santos; José Jorge Silva da Costa; Patricia Azevedo Chagas **(Compareceram)**

Em face do encerramento dos trabalhos da Comissão, todavia, muitas das diligências e audiências requeridas não puderam ser realizadas.

5 – AUDIÊNCIAS PÚLICAS

Durante os trabalhos desta Comissão Parlamentar de Inquérito foram realizadas diversas audiências públicas, com o intuito de dar voz a todos aqueles que, de alguma forma, poderiam auxiliar no entendimento das diversas nuances que rondam o tema “crimes cibernéticos”, assim como possibilitar a discussão sobre melhorias legislativas concernentes à matéria.

5.1 – Audiência Pública realizada no dia 20 de agosto de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **STÊNIO SANTOS** – Chefe do Grupo de Repressão a Crimes Cibernéticos – Polícia Federal;

b) Sr. **ELMER COELHO VICENTE** – Chefe do Serviço de Repressão a Crimes Cibernéticos – Polícia Federal;

c) Sr. **CARLOS EDUARDO MIGUEL SOBRAL** – Assessor da Coordenação-Geral de Projetos de Tecnologia da Informação da Secretaria Extraordinária de Segurança em Grandes Eventos – Ministério da Justiça.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt200815-crc

5.2 – Audiência Pública realizada no dia 27 de agosto de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **MARCEL LEONARDI** – Diretor de Políticas Publicas do Google Brasil Internet;

b) Sr. **BRUNO MAGRANI** – Diretor de Relações Governamentais do Facebook Serviços Online do Brasil;

c) Sr. **FELIPE MAGRIM** – Diretor de Relações Governamentais do Twitter Brasil Rede de Informação;

d) Sr. **DIEGO GUALDA** – Diretor Jurídico do Yahoo do Brasil Internet Ltda.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt270815-crc

5.3 – Audiência Pública realizada no dia 03 de setembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **Marcos Vinícius Ferreira Mazoni** – Diretor-Presidente do Serviço Federal de Processamento de Dados - SERPRO;

b) Sr. **Renato Martini** - Diretor-Presidente do Instituto

Nacional de Tecnologia da Informação - ITI;

c) Sra. **Cristine Hoepers** - Gerente-Geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br (vinculado ao Comitê Gestor da Internet - CGI);

d) Sr. **Eduardo Levy Cardoso Moreira -** Presidente do Sindicato Nacional das Empresas de Telefonia e de Serviços Móvel Celular e Pessoal - SindiTelebrasil.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt030915-crc-sem-revisao

5.4 – Audiência Pública realizada no dia 08 de setembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sra. **HELOIZA DE ALMEIDA PRADO BOTELHO EGAS** – Coordenadora-Geral de Enfrentamento da Violência Sexual Contra Criança e Adolescentes da Secretaria Nacional de Promoção dos Direitos da Criança e do Adolescente;

b) Sr. **PEDRO AFFONSO DUARTE HARTUNG**- Conselho Nacional dos Direitos da Criança e do Adolescente;

c) Sr. **MAGNO MALTA** – Presidente da CPI que investigou

a Pedofilia na Internet.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt080915-crc-sem-revisao

5.5 – Audiência Pública realizada no dia 10 de setembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sra. **Fernanda Teixeira Souza Domingos** – Procuradora da República do Estado de São Paulo;

b) Sra. **Neide Mara Cavalcanti Cardoso de Oliveira** - Procuradora Regional da República da 2ª Região

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt100915-crc-sem-revisao

5.6 – Audiência Pública realizada no dia 15 de setembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **ANDRÉ ABREU MAGALHÃES** – Perito da Polícia Federal;

b) Sr. **LEONARDO BUENO DE MELO** – Representante do Instituto Nacional de Criminalística;

c) Sr. **EVANDRO MÁRIO LORENS** – Representante do Instituto Nacional de Criminalística;

d) Sr. **ALESSANDER FLORINDO DA SILVA** – Representante do Instituto Nacional de Criminalística;

e) Sr. **BRUNO TELLES** – Presidente da Associação Brasileira de Criminalística.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt150915-crc-sem-revisao

5.7 – Audiência Pública realizada no dia 17 de setembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **MARCONI DOS REIS BEZERRA** – Diretor do Departamento de Segurança da Informação e Comunicação – DSIC, do Gabinete de Segurança Institucional da Presidência da República - GSI

b) Sr. **OTÁVIO CARLOS CUNHA DA SILVA** – Diretor do Centro de Pesquisa e Desenvolvimento da Segurança e das Comunicações – CPESC/ABIN.

c) Sr. **PAULO ROBERTO DE ARAÚJO CASTRO VIANNA** – Chefe da Divisão de Operações do Centro de Defesa Cibernética do Exército.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt170915-crc-sem-revisao

5.8 – Audiência Pública realizada no dia 22 de setembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sra. **PATRÍCIA PECK PINHEIRO** – Advogada especialista em direito digital;

b) Sra. **CRISTIANA DE OLIVEIRA GONZALEZ** – Instituto Brasileiro de Defesa do Consumidor

As notas taquigráficas da reunião se encontram, na íntegra,

no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt220915-crc-sem-revisao

5.9 – Audiência Pública realizada no dia 24 de setembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **RODRIGO ORTIZ D'ÁVILA ASSUMPÇÃO** – Presidente da Empresa de Tecnologia e Informação da Previdência Social – Dataprev;

b) Sr. **CRISTIANO ROCHA HECKERT –** Secretário de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão;

c) Sr. **ADRIANO CABRAL VOLPINI –** Diretor Setorial da Comissão Executiva de Prevenção a Fraudes da Federação dos Bancos Brasileiros – Febraban;

d) Sra. **CLAUDIA MARIA DE ANDRADE –** Coordenadora-Geral de Tecnologia da Informação da Receita Federal.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt220915-crc-sem-revisao

5.10 – Audiência Pública realizada no dia 29 de setembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **THIAGO TAVARES NUNES DE OLIVEIRA** – Presidente da SaferNet Brasil;

b) Sr. **ITAMAR BATISTA GONÇALVES** – Gerente de Avocacy da Childhood Brasil;

c) Sra. **JULIANA PEREIRA DA SILVA** – Secretária Nacional do Consumidor – Senacon/MJ;

d) Sr. **ADAUTO CÂNDIDO SOARES** – Coordenador de Comunicação e Informação da UNESCO.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt290915-crc-sem-revisao

5.11 – Audiência Pública realizada no dia 05 de outubro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **MARCIO TENÓRIO WANDERLEY –** Delegado-Chefe

do Núcleo de Inteligência da Superintendência Regional da Polícia Federal do Rio Grande do Norte;

b) Sr. **RUBENS ALEXANDRE DE FRANÇA** – Delegado-Chefe da Delegacia Regional de Investigação e Combate ao Crime Organizado (DRCOR) da Superintendência Regional do Rio Grande do Norte;

c) Sr. **MÁRIO AZEVEDO JAMBO –** Juiz Federal da 2ª Vara do Tribunal Regional Federal da 5ª Região;

d) Sr. **MARIA DILMA FELIZARDO BEZERRA –** Presidente do Instituto Brasileiro de Estudos, Pesquisas e Formação para a Inovação Social (IBEPIS);

e) Sr. **RICARDO KLEBER MARTINS -** Professor das áreas de segurança de redes e perícia forense computacional no Instituto Federal de Educação, Ciência e Tecnologia (IFRN).

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt051015-crc-sem-revisao

5.12 – Audiência Pública realizada no dia 06 de outubro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **VIRGÍLIO ALMEIDA** – Secretário de Política de

Informática – SEPIN do Ministério da Ciência e Inovação - MCTI

b) Sr. **RONALDO LEMOS** – Advogado e Professor da Faculdade de Direito UERJ;

c) Sra. **CHARLENE NEGAE** – Advogada da Associação Brasileira de Internet - Abranet.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt061015-crc-sem-revisao

5.13 – Audiência Pública realizada no dia 08 de outubro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **EDINHO SIVLA –** Ministro da Secretaria de Comunicação Social da Presidência da República – Secom;

b) Sr. **ORLANDO MARQUES** – Presidente da Associação Brasileira de Agências de Publicidade - Abap

c) Sra. **SANDRA MARTINELLI –** Presidente-Executiva da Associação Brasileira de Anunciantes - ABA.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt081015-crc-sem-revisao

5.14 – Audiência Pública realizada no dia 13 de outubro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **PABLO XIMENES –** Diretor de Segurança da Informação da Empresa de Tecnologia da Informação do Estado do Ceará – ETICE;

b) Sr. **PEDRO MIZUKAMI** – Professor do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas;

c) Sr. **PEDRO REZENDE –** Professor de Ciência da Computação da Universidade de Brasília – Unb;

d) Sr. **PEDRO MARKUN –** Hacker do Labhacker e do Transparência Hacker.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt131015-crc-sem-revisao

5.15 – Audiência Pública realizada no dia 15 de outubro de 2015

Compareceram à audiência os seguintes convidados:

a) Sra. **VANESSA FONSECA - ** Diretora da Unidade de Combate a Crimes Cibernéticos da Microsoft Brasil;

b) Sr. **JOHNATAN RAZEN FERREIRA GUIMARÃES** – Diretor do Instituto Beta para Internet e Democracia – IDIDEM.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt151015-crc-sem-revisao

5.16 – Audiências Públicas realizadas nos dias 20, 27 e 29 de outubro de 2015

Nos dias 20, 27 e 29 de outubro foram realizadas audiências públicas com os seguintes convidados:

a) Sr. **RUBENS ALBERTO GATTI NUNES –** Coordenador Nacional do Movimento Brasil Livre (MBL);

b) Sra. **BEATRIZ KICIS TORRENTS DE SORDIS** – Perfil Beatriz Kicis;

c) Sr. **MARCELO REIS** – Coordenador Nacional do Movimento Revoltados ON LINE;

d) Sr. **JEFERSON MONTEIRO** – Perfil Dilma Bolada.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt291015-crc-sem-revisao

5.17 – Audiência Pública realizada no dia 03 de novembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **JOSÉ DE MELO CRUZ –** Coordenador de Sistemas Eleitorais do TSE;

b) Sra. **MARIA APARECIDA DA ROCHA CORTIZ** – Advogada, membro do Conselho Multidisciplinar Independente;

c) Sr. **GIUSEPPE JANINO –** Secretário de Tecnologia da Informação do Tribunal Superior Eleitoral - TSE

Destacamos, nos esclarecimentos prestados, os seguintes trechos, sendo que as notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt031115-crc-sem-revisao

5.18 – Audiência Pública realizada no dia 10 de novembro de 2015

Compareceu à audiência o seguinte convidado:

a) Sr. **ELI JOSÉ OLIVEIRA –** Delegado de Polícia de Classe Especial Titular da 4ª DDP/GO

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt101115-crc-sem-revisao

5.19 – Audiência Pública realizada no dia 12 de novembro de 2015

Compareceu à audiência o seguinte convidado:

a) Sr. **DENNYS MARCELO ANTONIALLI –** Diretor-Presidente da InternetLab.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-

temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt121115-crc-sem-revisao

5.20 – Audiência Pública realizada no dia 19 de novembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **FABRÍCIO RABELO PATURY –** Promotor de Justiça do Núcleo de Crimes Cibernéticos do Ministério Público do Estado da Bahia;

b) Sra. **MAYANA REZENDE** – Delegada do Grupo de Repressão a Estelionato da Delegacia Estadual de Investigações Criminais – DEIC/Goiânia/GO;

c) Sr. **SILVIO KIST HUPPES –** Delegado de Polícia, Titular da Delegacia de Policiamento do Interior DPI 19ª RP, Cidade de Encantado - Rio Grande do Sul;

d) Sr. **FERNANDO MERCES –** Analista de Segurança da Informação.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt191115-crc-sem-revisao

5.21 – Audiência Pública realizada no dia 24 de novembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **MARCOS AUGUSTO MESQUITA COELHO –** Diretor de Relações Institucionais da Oi;

b) Sr. **FÁBIO ANDRADE** – Diretor de Relações Institucionais da Claro/Embratel;

c) Sr. **ENYLSON FLÁVIO MARTINEZ CAMOLESI –** Diretor de Relações Institucionais da Telefonica/Vivo;

d) Sr. **NELSON DE SÁ –** Diretor de Segurança em T.I. da Tim;

e) Sr. **LEANDRO GUERRA** – Diretor de Relações Institucionais da Tim

f) Sr. **NILO PASQUALI** – Gerente de Regulamentação da Agência Nacional de Telecomunicações – Anatel.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt241115-crc-sem-revisao

5.22 – Audiência Pública realizada no dia 26 de novembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **ARTHUR CÉSAR OREANA –** Especialista em Segurança da Informação;

b) Sr. **GABRIEL DE CARVALHO SAMPAIO** – Diretor da Secretaria de Assuntos Legislativos do Ministério da Justiça.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt261115-crc-sem-revisao

5.23 – Audiência Pública realizada no dia 1º de dezembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **MARK KAHN –** Vice-Coordenador Jurídico Geral do WhatsApp;

b) Sr. **BRUNO MAGRANI** – Diretor de Relações Institucionais do Facebook Serviços Online do Brasil;

c) Sr. **ALEXANDRE CASTRO** – Diretor Regulatório do Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal – SINDITELEBRASIL;

d) Sr. **LUIZ FERNANDO MONCAU** – Professor do Centro

de Tecnologia e Sociedade da Fundação Getúlio Vargas;

e) Sr. **PABLO DE CAMARGO CERDEIRA** – Professor da Fundação Getúlio Vargas.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt011215-crc-sem-revisao

5.24 – Audiência Pública realizada no dia 15 de dezembro de 2015

Compareceu à audiência o seguinte convidado:

a) Sr. **JOSÉ CARLOS MARTINS DA CUNHA** – Diretor Substituto de Contraterrorismo da Agência Brasileira de Inteligência – ABIN.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt151215-crc

5.25 – Audiência Pública realizada no dia 17 de dezembro de 2015

Compareceram à audiência os seguintes convidados:

a) Sr. **RONALDO TOSSUNIAN** – Delegado do Departamento de Investigações Criminais de São Paulo;

b) Sr. **VALDEMAR LATANCE NETO** – Delegado da Polícia Federal.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt171215-crc

5.26 – Audiência Pública realizada no dia 16 de fevereiro de 2016

Compareceram à audiência as seguintes convidadas:

a) Sra. **JULIANA DE FARIA** – Jornalista e idealizadora do sítio de internet “Think Olga”;

b) Sra. **MAÍRA LIGUORI**;

c) Sra. **LUÍSE BELLO.**

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt160216-crc-sem-revisao

5.27 – Audiência Pública realizada no dia 25 de fevereiro de 2016

Compareceram à audiência o seguinte convidado:

a) Sr. **ANTÔNIO MEGALE** – Diretor de Assuntos Governamentais da Volkswagen do Brasil e 1º Vice-Presidente da Anfavea.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt250216-crc-sem-revisao

5.28 – Audiência Pública realizada no dia 01 de março de 2016

Compareceram à audiência o seguinte convidado:

a) Sr. **FABIANO FONSECA BARBEIRO** – Delegado do Departamento de Investigações Criminais de São Paulo (DEIC/SP).

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt010316-crc

5.29 – Audiência Pública realizada no dia 03 de março de 2016

Compareceram à audiência as seguintes convidadas:

a) Sra. **GISELE TRUZZI** – Advogada especialista em direito digital;

b) Sra. **MARIA TEREZA MALDONADO** – Psicóloga.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt030316-crc

5.30 – Audiência Pública realizada no dia 08 de março de 2016

Compareceram à audiência os seguintes convidados:

a) Sra. **VALÉRIA DIEZ SCARANCE FERNANDES** – Promotora de Justiça, Coordenadora do Núcleo de Violência Doméstica do Ministério Público de São Paulo;

b) Sra. **DIANA CALAZANS MANN** – Delegada da Polícia Federal;

c) Sra. **DULCIELLY NÓBREGA DE ALMEIDA** – Defensora Pública, Coordenadora do Núcleo de Defesa da Mulher da Defensoria Pública do Distrito Federal;

d) Sr. **THIAGO ANDRÉ PIEROBOM DE ÁVILA** – Coordenador do Núcleo de Defesa da Mulher do Ministério Público do Distrito Federal;

e) Sra. **ANA CRISTINA MELO SANTIAGO** – Delegada de Polícia, Chefe da Delegacia de Atendimento à Mulher do Distrito Federal.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt080316-crc

5.31 – Audiência Pública realizada no dia 15 de março de 2016

Compareceram à audiência os seguintes convidados:

a) Sr. **JIVAGO DE CASTRO RAMALHO** – vítima de calúnia da Internet;

b) Sr. **JOSÉ ANTONIO MILAGRE** – advogado, consultor e perito em informática.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt150316-crc-sem-revisao

5.32 – Audiência Pública realizada no dia 17 de março de 2016

Compareceram à audiência os seguintes convidados:

a) Sr. **ANTONIO CARLOS FRANÇA KRUEL** – Gerente Corporativo de Gestão do Portifólio de Encomendas/Vice-Presidência de Encomendas dos Correios;

b) Sr. **NAILTON ALVES DE OLIVEIRA** – Gerente Corporativo de Negócios Internacionais de Importação/Vice-Presidência de Logística dos Correios;

c) Sra. **MARILEIDE ALMEIDA SANTOS** – Gerente Corporativo de Prevenção e Apuração de Ilícitos/Vice-Presidência Corporativa dos Correios;

d) Sr. **JOSÉ JORGE SILVA DA COSTA** – Responsável pelo Parqueamento dos Equipamentos de Segurança no controle de objetos proibidos e perigosos/Vice-Presidência Corporativa dos Correios;

e) Sra. **PATRICIA AZEVEDO CHAGAS** – Assessora da Diretoria de Controle e Monitoramento Sanitários da Anvisa.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt080316-crc

5.33 – Seminário realizado no dia 29 de março de 2016

Compareceram ao seminário os seguintes convidados:

a) Sr. **GABRIEL BOFF MOREIRA** – Coordenador-Geral de Combate aos Ilícitos Internacionais do Ministério das Relações Exteriores;

b) Sr. **MARCONI DOS REIS BEZERRA** – Diretor do Departamento de Segurança da Informação e Comunicações da Casa Militar da Presidência da República — DSIC;

c) Sr. **JOSÉ RICARDO SOUZA CAMELO** – Chefe da Divisão de Operações do Centro de Defesa Cibernética — CDCIBER;

d) Sr. **WILLIAM MURAD** – Diretor de Inteligência da Secretaria Extraordinária de Segurança para Grandes Eventos do Ministério da Justiça;

e) Sr. **LEONARDO BOSELLI DA MOTTA** – Diretor do Departamento de Infraestrutura e Serviços de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão;

f) Sr. **EDUARDO ARTHUR IZYCKI** – Oficial de Inteligência da ABIN;

g) Sr. **ELMIZ ANTONIO ROCHA JUNIOR** – Delegado da Coordenação-Geral da Diretoria Executiva da Polícia Federal — CGE/DIREX.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt290316-crc

5.34 – Audiência Pública realizada no dia 31 de março de 2016

Compareceram à audiência a seguinte convidada:

a) Sra. **ANA MARIA DUARTE AMARANTE BRITO** – Desembargadora do Tribunal de Justiça do Distrito Federal e Territórios.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt310316-crc

5.35 – Audiência Pública realizada no dia 06 de abril de 2016

Compareceram à audiência os seguintes convidados:

a) Sra. **CAROL ELISABETH CONWAY** – Diretora de Assuntos Regulatórios do UOL;

b) **Sr. JÚLIO CESAR SCHMIDT** – Presidente do Egrana.

As notas taquigráficas da reunião se encontram, na íntegra, no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt060416-crc-1

6 – OITIVAS

Esta Comissão Parlamentar de Inquérito também convocou pessoas para serem ouvidas na condição de testemunhas, compromissadas em dizer a verdade, nos termos da lei.

A reunião convocada com esse objetivo foi realizada no dia 17 de novembro de 2015, para a qual foram convocadas as seguintes pessoas:

a) Sr. **LUCIANO GARCIA MIGUEL –** Coordenador da Coordenadoria de Administração Tributária da Secretaria da Fazenda do Estado de São Paulo;

b) **FLÁVIO SAMPAIO DANTAS** – Servidor da Secretaria Municipal de Finanças e Desenvolvimento Econômico da Prefeitura de São Paulo;

c) **REGINA CÉLIA CÂMARA NUNES** – Servidora da Secretaria Municipal de Finanças e Desenvolvimento Econômico da Prefeitura de São Paulo;

d) **CARLOS KATSUHITO YOSHIMORI** – Servidor da Secretaria Municipal de Finanças e Desenvolvimento Econômico da Prefeitura de São Paulo.

As notas taquigráficas da reunião podem ser consultadas no seguinte endereço eletrônico:

http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt171115-crc-sem-revisao

PARTE II – CONSTATAÇÕES E CONCLUSÕES

1 – INTRODUÇÃO

1.1 – CONSIDERAÇÕES GERAIS SOBRE A INTERNET

1.1.1 – O surgimento da Internet

A Internet surgiu no final dos anos 60, em razão da necessidade do Departamento de Defesa do Governo dos Estados Unidos por um sistema informatizado de defesa capaz de resistir a ataques inimigos. Para o atendimento desse requisito, pensou-se em se criar um sistema baseado em uma rede de computadores distribuídos com a capacidade de permanecer em operação mesmo que um ou mais dispositivos da rede fossem destruídos.

> Em lugar de um sistema de controle centralizado, a rede operaria como um conjunto de computadores autônomos que se comunicariam entre si. Joseph Licklider, um dos cientistas que trabalharam nesse conceito, criou o curioso nome de "rede galáctica" para o mesmo. O coração dessa rede seria uma fonte de comunicação por "pacotes", concebida pelo britânico Donald Davies, na qual cada informação seria dividida em blocos de tamanho fixo (os tais pacotes), que seriam enviados ao destinatário. Este último de encarregaria de remontar a mensagem inicial (LEINER et. Al. 1997: 102-103; ISAACSON, 2014: 221, 227, 236-237).[1]

Nesse contexto, a empresa ARPA (*Advanced Research and Projects Agency*) desenvolveu um sistema de comunicação de computadores em rede em 1969, no contexto histórico da Guerra Fria, com o nome de ARPANET, com o objetivo de manter a comunicação das bases militares dos Estados Unidos.

Passada a Guerra Fria, o acesso da ARPANET foi liberado para os cientistas que, mais tarde, disponibilizaram a rede para as universidades norte-americanas, que, sucessivamente, passaram-na para as universidades de outros países, permitindo que pesquisadores a acessassem de maneira global[2].

Na prática, o que os pesquisadores desenvolveram foi um conjunto de tecnologias muito simples, entretanto, extremamente confiável,

[1] LINS, Bernardo Felipe Estelita*. A evolução da internet: uma perspectiva história*. *In* Cadernos ASLEGIS nº 48. Brasília: ASLEGIS, 2015, p. 15.
[2] http://www.nethistory.info/Resources/Internet-BR-Dissertacao-Mestrado-MSavio-v1.2.pdf

voltadas para a interligação de computadores em condições precárias de comunicação. A esse conjunto de tecnologias se deu o nome de Internet[3].

> No início da década de 1980, houve uma separação da rede, dividindo-se em ARPANET e Milnet, sendo a segunda uma rede dedicada exclusivamente à troca militar de dados. Em 1986, os supercomputadores da NSF – National Science Foundation ou Fundação Nacional de Ciência – foram interligados com os da ARPANET, criando-se a espinha dorsal (backbone) da rede formada por um feixe de computadores superpotentes, permitindo-se a expansão da rede como se conhece, no final da década de 1980.
>
> A rede iniciou-se como canal de trocas de informações notadamente escritas, além de arquivos e programas simples. Sequencialmente, em 1989, Tim Bernes-Lee, um cientista inglês que trabalhava na European Organization dor Nuclear Research (Organização Europeia para Pesquisa Nuclear) na Suíça, desenvolveu um complexo sistema de documentos interligados que misturava texto, imagem, som e mídia e se inter-relacionava através da internet, por meio de ligações (links) que poderiam ser acionadas, levando o usuário conectado à internet a trafegar por diversos ambientes e plataformas diferentes, num ambiente visual mais rico e amigável.
>
> Essa tecnologia foi lançada em 1992 e conquistou os usuários por sua versatilidade, recebendo o nome de world wide web (larga teia mundial), ou simplesmente web, e popularmente conhecida pelas letras "www".[4]

Desde seu surgimento, portanto, a Internet não parou de evoluir. Há autores que apontam, nesse processo, quatro grandes períodos (levando-se em consideração a experiência do usuário): **a)** o período do uso privado das redes (em que as conexões eram predominantemente feitas entre computadores de maior porte); **b)** o período de abertura da rede ao público (caracterizado pelo uso da rede via linha discada e mediante um provedor de acesso); **c)** período do acesso em banda larga (caracterizado por velocidades cada vez mais elevadas e pela diversificação de conteúdos); e **d)** período da diversificação de telas (a Internet deixa de ser uma rede que acessamos para se tornar uma rede que nos envolve, pois todo usuário tem a seu dispor formas distintas de buscar seus dados e relacionar-se: o computador, o tablet, o telefone pessoal, a televisão digital, etc.)[5].

1.1.2 – O surgimento da Internet no Brasil

[3] http://www.rnp.br/
[4] SYDOW, Spencer Toth. Crimes informáticos e suas vítimas. 2. ed. São Paulo: Saraiva, 2015, p. 31.
[5] LINS, Bernardo Felipe Estelita. *A evolução da internet: uma perspectiva história*. *In* Cadernos ASLEGIS nº 48. Brasília: ASLEGIS, 2015, p. 13-14.

O embrião da internet brasileira originou-se com o Projeto da Rede Nacional de Pesquisa – RNP, criado em 1989 pelo MCT (Ministério de Ciência e Tecnologia), com apoio de instituições governamentais de vários estados, principalmente a Fundação de Amparo à Pesquisa do Estado de São Paulo – FAPESP. Já a Internet, como rede nacional interconectando diversas redes pelo Brasil, teve início, efetivamente em 1991, com a estruturação da RNP como instituição específica para esse fim e veiculada ao MCT.

Somente em 1995 foi possível, por iniciativa do Ministério das Telecomunicações e do Ministério da Ciência e Tecnologia, a abertura da Internet ao setor privado para exploração comercial pela população brasileira. A rede brasileira deixou de ser somente acadêmica, como acontecera em 1994 nos Estados Unidos, e empresas e indivíduos também passaram a usar os serviços da Internet. A RNP ficou responsável pela infraestrutura básica de interconexão em nível nacional, tendo controle do *backbone*, que representa a via principal de interconexão entre os diversos pontos de tráfego existentes pelo país.

Por fim, ressalte-se que, com a grande difusão de dispositivos móveis no país, somado ao fato de que mais da metade dos domicílios brasileiros possuem computadores, estima-se que mais da metade da população brasileira possuiu acesso à internet, segundo dados coletados pela Pesquisa Brasileira de Mídia em 2015.

1.1.3 – Conceitos importantes

Quando se cuida de analisar a Internet e todas as circunstâncias a ela relacionadas, alguns conceitos se mostram importantes. Abaixo serão apontados alguns, sem a pretensão, obviamente, de exaurir o tema, cuja vastidão demandaria uma análise muito mais profunda.

1.1.3.1 – **Internet**:

É uma rede mundial de computadores ou terminais ligados

entre si, que tem em comum um conjunto de protocolos e serviços, de forma que os usuários conectados possam usufruir de serviços de informação e comunicação de alcance mundial através de linhas telefônicas comuns (as antigas linhas discadas que têm sido substituídas por acessos em banda larga), linhas de comunicação privadas (ou linhas de dados dedicadas alugadas por empresas com grande volume de dados), satélites e outros serviços de telecomunicações.

1.1.3.2 – CERT.br[6]

É o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet Brasileira.

Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo coordenação e o apoio no processo de respostas a incidentes.

Suas principais atividades são:

a) Tratamento de Incidentes:

   1. Dar suporte ao processo de recuperação e análise de ataques e de sistemas comprometidos;
   2. Estabelecer um trabalho colaborativo com outras entidades, como outros Grupos de Segurança e Resposta a Incidentes, empresas, universidades, provedores de acesso e serviços Internet e backbones;
   3. Manter estatísticas públicas dos incidentes tratados e das reclamações de spam recebidas.

b) Treinamento e Conscientização:

   1. Oferecer treinamentos na área de tratamento de

[6] http://www.cert.br/sobre/

incidentes de segurança, especialmente para membros de Grupos de Segurança e Resposta a Incidentes e para instituições que estejam criando seu próprio grupo;

2. Desenvolver documentação de apoio para administradores de redes Internet e usuários;

3. Realizar reuniões com setores diversos da Internet no Brasil, de modo a articular a cooperação e implantação de boas práticas de segurança.

c) Análise de Tendências de Ataques:

1. Aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro, através da manutenção de uma rede de honeypots distribuídos em diversas redes do país;

2. Obter, através de honeypots de baixa interatividade, dados sobre o abuso da infraestrutura de redes conectadas à Internet para envio de spam.

1.1.3.3 – *Honeypots*

Honeypot é um recurso computacional de segurança desejado a ser sondado, atacado ou comprometido[7]. Consiste em um sistema que se mostre vulnerável, propositalmente, com o objetivo de atrair e monitorar os invasores. Em outras palavras, é um sistema criado para ser uma espécie de armadilha para os criminosos virtuais.

1.1.3.4 – Engenharia Social

[7] http://www.cert-rs.tche.br/index.php/honeypots

No contexto de segurança da informação, a engenharia social, ciência inserida no escopo das relações humanas, é um campo muito explorado por autores de crimes cibernéticos para preparar seus ataques. É utilizada quando os sistemas computacionais são praticamente fechados e seguros, a exemplo dos sistemas bancários, nos quais a falha mais possível de ser explorada é a humana.

Além de outros subterfúgios, é muito utilizada a manipulação psicológica de pessoas para que executem determinadas ações ou para que se divulguem para o criminoso dados confidenciais. Por isso, considera-se a engenharia social com um tipo não técnico de intrusão que depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança.

1.1.3.5 – Códigos Maliciosos[8]

Códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em computadores. Algumas das diversas maneiras de como os códigos maliciosos podem infectar ou comprometer um computador são:

a) pela exploração de vulnerabilidades existentes nos programas instalados;

b) pela auto-execução de mídias removíveis infectadas, como pen-drives;

c) pelo acesso a páginas Web maliciosas, utilizando navegadores vulneráveis;

d) pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;

e) pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias

[8] http://cartilha.cert.br/malware/

removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.

Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disso, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de spam.

1.1.3.6 – *Worm*

Worm é um programa capaz de se propagar automaticamente através de redes de computadores, enviando cópias de si mesmo de computador para computador. Esses programas são capazes, depois de se instalarem na máquina hospedeira, de gravar áudio do microfone, de capturar telas (*screenshots)*, de capturar toques do teclado e de enviar toda informação capturada para servidores do seu criador.

Para se ter uma noção da potencialidade ofensiva da utilização desses programas, tem-se notícia da atuação do *worm* denominado de *Flame*, cujo objetivo principal era alterar a atividade de equipamento de controle de usinas nucleares no Irã, que se alastrou por equipamentos computacionais pelo Oriente Médio, tendo gerado temor na comunidade internacional pela possibilidade da infecção alcançar a Europa[9].

1.1.3.7 – *Spyware*

Spyware é um programa que objetiva observar e roubar

[9] http://www1.folha.uol.com.br/fsp/ilustrissima/57291-guerra-ciberespacial.shtml

informações de uma máquina alvo. Depois de instalado na máquina hospedeira, ele recolhe informações sobre o usuário, seus costumes na Internet, transmitindo essas informações a uma entidade externa na Internet, sem o conhecimento e consentimento do usuário.

1.1.3.8 – Cavalo de Troia

O arquivo malicioso denominado de *trojan horse* (cavalo de Troia) serve para possibilitar a abertura de uma porta na máquina alvo, de forma que seja possível acessá-la de forma remota, a fim de se obter dados confidenciais da vítima e enviá-los para o criminoso.

Normalmente configura o primeiro estágio de infecção do dispositivo alvo, mantendo-se ocultos enquanto baixam e instalam ameaças mais robustas na unidade computacional hospedeira. Podem ser escondidos em arquivos de música, mensagens de e-mails, programas legítimos, etc.

1.1.3.9 – *Botnets*

Os *botnets* são computadores infectados por arquivos maliciosos que possibilitam ao criminoso, de forma remota, realizar qualquer atividade com o computador da vítima. Eles exploram vulnerabilidades ou falhas na configuração do sistema operacional ou de seus softwares.

1.1.3.10 – *Backdoor*

O *backdoor* (“porta dos fundos”), é um tipo de programa que, ao ser instalado no computador, deixa uma “porta dos fundos” aberta, ou seja, deixa o computador vulnerável para ataques ou invasões. Após instalados, permitem que um computador seja totalmente controlado remotamente, possibilitando ao invasor ler os arquivos, e-mails, obter as senhas, apagar arquivos, conectar, via rede, outros dispositivos aos quais a máquina hospedeira tenha acesso, executar programas, etc.

1.1.3.11 – *Hoax*

Hoax em inglês significa embuste ou farsa. É um conjunto de falsas histórias elaboradas com o objetivo de enganar as pessoas. A definição mais precisa é de que o hoax seja um vírus social, que utiliza da boa-fé do usuário para inundar o tráfico da Internet com informações desnecessárias.

Normalmente, os hoaxes exploram o lado emocional das pessoas, por meio da utilização de conteúdo apelativo. Por exemplo: é comum as mensagens mostrarem fotos de adultos ou crianças acidentadas ou sofrendo de doenças graves[10].

1.1.3.12 – *Deface*

A palavra *deface* oriunda do inglês (defacing) e, no âmbito dos crimes cibernéticos, é utilizada para caracterizar aqueles que desfiguram sites ou perfis de redes sociais. Os defacers são semelhantes a pichadores, mas suas atividades não são realizadas em muros e, sim, em sites, blogs e outros meios.

1.1.3.13 – *Keylogger*

O *Keylogger* é um aplicativo ou dispositivo utilizado para monitorar todas as entradas do teclado da máquina hospedeira, ou seja, realiza a monitoração das informações digitadas pelo usuário do computador, como senhas, nome de usuário, etc.

1.1.3.14 – *Sniffer*

Os *sniffers* possuem a finalidade de monitorar todo o tráfego da rede, de modo que todos os dados transmitidos por ela possam ser interceptados e analisados. *Sniffers* são úteis para o gerenciamento de rede, mas nas mãos de hackers permitem roubar senhas e outras informações sigilosas.

[10] http://www.ufpa.br/dicas/net1/spa-hoax.htm

1.1.3.15 – Phishing

O *phishing* (ao invés de fishing - pescaria) é o procedimento destinado a ludibriar o usuário de modo a obter dados pessoais, geralmente via e-mail, para fins de perpetuar outros delitos. Um cenário comum desse procedimento é a criação, por parte do criminoso, de uma página Web falsa projetada para ser idêntica (por isso phishing) à página Web de uma instituição financeira (banco, empresa de cartão de crédito, etc.).

Após, o autor envia e-mails com algum conteúdo que chame a atenção da vitima, levando-a acessar o link que a direcione para a página falsa sendo, portanto, fisgado. Uma vez que a vítima acessa a página falsa e tenta realizar o acesso, com o seu código de usuário e senha, esses dados são automaticamente redirecionados para o criminoso. De posse desses dados, o infrator consegue acessar a conta bancária da vítima.

1.1.3.16 – *Denail of Service* (DoS - Ataque de negação de serviço)

O ataque de Negação de Serviço tem como objetivo interromper atividades legítimas por meio de ataques múltiplos pelo envio de um grande número de mensagens esgotando os recursos da vítima, como CPU, memória, banda, etc.

Todavia, esses ataques que se utilizam basicamente de força bruta, não são um fim em si mesmo. Os primeiros ataques de negação de serviço eram feitos por hackers apenas para provar que a segurança de um website nunca era robusta o suficiente para impedir de ser quebrada, e, a partir disso, buscar ser reconhecido por sua eficiência em interromper serviços na internet. Também, os ataques de negação de serviço, em sua gênese, eram utilizados com finalidade política e de extorsão pela cobrança de proteção contra outros ataques.

1.1.3.17 – *Hacking*

Hacking envolve a tentativa de quebrar a segurança de um sistema, objetivando ganhar acesso não autorizado a um determinado sistema computacional. Há inúmeras maneiras para se atingir esse objetivo, incluindo métodos bastante sofisticados que necessitam de alto conhecimento computacional para exploração de falhas existentes no sistema operacional da unidade computacional alvo. Seja qual for o método, uma vez garantido o acesso, o atacante tem acesso a todos os dados computacionais disponíveis no sistema acessado.

1.1.3.18 – Quebra de Senha

O quebrador (ou *cracker*) de senha é um programa usado pelo invasor para descobrir uma senha do sistema. O método mais comum consiste em testar sucessivamente as palavras de um dicionário até encontrar a senha correta.

1.1.3.19 – *WikiLeaks*

WikiLeaks é uma organização transnacional sem fins lucrativos, sediada na Suécia, que publica, em sua página, postagens de fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas, sobre assuntos sensíveis

1.1.3.20 – *Mail Bomb*

É a técnica de inundar um computador com mensagens eletrônicas. Em geral, o agressor usa um *script* para gerar um fluxo contínuo de mensagens e abarrotar a caixa postal de alguém. A sobrecarga tende a provocar negação de serviço no servidor de e-mail.

1.1.3.21 – Deep Web

Assim como o ARPANET, a internet profunda é derivada de aplicações desenvolvidas inicialmente para o âmbito militar. Suscintamente, a

deep web é a zona da internet em que os sites, fóruns e comunidades não podem ser detectados pelos tradicionais mecanismos de busca (como o Google e o Bing, por exemplo). Para se acessar a deep web são necessários sistemas operacionais e programas específicos que acessam servidores dedicados que funcionam como porta de entrada para esses domínios não indexados pelos sistemas abertos.

1.2 – CONSIDERAÇÕES GERAIS SOBRE OS CRIMES CIBERNÉTICOS

1.2.1 – Conceito de crime cibernético

Inicialmente, insta consignar que a expressão crimes cibernéticos não é adotada de maneira uniforme pela doutrina. De fato, apenas a título de exemplo, as seguintes nomenclaturas podem ser encontradas: “crimes informáticos”, “crimes da era da informação”, “crimes mediante computadores”, “cibercrimes”, “crimes de computador”, “crimes eletrônicos”, “crimes tecnológicos”, “crimes digitais”, “crimes high-tech”, “tecnocrimes”, “netcrimes”, “crimes virtuais”, “crimes da tecnologia da informação” e até mesmo “e-crimes”[11]. No presente relatório, portanto, alguns desses termos podem ser utilizados como sinônimos.

Os estudos realizados até o momento se concentram em dividir os crimes cibernéticos em puros, mistos e comuns.

O **crime virtual puro** seria toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas. Em contrapartida, podem ser considerados **crimes virtuais mistos** aqueles em que o uso de meios computacionais é condição necessária para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático. Por fim, o **crime virtual comum** seria aquele em que se utiliza da Internet apenas como instrumento para a realização do delito já tipificado pela lei penal[12].

[11] SYDOW, Spencer Toth. Crimes informáticos e suas vítimas. 2. ed. São Paulo: Saraiva, 2015, p. 55-56
[12] FIORILLO, Celso Antonio Pacheco. Crimes no meio ambiente digital. São Paulo: Saraiva, 2013, pgs. 140 a 145.

Ou seja:

a) Os **crimes virtuais puros** englobam toda e qualquer conduta ilícita cujo objetivo seja a violação da integridade física ou lógica do sistema computacional, isto é, tem como finalidade atacar o software (programa), hardware (componente físico do computador, tais como: CPU, monitor, teclado, circuito), dados, sistemas e meios de armazenamentos, etc;

b) Os **crimes virtuais mistos** são as condutas em que a utilização de meios computacionais é condição necessária para a efetivação da conduta, embora o bem jurídico lesado seja diverso do informático, tais como a transferência ilícita de valores em uma "*homebanking*" ou a prática de "*salemislacing*" (retirada diárias de pequenas quantias em milhares de contas, também conhecida como retirada de saldo).

c) Os **crimes virtuais comuns** são aqueles em que os dispositivos computacionais são utilizados apenas como instrumento para a realização de um delito já tipificado pela lei penal, constituindo-se em apenas mais um meio de execução desses delitos, tal como ocorre nos seguintes crimes, já tipificados pela lei penal: o estelionato (art. 171 do CP), a ameaça (art. 147 do CP - Código Penal), os crimes contra a honra (arts. 138 a 140 do CP), a veiculação de pornográfica infantil (art. 241-A do Estatuto da Criança e do Adolescente – Lei nº 8.069/90), o crime de violação ao direito autoral (art. 184 do CP), entre outros.

Com base nos dados do relatório "*Subindo na Hierarquia: O Submundo Cibercriminoso Brasileiro em 2015*", da *Trend Micro*,[13] empresa atuante em segurança na internet, observa-se que é conveniente analisar o assunto sob duas outras dimensões: a dos tipos de participantes e a dos tipos de produtos disponíveis.

Os participantes podem ser divididos em dois grupos: o dos

[13] Relatório disponível em: http://www.trendmicro.com.br/cloud-content/br/pdfs/business/submundo-cibercrime-brasil-2015.pdf, acessado em 25/2/16.

desenvolvedores e o dos **operadores**. Desenvolvedores são criminosos que se dedicam propriamente à construção das ferramentas computacionais utilizadas para a prática de ilícitos no ciberespaço. Em geral esses criminosos vendem ou alugam suas ferramentas para o grupo dos operadores utilizando a própria internet, por vezes se valendo até mesmo de mídias sociais como o *Facebook* para divulgar seus "serviços" e "produtos". Já os operadores são aqueles que utilizam as ferramentas computacionais para o efetivo cometimento dos crimes cibernéticos. Neste ponto, cumpre mencionar que, tipicamente, uma investigação policial bem-sucedida redunda no desbaratamento de um grupo de operadores de crimes cibernéticos, sendo muito raro que se consiga chegar aos desenvolvedores das ferramentas.

Com relação aos produtos disponíveis aos operadores, verifica-se que a quantidade, a variedade e a diversidade de ofertas aumenta rapidamente, com inovações que demonstram uma crescente ousadia dos participantes desse submundo. Além dos já bem-conhecidos cavalos de tróia, *spyware*, *malware*, *sniffers* e *keyloggers*, já descritos anteriormente, há de se destacar, também, a existência mais recente dos *ransomware* e dos *crypters*. Os *ransomware* são ferramentas utilizadas para invadir um computador e criptografar arquivos possivelmente importantes ou valiosos gravados no disco rígido, impedindo o uso por parte do agredido. Na sequência, o invasor entra em contato com a vítima, solicitando o pagamento de algum valor, a título de "resgate", para que os arquivos sejam descriptografados. Casos notórios recentes aconteceram no País com Prefeituras e empresas, conforme noticiado pela imprensa.

Já os *crypters* são ferramentas utilizadas para dificultar a detecção e o bloqueio de algum programa malicioso, visando assim superar as barreiras de proteção por ventura existentes no sistema que se pretende invadir.

Chama ainda atenção a oferta cada vez mais recorrente na *web* de cursos destinados ao treinamento de novos desenvolvedores e operadores de cibercrimes. São cursos destinados a ensinar como utilizar *crypters*, como realizar o furto de dados e a clonagem de cartões de crédito, conhecido como *carding*, e como viabilizar a aprovação de transações de cartões de crédito clonados.

Por fim, está também fartamente disponível na internet uma gama de serviços para aqueles que pretendem se beneficiar indevidamente da atividade praticada pelos operadores do cibercrime. São ofertas de criação de

documentos ou certificados de conclusão de cursos falsos, venda de dinheiro falso e prestação de serviço de modificação ilegal da velocidade de conexão à internet provida pelas prestadoras de telecomunicações.

1.2.2 – Crimes cibernéticos na legislação brasileira

Neste tópico, apontaremos, de forma breve, os crimes cibernéticos tipificados na legislação brasileira. Priorizaremos os **crimes virtuais puros** e os **crimes virtuais mistos**. Afinal, nos crimes virtuais comuns, os dispositivos computacionais são utilizados apenas como instrumento para a realização de um delito já tipificado pela lei penal, constituindo-se em apenas mais um meio de execução desses delitos (o elemento informático, nesses delitos, é meramente "acidental"). Em tese, qualquer crime pode ser um crime virtual comum.

Alguns dos crimes virtuais puros e os crimes virtuais mistos previstos em nosso ordenamento jurídico são os seguintes:

a) Art. 10 da Lei nº 9.296/96: é crime, punível com reclusão de 2 a 4 anos e multa, "*realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei*";

b) Art. 313-A, do Código Penal: constitui crime, punível com reclusão de 2 a 12 anos e multa, "*inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano*";

c) Art. 313-B, do Código Penal: constitui crime, punível com reclusão de 3 meses a 2 anos e multa, "*modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação*

de autoridade competente";

d) Art. 12 da Lei nº 9.609/98, que tipifica o crime de violação de direito de autoral de programa de computador, aplicando-se penas que variam de seis meses a quatro anos, e multa;

e) Art. 2º, inciso V, da Lei nº 8.137/90: constitui crime contra a ordem tributária, punível com detenção de 6 meses a 2 anos e multa, "*utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública*";

f) Art. 72 da Lei nº 9.504/97: constituem crimes, puníveis com reclusão, de 5 a 10 anos, "*obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos*", "*desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral*", ou "*causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes*";

g) Art. 154-A do Código Penal: tipifica a conduta de invasão de dispositivo informático (Lei "*Carolina Dieckmann*").

h) Art. 266, § 1º, do Código Penal: constitui crime, punível com a pena de detenção, de um a três anos, e multa, interromper serviço telemático.

1.2.3 – Competência para apuração e julgamento dos

crimes cibernéticos

O Código de Processo Penal brasileiro estabelece, em seu art. 69, os critérios de determinação de competência para processamento e julgamento de atos criminosos:

> Art. 69. Determinará a competência jurisdicional:
>
> I - o lugar da infração:
>
> II - o domicílio ou residência do réu;
>
> III - a natureza da infração;
>
> IV - a distribuição;
>
> V - a conexão ou continência;
>
> VI - a prevenção;
>
> VII - a prerrogativa de função.

Por sua vez, o art. 109 da Constituição Federal cuida da competência da justiça federal em razão da matéria, assim dispondo:

> Art. 109. Aos juízes federais compete processar e julgar:
>
> I - as causas em que a União, entidade autárquica ou empresa pública federal forem interessadas na condição de autoras, rés, assistentes ou oponentes, exceto as de falência, as de acidentes de trabalho e as sujeitas à Justiça Eleitoral e à Justiça do Trabalho;
>
> II - as causas entre Estado estrangeiro ou organismo internacional e Município ou pessoa domiciliada ou residente no País;
>
> III - as causas fundadas em tratado ou contrato da União com Estado estrangeiro ou organismo internacional;
>
> IV - os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral;
>
> V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;
>
> V-A as causas relativas a direitos humanos a que se refere o § 5º deste artigo;
>
> VI - os crimes contra a organização do trabalho e, nos casos determinados por lei, contra o sistema financeiro e a ordem econômico-financeira;
>
> VII - os *habeas corpus*, em matéria criminal de sua competência ou quando o constrangimento provier de autoridade cujos atos não estejam diretamente sujeitos a outra jurisdição;

> VIII - os mandados de segurança e os *habeas data* contra ato de autoridade federal, excetuados os casos de competência dos tribunais federais;
>
> IX - os crimes cometidos a bordo de navios ou aeronaves, ressalvada a competência da Justiça Militar;
>
> X - os crimes de ingresso ou permanência irregular de estrangeiro, a execução de carta rogatória, após o "exequatur", e de sentença estrangeira, após a homologação, as causas referentes à nacionalidade, inclusive a respectiva opção, e à naturalização;
>
> XI - a disputa sobre direitos indígenas.
>
> § 1º As causas em que a União for autora serão aforadas na seção judiciária onde tiver domicílio a outra parte.
>
> § 2º As causas intentadas contra a União poderão ser aforadas na seção judiciária em que for domiciliado o autor, naquela onde houver ocorrido o ato ou fato que deu origem à demanda ou onde esteja situada a coisa, ou, ainda, no Distrito Federal.
>
> § 3º Serão processadas e julgadas na justiça estadual, no foro do domicílio dos segurados ou beneficiários, as causas em que forem parte instituição de previdência social e segurado, sempre que a comarca não seja sede de vara do juízo federal, e, se verificada essa condição, a lei poderá permitir que outras causas sejam também processadas e julgadas pela justiça estadual.
>
> § 4º Na hipótese do parágrafo anterior, o recurso cabível será sempre para o Tribunal Regional Federal na área de jurisdição do juiz de primeiro grau.
>
> § 5º Nas hipóteses de grave violação de direitos humanos, o Procurador-Geral da República, com a finalidade de assegurar o cumprimento de obrigações decorrentes de tratados internacionais de direitos humanos dos quais o Brasil seja parte, poderá suscitar, perante o Superior Tribunal de Justiça, em qualquer fase do inquérito ou processo, incidente de deslocamento de competência para a Justiça Federal.

Esses dispositivos aplicam-se, também, aos crimes cibernéticos, tendo em vista que não existe disposição em contrário em nosso ordenamento jurídico.

Ou seja, se o crime cibernético for cometido, por exemplo, em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, a competência para o seu processamento e julgamento será da justiça federal (art. 109, IV, da CF). Caso o crime não se enquadre em nenhuma das hipóteses de competência da justiça federal ou especializada, a competência será da justiça comum estadual.

Quanto à competência territorial, os problemas são maiores. Afinal, segundo dispõe o art. 6º do Código Penal, "*considera-se praticado o crime*

no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado". O problema é que, no caso dos crimes virtuais, os atos podem ser praticados em vários locais, o que dificulta bastante a delimitação da competência.

Os tribunais brasileiros têm entendido, por exemplo, que a competência territorial, nesses casos, se firma pelo local em que se localiza o provedor do site de onde partiu o ato delituoso, o que pode dificultar a produção probatória (afinal, o provedor se localizar em local diverso da residência do réu ou da vítima).

Outra questão que também merece análise diz respeito à competência para investigar esses atos criminosos (se da Polícia Federal ou se da Polícia Civil). E é preciso esclarecer, desde já, que não há uma relação de absoluta congruência entre as atribuições de polícia investigativa da Polícia Federal e as hipóteses de competência criminal da Justiça Federal. Ou seja, há casos em que a Polícia Federal é a competente para investigar infrações penais de competência da Justiça Estadual.

Isso porque, nos termos do art. 144, § 1º, inciso I, da Constituição Federal, compete à Polícia Federal apurar "*infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei*". A lei que disciplina essas infrações que devem ser apuradas pela Polícia Federal, quando houver repercussão interestadual ou internacional que exija repressão uniforme, é a Lei nº 10.446, de 2002. Dentre esses crimes, porém, não se encontram, de forma específica, os crimes cibernéticos.

Daí se conclui que aos crimes virtuais, também no caso de delimitação de competência investigativa, se aplicam as regras gerais.

1.3 – PANORAMA DA SEGURANÇA PÚBLICA NO COMBATE À CRIMINALIDADE CIBERNÉTICA

Com a veloz ampliação do acesso à internet no Brasil, ocorrido a partir da década de 1990, os órgãos policiais passaram a se dedicar,

também, ao combate aos chamados crimes cibernéticos impróprios, isto é, crimes comuns cometidos mediante um novo instrumento, a internet. O surgimento da tecnologia de telefonia celular, mais ou menos à mesma época, propiciou o uso dessas novas plataformas para o cometimento de crimes.

Assim surgiram e se aperfeiçoaram ao longo do tempo as fraudes financeiras, campeãs dos crimes cibernéticos, como o estelionato, o furto mediante fraude e a extorsão, todas cometidas no ambiente virtual. Entretanto, tratavam-se de novos crimes apenas, não necessariamente se vislumbrava uma nova onda de gênero criminal que alterasse os paradigmas preventivo-repressivos.

Logo, porém, o avanço tecnológico – sempre um passo à frente dos órgãos de repressão criminal – permitiu a atuação de delinquentes no ambiente virtual, cada vez mais protegidos pelo anonimato e impessoalidade que a internet permite. Com o surgimento dos smartphones, o compartilhamento de dados digitais como imagens e vídeos passou a acompanhar o criminoso onde quer que ele estivesse, não mais apenas à frente de um *desktop*.

Não tardou, portanto, para que os órgãos policiais instituíssem unidades ou equipes especializadas no combate a tais crimes, notadamente no âmbito da investigação. Infelizmente algumas dessas unidades foram desativadas, na contramão do incremento dos crimes cibernéticos, mas outras lograram sucesso com a agregação de equipamentos de ponta e incremento dos recursos humanos, tanto quantitativa como qualitativamente.

O surgimento ou especialização de espécies delituosas, contudo, sejam crimes cibernéticos próprios ou impróprios, apontam para uma demanda maior aos órgãos policiais e, consequentemente, resposta adequada à delinquência virtual.

É o caso dos crimes mais lucrativos do mundo, como o narcotráfico, o tráfico de armas e o tráfico de pessoas, pelo impacto socioeconômico que geram nas sociedades, seja em relação às políticas públicas, seja no tocante à situação das vítimas, diretas e indiretas.

No dizer de Cerqueira e Rocha (2015),

A instantaneidade das ações e a possibilidade de assincronia no

> uso da internet atenua os graus de segurança e certeza nas transações nela realizadas, o que gera a brecha (*breach*) para a atuação dos delinquentes. Cabe à norma de natureza penal, portanto, dispor a respeito dessas vulnerabilidades, de sorte a proteger os objetos jurídicos que o Estado considera sujeitos à tutela legal.[14]

Novos parâmetros regulatórios visando a disciplinar a nova e já conturbada relação entre provedores e usuários dos serviços de internet – ambiente onde ocorrem os crimes cibernéticos – foi propiciado por uma norma de natureza não penal, mas administrativa, não obstante seus princípios se aplicarem ao esforço de repressão a mencionados crimes.

Trata-se do Marco Civil da Internet (MCI), instituído pela Lei n. 12.965, de 23 de abril de 2014[15], que "estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil", sendo considerada uma das leis mais avançadas no tema. Por essa razão vários países têm se inspirado na norma brasileira para editar suas próprias leis sobre o assunto. Resultado de intensa discussão parlamentar, com a participação direta da sociedade por meios dos canais que a própria internet propiciou, o MCI buscou o justo equilíbrio entre os interesses em disputa, variando desde os extremos que propunham estrito controle ou liberdade total.

A nova lei, tendo como fundamento a responsabilidade civil na internet, trouxe garantia da liberdade de expressão, privacidade, intimidade dos usuários e inviolabilidade das comunicações; vedação de divulgação de dados pessoais; obrigatoriedade de guarda dos registros de conexão por um ano e proibição de guarda dos registros de navegação; obrigação de retirada dos conteúdos infringentes; e garantia de neutralidade.

Antes da edição do MCI outras normas inovaram no ordenamento jurídico visando a reprimir os crimes cibernéticos. A primeira delas foi a Lei n. 9.609, de 19 de fevereiro de 1998, que dispusera sobre a proteção da

---

[14] CERQUEIRA, Sílvio Castro; ROCHA, Claudionor. **Crimes cibernéticos**: desafios da investigação. *Cadernos Aslegis*, 20 anos da Internet no Brasil (Parte II). Brasília: Associação dos Consultores Legislativos e de Orçamento e Fiscalização Financeira da Câmara dos Deputados, n. 49, maio/ago 2013. Disponível em <http://www.aslegis.org.br/ files/aslegis49_baixa.pdf>. Acesso em 30 nov 2015.
[15] Toda a legislação mencionada está disponível no site governamental <www.planalto.gov.br>.

propriedade intelectual de programa de computador e sua comercialização no país (contra a pirataria de *softwares*). A Lei n. 9.983, de 14 de julho de 2000, alterou o Código Penal, acrescentando os arts. 313-A e 313-B, acerca de crimes previdenciários cometidos por computador (inserção de dados falsos em sistema de informações; modificação ou alteração não autorizada de sistema de informações). Depois, a Lei n. 11.829, de 25 de novembro de 2008, criminalizou condutas relacionadas à pornografia envolvendo crianças e adolescentes, mediante a utilização de recursos de alta tecnologia como meio propiciador da conduta, incluindo os arts. 241-A e 241-B no Estatuto da Criança e do Adolescente (ECA), Lei n. 8.069, de 13 de julho de 1990.

O inciso III do § 3º do art. 20 da Lei n. 7.716, de 5 de janeiro de 1989 (Lei Anti-Racismo) foi incluído pela Lei n. 12.288, de 20 de julho de 2010 (Estatuto da Igualdade Racial), facultando ao juiz interditar as respectivas mensagens ou páginas de informação na rede mundial de computadores.

Em termos de facilitação da investigação de crimes cibernéticos, a Lei n. 12.735, de 30 de novembro de 2012 (Lei Azeredo), alterou o Código Penal, o Decreto-Lei n. 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei n. 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. Seu projeto inicial, PL 84/1999[16], redigido sob forte influência da Convenção de Budapeste, foi apelidado de 'AI-5 digital'.

A Lei n. 12.737, de 30 de novembro de 2012, que "dispõe sobre a tipificação criminal de delitos informáticos", alterou o Código Penal, incluindo os arts. 154-A e 154-B e dando nova redação aos arts. 266 e 298. Essa norma, conhecida como Lei Carolina Dieckmann, foi aprovada em contexto de invasão da privacidade de conhecida atriz brasileira. O núcleo do tipo principal é 'invadir' dispositivo informático alheio, o que gerou críticas pois a invasão pressuporia alguma ação agressiva, ao contrário de somente 'acessar', por exemplo.

por fim, a Lei n. 12.894, de 17 de dezembro de 2013, que

[16] Todas as proposições mencionadas estão disponíveis no Portal da Câmara dos Deputados: <www2.camara.leg.br>.

acrescenta inciso V ao art. 1º da Lei n. 10.446, de 8 de maio de 2002, previu a atribuição da polícia federal para apurar os crimes de falsificação, corrupção e adulteração de medicamentos, assim como sua venda, inclusive pela internet, quando houver repercussão interestadual ou internacional.

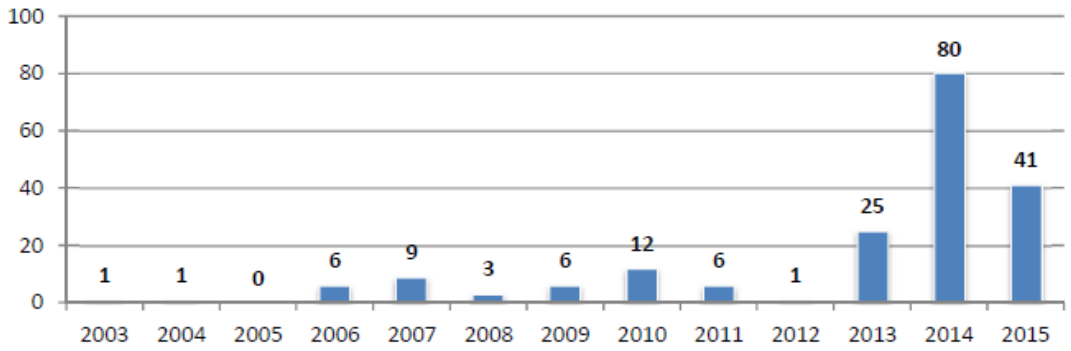
Apesar desse panorama esparso de leis em voga no País, discute-se acerca da necessidade de uma lei que trate apenas dos crimes cibernéticos, ao tempo em que novos órgãos e entidades surgem para disciplinar o sistema, diante de novas espécies delinquenciaisO uso da chamada *deep web* ou *dark net* e novas ameaças, como o terrorismo virtual, reforçam esses argumentos.

1.3.1 – Papel da Polícia Federal

A Portaria n. 2.877, de 30 de dezembro de 2011, que aprovou o Regimento Interno do Departamento de Polícia Federal, criou, no âmbito da Diretoria de Investigação e Combate ao Crime Organizado (Dicor) e da sua Coordenação-Geral de Polícia Fazendária (CGPFAZ), o Serviço de Repressão a Crimes Cibernéticos (SRCC). Embora a DPF tenha a competência de reprimir vários crimes cibernéticos, a corporação dispõe apenas de um serviço, o SRCC, em sua estrutura orgânica. Além do mais e em que pese a polícia federal se utilize de equipamentos sofisticados, muito embora os delinquentes estejam sempre um passo à frente, o efetivo é escasso em relação a esse tipo de demanda.

Tendo em vista que compete à polícia federal apurar os crimes mais rentáveis do mundo, como o narcotráfico, o tráfico de armas e o tráfico de pessoas, os quais utilizam profusamente o ambiente cibernético, é vital que o órgão seja aquinhoado com recursos humanos e materiais suficientemente adequados para fazer face á nova criminalidade virtual. Desafortunadamente, como foi visto nas diversas Audiências Públicas realizadas pela CPI, a estrutura do Departamento é deficitária.

Segundo informações da Polícia Federal, o quantitativo de Operações Especiais do SRCC realizadas entre 2003 e setembro de 2015 pode ser representado no seguinte gráfico.



Fonte: QOPs, 08/10/2015

1.3.2 – Papel da Polícia Civil

O art. 4º da mencionada Lei n. 12.735/2012 (Lei Azeredo) dispõe que "os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado". Entretanto o dispositivo é propositivo, não obrigando os entes federados a cumpri-lo. O próprio decreto regulamentar nele previsto sequer foi editado.

A própria constitucionalidade desse dispositivo é questionável, vez que impõe despesas aos Estados, por meio de lei ordinária, afetando, assim, o pacto federativo que confere o poder de legislar internamente aos entes federados, segundo os princípios da autonomia política, normativa, financeira e administrativa.

O projeto original tipificava os crimes digitais e previa que os dados dos usuários deveriam ser guardados por três anos para fins de investigação criminal. Como visto, o MCI obriga a preservação dos dados por apenas um ano, o que é considerado insuficiente pelos órgãos de repressão, embora seguindo tendência mundial, pois a maioria dos países prevêm esse prazo um ano, alguns em seis meses e outros não estabelecem qualquer prazo.

No âmbito das Unidades da Federação, a Lei n. 15.026, de 20 de junho de 2013, de Pernambuco, cria a Delegacia de Polícia de Repressão

aos Crimes Cibernéticos – DPCRCI (art. 7º), com competência para: prevenir e reprimir, com exclusividade no Município do Recife, a prática de crimes tecnológicos, virtuais e eletrônicos, que envolvam delitos praticados com o uso da tecnologia, sobretudo através da internet; e apurar com uniformidade de ação ou maior especialização, concorrentemente com a Delegacia da Circunscrição do local do fato, no Estado de Pernambuco, a prática de crimes de que trata a alínea 'a' deste inciso.

Outro exemplo de legislação estadual é o Decreto n. 44.453, de 25 de maio de 2006, do Rio Grande do Sul, o qual estabelece que "a Delegacia de Polícia de Repressão aos Crimes Informáticos – DRCI, do DEIC, compete investigar os crimes cometidos por meios eletrônicos, telemáticos ou através da Internet, cuja abrangência, incidência ou repercussão exijam investigação especializada" (art. 247).

No Rio de Janeiro, o Decreto n. 26.209 de 19 de abril de 2000, criou a Delegacia de Repressão aos Crimes de Informática – DRCI.

Há ainda outras unidades da federação que possuem estruturas específicas para o combate ao crime cibernético, porém, mesmo naquelas que possuem unidades especializadas, há um histórico de infraestrutura deficitária, como visto nos inúmeros depoimentos realizados na CPI.

1.3.3 – Papel do Exército

O Ministério da Defesa editou a Portaria Normativa n. 3.389/MD, de 21 de dezembro de 2012, que "dispõe sobre a Política Cibernética de Defesa", a qual prevê, dentre seus objetivos:.

- colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR);

- conceber e implantar o Sistema Militar de Defesa Cibernética (SMDC), contando com a participação de militares das FA e civis;

- incluir o conteúdo Defesa Cibernética nos currículos dos cursos, em todos os níveis, no que couber, dos estabelecimentos de ensino do MD.

- implementar metodologia de Gestão de SIC na Defesa, levando em conta a legislação e normas vigentes, as melhores práticas, a Doutrina de Inteligência de Defesa e padrões internacionais de interesse;

- implementar uma infraestrutura de chaves públicas da Defesa (ICP Defesa);

- determinar padrões interoperáveis de criptografia de Defesa em complemento aos das FA;

- criar programas, no âmbito do MD, em parceria com o MCTI, que contemplem a característica dual (emprego civil e militar) das tecnologias de informação e comunicações (TIC) empregadas na área cibernética, para fortalecer o envolvimento do setor industrial nas fases de desenvolvimento dos projetos de interesse do St Ciber;

- colaborar com o órgão da Presidência da República (PR) encarregado da elaboração da Política Nacional de Segurança Cibernética.

O Decreto n. 5.751, de 12 de abril de 2006, aprovou a Estrutura Regimental do Comando do Exército, tendo nele sido instituído, como órgão de assistência direta e imediata ao Comandante do Exército, o Centro de Defesa Cibernética, na redação dada pelo Decreto n. 8.491, de 13 de julho de 2015. Essa iniciativa estava prevista na Estratégia Nacional de Defesa, aprovada pelo Decreto n. 6.703, de 18 de dezembro de 2008.

Compete ao Centro de Defesa Cibernética, nos termos do art. 11-B, incluído pelo referido Decreto n. 8.491/2015:

> I – assessorar o Comandante do Exército e o Ministro de Estado da Defesa nas atividades do setor, formular doutrina e obter e empregar tecnologias;
>
> II – planejar, orientar e controlar as atividades operacionais, doutrinárias e de desenvolvimento das capacidades cibernéticas; e
>
> III – executar atividades de exploração cibernética, em

> conformidade com as políticas e diretrizes do Ministério da Defesa.

O papel do Exército está consubstanciado, portanto, na formulação da Estratégia Nacional de Defesa, segundo os princípios constitucionais da não-intervenção, defesa da paz e solução pacífica dos conflitos. Pressupõe o desenvolvimento de três setores estratégicos: o espacial, a cargo da Aeronáutica; o cibernético, a cargo do Exército; e o nuclear, a cargo da Marinha. Embora prevista constitucionalmente o emprego das Forças Armadas na garantia da lei e da ordem, a vocação não é para desempenhar o papel de polícia. Destarte, as ações do Exército no tocante à defesa cibernética pressupõe, essencialmente, a defesa externa e segurança interna, isto é, a defesa do território na hipótese de agressão externa. Segundo o próprio texto da END,

> As capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar.

Segundo a END, o objetivo síntese das ações estratégicas a serem executadas, no tocante à Segurança Nacional, é contribuir para o incremento do nível de Segurança Nacional. Para tanto, todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional, com particular ênfase sobre os seguintes aspectos:

- o aperfeiçoamento de processos para o gerenciamento de crises;

- a integração de todos os órgãos do Sistema de Inteligência Nacional (SISBIN);

- a prevenção de atos terroristas e de atentados massivos aos Direitos Humanos, bem como a condução de operações contra-terrorismo, a cargo dos Ministérios da Defesa e da Justiça e do Gabinete de Segurança

Institucional da Presidência da República (GSI-PR);

- as medidas para a segurança das áreas de infra-estruturas críticas, incluindo serviços, em especial no que se refere à energia, transporte, água e telecomunicações, a cargo dos Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações, e ao trabalho de coordenação, avaliação, monitoramento e redução de riscos, desempenhado pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR);

- as medidas de defesa química, bacteriológica e nuclear, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, da Saúde, da Integração Nacional, das Minas e Energia e da Ciência e Tecnologia, e do GSI-PR, para as ações de proteção à população e às instalações em território nacional, decorrentes de possíveis efeitos do emprego de armas dessa natureza;

- as ações de defesa civil, a cargo do Ministério da Integração Nacional;

- as ações de segurança pública, a cargo do Ministério da Justiça e dos órgãos de segurança pública estaduais;

- o aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia, e do GSI-PR;

- a execução de estudos para viabilizar a instalação de um centro de pesquisa de doenças tropicais para a região amazônica, a cargo dos Ministérios da Defesa, da Ciência e Tecnologia, da Saúde e órgãos de saúde estaduais e municipais;

- medidas de defesa contra pandemias; e

- o atendimento aos compromissos internacionais relativos à salvaguarda da vida humana no mar e ao tráfego aéreo internacional, a cargo do Ministério da Defesa, por intermédio dos Comandos da Marinha e da Aeronáutica, respectivamente, e do Ministério das Relações Exteriores

Tirante algumas ações estratégicas, atribuídas especificamente à esfera de determinados Órgãos, praticamente todas têm interesse imediato do Exército, como força responsável pela dimensão da defesa cibernética, destacadas em negrito no rol acima.

1.3.4 – Papel do Gabinete de Segurança Institucional

O antigo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) passou a denominar-se Casa Militar, por força da Medida Provisória n. 696, de 2 de outubro de 2015, que "extingue e transforma cargos públicos e altera a Lei nº 10.683, de 28 de maio de 2003, que dispõe sobre a organização da Presidência da República e dos Ministérios". A MP extigue o cargo de Ministro de Estado Chefe do GSI, transformando o órgão na Casa Militar. Subordina a Abin à Secretaria de Governo, a qual passa a atuar, também, a "na prevenção da ocorrência e na articulação do gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional", que era incumbência do GSI/PR.

1.3.5 – Papel da Abin

A Agência Brasileira de Inteligência (Abin) foi criada pela Lei n. 9.883, de 7 de dezembro de 1999, que "institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – Abin, e dá outras providências".

Tal norma previu, em seu art. 6º, acerca do controle da atividade, consubstanciada na edição da Resolução n. 2, de 2013, do Congresso Nacional, que "dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI), comissão permanente do Congresso Nacional, órgão de controle e fiscalização externos da atividade de inteligência, previsto no art. 6º da Lei nº 9.883, de 7 de dezembro de 1999".

A publicação "Desafios Estratégicos para a Segurança e Defesa Cibernética" destaca a importância da Abin nos seguintes termos:

> A Abin é o órgão central do Sistema Brasileiro de Inteligência

(Sisbin), que tem como objetivo estratégico desenvolver atividades de inteligência voltadas para a defesa do Estado democrático de direito, da sociedade, da eficácia do poder público e da soberania nacional.

Dentre suas atribuições, no que interessa especificamente ao Setor Cibernético, destaca-se a de avaliar as ameaças internas e externas à ordem constitucional, entre elas a cibernética.

Conta, em sua estrutura organizacional, com o Centro de Pesquisa e Desenvolvimento de Segurança das Comunicações (Cepesc), que busca promover a pesquisa científica e tecnológica aplicada a projetos de segurança das comunicações.[17]

1.3.6 – Dados sensíveis à Segurança Nacional

No nível das ameaças cibernéticas, pode-se classificá-las da seguinte forma:

- nível 1: crime de baixo nível/individual (hacking);

- nível 2: criminalidade cibernética organizada, explorada por organizações criminosas tradicionais; e

- nível 3: ideológico e extremismo político, incluindo o terrorismo cibernético e de fundo religioso, de que são exemplos atuais as ações do jihadismo do grupo terrorista autodenominado Estado Islâmico.

Ainda segundo a publicação “Desafios Estratégicos para a Segurança e Defesa Cibernética”, as potenciais ameaças cibernéticas no campo da segurança das informações são:

- o bloqueio e desinformação em recursos de informação e telecomunicação;

- ação de guerra ou terrorista contra fluxo de informação em estruturas vitais;

- desestabilização da sociedade por meio da manipulação da consciência da população;

- adoção de doutrinas e políticas, individualmente, pelas nações,

[17] BRASIL. Presidência da República. *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Brasília: Secretaria de Assuntos Estratégicos, 2011, pp. 21-22.

> com respeito à segurança das informações, provocando uma corrida armamentista;
>
> - uso de recursos de TI em detrimento dos direitos humanos e da liberdade de acesso à informação;
>
> - a disseminação generalizada de informação, violando os princípios e as normas da legislação internacional; e
>
> - o desenvolvimento de conceitos e meios por países membros, visando à guerra cibernética.[18]

No Brasil, os assuntos relacionados à Segurança da Informação e das Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas vêm sendo tratados no âmbito do Conselho de Defesa Nacional (CDN) e da Câmara de Relações Exteriores e Defesa Nacional (Creden), do Conselho de Governo, por intermédio da Casa Militar da Presidência da República (ex-GSI/PR). As competências, organização e normas de funcionamento do Conselho de governo e da Creden são disciplinadas pela Lei n. 10.683, de 28 de maio de 2003, que "dispõe sobre a organização da Presidência da República e dos Ministérios" e pelo Decreto n. 4.801, de 6 de agosto de 2003, que "cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo".

Importantes organismos funcionam sob a coordenação da Casa Militar:

- Comitê Gestor de Segurança da Informação;

- Grupo de Trabalho de Segurança das Infraestruturas Críticas, nas áreas de energia, telecomunicações, transportes, suprimento de água e finanças;

- Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação;

- Grupo Técnico de Segurança Cibernética; e

- Grupo Técnico de Criptografia.[19]

---

[18] ALMEIDA, José Eduardo Portella. A tendência mundial para a defesa cibernética. In: BRASIL. Presidência da República. *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Brasília: Secretaria de Assuntos Estratégicos, 2011, pp. 79-102, p. 99.

[19] OLIVEIRA, João Roberto de. Sistema de Segurança e Defesa Cibernética Nacional: abordagem com foco nas atividades relacionadas à Defesa Nacional. In: BRASIL. Presidência da República. *Desafios*

Existe, ainda, a Rede Nacional de Segurança da Informação e Criptografia (Renasic), coordenada pelo Ministério da Defesa, constituída por rede virtual de troca de informações da qual participam pesquisadores, profissionais de entidades públicas e privadas, academia e outros interessados, visando a discutir problemas e soluções práticas de Tecnologia da Informação e Comunicações (TIC) e Segurança da Informação e Comunicações (SIC). (p.120).

No âmbito do Conselho de Governo, o Decreto n. 4.801, de 6 de agosto de 2003, criou a Câmara de Relações Exteriores e Defesa Nacional, com a finalidade de formular políticas públicas e diretrizes de matérias relacionadas com a área das relações exteriores e defesa nacional do Governo Federal, aprovar, promover a articulação e acompanhar a implementação dos programas e ações estabelecidos, no âmbito de ações cujo escopo ultrapasse a competência de um único Ministério, inclusive aquelas pertinentes a segurança cibernética, dentre outras, na redação dada pelo Decreto nº 7.009, de 12 de novembro de 2009.

Outros órgãos afins importantes integram as estruturas da Casa Civil da Presidência da República, do Ministério da Defesa (Comando do Exército) e Ministério da Justiça (Departamento de Polícia Federal).[20]

Por último lembre-se, a propósito, a Lei n. 7.170, de 14 de dezembro de 1983, que "define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências", a qual está praticamente derrogada em face dos novos valores constitucionalmente garantidos, mas ainda é o marco legal que regula a ordem política e social.

1.3.7 – Caso Snowden

O chamado Caso Snowden foi um escândalo de espionagem revelado pelo ex-funcionário da agência americana de inteligência, *Central Intelligence Agency* (CIA), Edward Snowden. O fato de que as agências

Estratégicos para a Segurança e Defesa Cibernética. Brasília: Secretaria de Assuntos Estratégicos, 2011, pp. 105-128, p. 120.

[20] Ibidem.

de inteligência interceptaram mensagens e dados inclusive da presidente Dilma Rousseff e da Petrobras teve como consequência a imposição de regime de urgência na tramitação do Projeto de Lei do Marco Civil da Internet na Câmara dos Deputados, trancando inclusive, a partir de outubro, a votação de qualquer outro projeto na casa legislativa.[21]

Algumas notícias específicas sobre o caso podem trazer melhores esclarecimentos, como os trechos transcritos a seguir.

Notícia publicada no jornal *Correio Braziliense*, de 28/05/2015, seção Opinião, à pág. 15, intitulada "A opinião pública global, o governo americano e Snowden", de autoria de Joaquim Falcão, informa o seguinte:

> O governo de Barack Obama agiu além da lei. O Tribunal de Apelações do Segundo Circuito dos Estados Unidos, no caso ACLU v. Clapper entendeu que o programa de guarda de registros telefônicos da Agência Nacional de Segurança dos Estados Unidos (NSA) foi além do que o *Patriot Act*, lei de proteção contra o terrorismo, passada depois de 11 de setembro, permitia.
>
> A lei não permite que o governo guarde os metadados, os registros de telefones, de milhões de cidadãos americanos que não são objeto de investigação ou que não estão ligados a investigações de terrorismo autorizadas por um tribunal, mesmo que os dados permaneçam secretos.
>
> O governo usou dos poderes que não tinha. Foi além do que permitia a lei e violou a privacidade de milhões de cidadãos americanos. Edward Snowden, nas denúncias sobre abusos nos poderes de investigação do governo, tinha razão. E agora?
>
> (...) A prática das comunidades de segurança nos Estados Unidos ou em qualquer outro país é de não revelar às autoridades que terão que tomar decisões difíceis, nem a fonte, nem o método pelo qual se obteve a informação. O presidente tem que lidar apenas com os fatos. Em cima deles, deve tomar decisões.
>
> Assim, a comunidade de segurança protege o presidente da República de eventuais ilegalidades na fonte e no método de obtenção da informação. Ocorre que, sem a legalidade do método, inexiste Estado de direito. (...)

Outra notícia foi publicada pelo jornal *Estado de São Paulo*, em 23/08/2015, na coluna Internacional, à pág. A17, intitulada "Lei fracassa em impedir EUA de espionarem", de autoria de Jéssica Otoboni*:*

> Segundo especialista americano, NSA continua monitorando registros telefônicos de países aliados

[21] ANDRADE, Simone Caixeta de. Trajetória legal do marco civil. (2014). Disponível em: . Acesso em 19 maio 2015.

> Em junho, o presidente dos Estados Unidos, Barack Obama, assinou a Lei de Liberdade, que limita a coleta de registros telefônicos em massa por parte da Agência de Segurança Nacional (NSA, na sigla em inglês). A partir de então, a agência tinha seis meses para reduzir seu programa de espionagem.
>
> No entanto, segundo Joseph Margulies, professor de direito da Universidade de Cornell, pouca coisa mudou. "Está um pouco mais difícil de coletar alguns dados de cidadãos, mas não houve mudanças significativas", diz.
>
> Em 2013, documentos divulgados por Edward Snowden, ex-funcionário da NSA, e obtidos pelo WikiLeaks revelaram que líderes mundiais foram espionados pelos EUA. Desde então, a agência é responsável pelo abalo nas relações entre americanos e aliados espionados.
>
> Reportagem publicada no dia 15 pelo jornal The New York Times, com base em análise de documentos fornecidos por Snowden, indica que a NSA teve a colaboração, entre 2003 e 2007, da gigante de telecomunicações AT&T. Durante esse período, a AT&T deu à NSA acesso a bilhões de e-mails, rastreados pela rede doméstica. Essa colaboração permitiu que fossem interceptadas todas as comunicações de internet da sede das Nações Unidas, em Nova York, uma cliente da AT&T.
>
> (...) As revelações de Snowden indicaram que os EUA também espionaram as comunicações de milhões de brasileiros e de empresas como a Petrobrás, além da presidente Dilma Rousseff. Em julho, o WikiLeaks revelou que Dilma continuava a ser alvo de interceptações telefônicas. (...)

O episódio demonstra uma dificuldade observada no caso das investigações levadas a efeito no Brasil, que é a sistemática recusa dos provedores de conteúdo em atenderem às requisições das autoridades policiais, sob a alegação de que os dados estariam sediados no país de origem. Tal fato é mais comum no tocante à rede social Facebook, que possui milhões de clientes no Brasil e mundo afora. Os depoimentos à CPI evidenciaram diversos conflitos entre autoridades judiciais e as principais empresas *ponto com*.

1.3.8 – Boas práticas na segurança de dados

A segurança de dados tornou-se um mercado promissor para empresas e técnicos especializados. Muitos livros, revistas e sites temáticos, além de artigos diversos estão disponíveis sobre o assunto. Empresas de segurança privada igualmente

É extremamente importante que a conduta individual não

seja geradora de oportunidades aos delinquentes virtuais. Assim, a chamada prevenção situacional aplicável ao mundo real é perfeitamente amoldável ao ambiente cibernético.

Ao se abordar boas práticas é possível entrevê-las como iniciativas institucionais, de entes públicos ou privados, assim como iniciativas individuais. Nesse caso, a mencionada prevenção situacional ganha vulto, na medida em que cada indivíduo seja responsável por sua segurança *on line.*

Dentre as boas práticas institucionais, vários órgãos públicos e entidades da sociedade civil buscam valorizar iniciativas, como grupos destinados à regulação, formal ou informal do uso da internet, assim como campanhas destinadas à educação dos usuários, especialmente crianças. Outras prováveis boas práticas estão no âmbito das cogitações, dos projetos e até dos sonhos. Assim, podem ser apontados as seguintes instâncias e produtos, existentes ou sugeridos e mencionados durante as audiências realizadas pela CPI, destinados à disciplina da internet e da relação dos usuários com provedores, anunciantes e internautas em geral:

- Grupo Especial de Combate à Pornografia Infantil e aos Crimes de Ódio (GCOP), da Polícia Federal;

- Comitê Interamericano Contra o Terrorismo (CICTE);

- Fórum de Governança da Internet da ONU (IGF);

- Frente Parlamentar de Combate a Crimes na Internet;

- Substituição da versão 4 do *Internet Protocol*, o IPV4, para a versão 6, que é o IPV6;

- Conferir efetividade às disposições das Leis nº 9.613, de 1998, a Lei nº 12.850, de 2013 — a Lei 9.613/98 é a que fala de lavagem de ativos; a Lei 12.850/13, de crime organizado, o próprio Marco Civil da Internet, no sentido da celeridade na investigação;

- Tornar prática inquestionável a requisição de dados

cadastrais pelas autoridades policiais;[22]

- Grupo de Repressão a Crimes Cibernéticos (GRCC);

- Implantar uma estratégia nacional de combate ao crime cibernético nos mesmos moldes da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro — ENCCLA, que cuida da corrupção e da lavagem de dinheiro;

- Reestruturar os órgãos policiais, pois a taxa de elucidação é diretamente proporcional à estrutura de investigação;

- *National Center for Missing & Exploited Children* (NCMEC);

- Childhood Brasil, integrante da *World Childhood Foundation*;

- SaferNet Brasil;

- Expedição Google de Segurança na Internet;

- Campanha *Pense Antes de Compartilhar*;

- PhotoDNA, *Amber Alerts*, botão de silenciar, botão de *report*[23], SpamCop, Abusix;

- Internet sem Vacilo;

- Humaniza Redes;

- Uso de protocolo de segurança aberto e livre;

- Instituir um sistema de identificação civil único (identificação unívoca);

- Utilizar *software* livre;

[22] A Lei nº 12.850, de 2013, por exemplo, no art. 15, diz que a autoridade policial poderá ter o acesso, independentemente de ordem judicial, aos dados cadastrais do investigado, seus endereços e todos os dados.

[23] A Inglaterra tem um *plugin* no *browser* que você aperta e vai uma denúncia de um *site* suspeito para a polícia investigar.

- Comitê de Implementação do Software Livre no Governo Federal;

- Promover compartilhamento de informações, trabalho cooperativado, fazer a informação circular com mais velocidade e com mais agilidade entre as diversas esferas do poder público;

- Controle parental; classificação indicativa;

- Plano Nacional de Enfrentamento da Violência Sexual contra Crianças e Adolescentes;

- Realizar pesquisas de vitimização, a exemplo da Tik Kids;

- Disque 100;

- Proteja Brasil (autoproteção e ao autocuidado; mídia *literacy*);

- Bloqueio e a retirada de páginas;

- Reduzir os prazos de entrega de dados: em caso risco de morte de uma criança, transferir o sigilo em 2 horas; uma criança correndo perigo que não tem crime de morte, em 24 horas, no máximo 48 horas;

- Embaixadas do Brasil de dar visto a qualquer cidadão que respondeu por crime de abuso de criança no seu país, a qualquer cidadão que está sendo investigado por crime de abuso de criança;

- Aprovação da difusão vermelha;

- Instituir o *Day of General Discussion,* que é o Dia de Discussão Geral (Comitê dos Direitos da Criança na ONU);

- Regular a publicidade infantil (conteúdo inapropriado e violento; publicidade abusiva e enganosa);

- Resolução n. 163, do Conanda (Política Regulatória da Publicidade Infantil);

- Grupo Especializado de Combate ao Crime Cibernético;

- Grupo de trabalho de enfrentamento aos crimes cibernéticos;

- Departamento de Segurança da Informação e Comunicações (DSIC);

- Comitê Gestor da Internet da Administração Pública Federal;

- *Safer Internet Day* (9 de fevereiro);

- Termos de Cooperação e Termos de Ajustamento de Conduta;

- Preservação de evidências;

- Grupo de Trabalho sobre Delito Cibernético da OEA;

- Aderir à Convenção de Budapeste;

- Fiscalía (Montevidéu);

- Conferência Octopus contra o Cibercrime;

- *Internet Governance Forum* (IGF);

- *National Center for Missing & Exploited Children* (NCMEC);

- *Digital Crimes Consortium*;

- *Global Conference on Cyberspace*;

- Ameripol, Europol, Interpol;

- Núcleos técnicos de Combate a Crimes Cibernéticos;

- Tipificar crimes cibernéticos no novo Código Penal;

- Reestruturar área pericial (fortalecer o Instituto

Nacional de Criminalística);

- Criação de mais grupos especializados no combate aos crimes cibernéticos dentro do Ministério Público;

- Criação de delegacias especializadas com maior capacitação e estrutura;

- Treinamento e a capacitação dos setores periciais e órgãos especializados;

- Maior integração do Ministério Público com a Polícia e com o Judiciário, uma cooperação para otimizar os resultados;

- Intensificação da comunicação entre os países, para facilitar a obtenção de provas;

- Acordo sobre o cumprimento da legislação local;

- Procuradoria Federal dos Direitos do Cidadão;

- *Ministério Público pela Educação Digital na Escola*;

- *Segurança, Ética e Cidadania: educando para boas escolhas on-line*;

- Termo de multa, de cooperação em matéria penal, com os Estados Unidos (*Mutual Legal Assistance Treaties* – MLAT);

- Integração entre os órgãos de prevenção, investigação e repressão a crimes cibernéticos;

- Equilibrar internet livre e segura;

- Proteger a vítima de pornografia infantil, interpelando os compartilhadores;

- Projeto de Lei do Senado n. 236, de 2012;

- Conferência Internacional de Perícias em Crimes Cibernéticos;

- Complexo Global para Inovação da Interpol, em

Singapura;

- *www.denunciar.org.br*;

- Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério da Justiça;

- Instituir uma agência reguladora de *software*;

- Garantir os princípios da segurança jurídica, da efetividade do processo e da verdade real;

- Proteger a cadeia de custódia de evidências;

- Aumento do efetivo policial e de perícia;

- Autorizar procedimentos básica aos agentes e delegados;

- Centro Nacional de Capacitação e Difusão de Ciências Forenses;

- Conferência Internacional de Perícias em Crimes Cibernéticos (ICCyber);

- ICMedia;

- NuDetective;

- Instituir carimbo de tempo com uma autenticação criptográfica das interceptações;

- Investir em análise integrada, ou seja, a propiciação de um ambiente de análise integrada pelos vários atores da polícia e até da persecução penal;

- Certificados digitais, uso de registros de resumos criptográficos e de uma Autoridade de Carimbo de Tempo – ACT (cartórios digitais de tempo);

- ETSI (identificação automática de locutor);

- Espiões, agentes, robôs, infiltrados na Internet

(policial sem rosto);

- Centros de combate unificado;

- Lei de Acesso à Informação;

- Núcleo de Segurança e Credenciamento;

- Coordenação-Geral de Tratamento de Incidente de Redes (Centro de Tratamento de Incidente de Redes de Governo – CTIR Gov);

- Guia de Boas Práticas do Planejamento de SIC;

- Elaborar uma política de segurança da informação;

- Instrução Normativa n. 01, de 2008;

- Norma nº 21, "*Coleta e preservação de vidências e incidentes de segurança de rede da APF*";

- Programa Defesa Nacional;

- Programa Democracia e Aperfeiçoamento da Gestão Pública;

- Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (Cepesc)/Abin;

- Criptografia de Estado;

- Escola Nacional de Defesa Cibernética (ENaDCiber);

- Instituto Militar de Engenharia (IME);

- Sistema Modular de Defesa Cibernética;

- Comando de Defesa Cibernética;

- Observatório de Defesa Cibernética;

- Criptografia, de certificação digital, de educação, de normas;

- Instituto Alana;

- Projeto Infância Livre;

- Campanha obrigatória de segurança pública digital em televisão e rádio;

- Preparo da polícia, a falta de treinamento, a falta de ferramenta, a capacidade de gerar uma punição mais elevada, a capacidade de guarda de provas e leis mais fortes relacionadas a combate de crime;

- Fazer campanhas de conscientização de segurança pública digital;

- Novas leis para combater mais efetivamente, inclusive o que é terrorismo digital;

- Atualizar a questão sobre o encarceramento digital e implementar o procedimento de polícia para revista digital;

- Combate mais ostensivo do crime cibernético;

- Integração entre os interessados: Poder Executivo poderia apoiar na implementação de campanhas educativas, inclusive com *enforcement* do MJ; a própria ANATEL junto com as operadoras exigir campanhas de segurança pública digital; o Judiciário combatendo a impunidade; a autoridade policial agindo de forma integrada e podendo coletar provas; a sociedade civil aprendendo a se proteger, não deixando mais a porta aberta;

- Decálogo do conteúdo gestor da Internet;

- Princípios da necessidade, proporcionalidade e a questão do consentimento (granularidade desse consentimento);

- Garantia da anonimização dos dados;

- Segurança da infraestrutura, da rede;

- Não discriminação dos consumidores *on-line*;

- Investir na capacidade de reação imediata da autoridade policial e do Ministério Público — não no pedido de preservação de uma prova, mas no acesso a ela enquanto se está procedendo à investigação para um flagrante conteúdo de pedofilia;

- Testemunhas-máquinas (dever de colaboração ágil);

- Denúncia de *spam para o hotline* de polícia;

- Identidade digital obrigatória;

- Restabelecer a autoridade policial;[24]

- Lei de proteção de dados pessoais (consentimento; proteção da privacidade; tecnologia de anonimização);

- Inhope;

- Declaração dos Direitos na Internet;

- Responsabilidade civil objetiva, responsabilidade penal objetiva;

- Rede Ibero-Americana de Proteção de Dados;

- Projeto Mapear (Polícia Rodoviária Federal);

- Cooperação internacional;

- Penas alternativas que possam recuperar;

- Polícias Civis dos Estados sejam fortalecidas. Elas precisam ser restruturadas e fortalecidas;

- Instituto Brasileiro de Estudos, Pesquisas e Formação para a Inovação Social (Ibepis);

- Núcleo de Investigação dos Crimes de Alta

[24] Nos Estados Unidos a preservação e apresentação de evidências em crimes flagrantes, no caso de crimes considerados mais graves — por isso temos que aumentar a gravidade de alguns crimes no Código Penal — ocorrem por ordem de autoridade policial, não por ordem judicial.

Tecnologia (Nicat)/RN;

- Associação Brasileira de Centros de Inclusão Digital (ABCID);

- Direito ao esquecimento;

- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (Cert);

- Associação Brasileira das Agências Digitais (ABRADi);

- *International Advertising Bureau* (IAB);

- *World Federation of Advertisers* (WFA);

- Movimento Criança Mais Segura na Internet;

- Campanha Mundial de Conscientização dos Consumidores frente à Pirataria;

- *www.somostodosresponsaveis.com.br;*

- *Internet Crime Complaint Center* (IC3);

- *Security and Stability Advisory Committee* (Comitê Consultor para Segurança e Estabilidade);

- *Internet Society Perspectives on Domain Name System Filtering;*

- InternetLab, de São Paulo;

- GPOPAI, da USP;

- Cadastro Nacional de Acesso à Internet.

O trabalho desta CPI consistiu na análise dessas contribuições e sugestões e verificar quais aspectos, instituições e arranjos são passíveis de serem implementados, incentivados ou, mesmo, necessários para o país. Nessa sistematização a Comissão partiu da seguinte premissa: como evitar

golpes e fraudes na internet.

As sugestões acatadas estão constantes em capítulo específico deste relatório, mais adiante. No entanto, neste ponto do documento é importante destacar as boas práticas individuais que deveriam ser seguidas por todos os internautas para se evitar cair em arapucas digitais.

Segundo o ditado popular que diz haver malandros porque há otários, é preciso apenas um pouco de perspicácia para não se cair nos golpes, muitas vezes antigos e agora apenas repaginados. Os antigos golpes e fraudes aplicados por malandros diversos utilizam, atualmente, componentes tecnológicos. Mas os prejuízos e a sensação de impotência é a mesma. Os golpes configuram um tipo de violência sutil, pois causa enormes prejuízos, principalmente a pessoas vulneráveis ou hipossuficientes, isto é, as físicas ou socioeconomicamente frágeis, como crianças, idosos, doentes e pouco escolarizados. Os estelionatários são muito espertos e convencem facilmente até pessoas com boa escolaridade. Há golpes com cartões bancários, em caixas eletrônicos, por telefone e por mensagens. Nestas, das mais comuns, são ofertadas oportunidades imperdíveis ou divulgados números de telefones por meio dos quais o estelionatário aplica o golpe.

Embora voltados também para os crimes ocorrentes no mundo físico, há vários sites na internet que dão conselhos para evitar golpes, dentre os quais:

- “Monitor das fraudes” (<http://www.fraudes.org/showext8.asp?pg=148>);

- “Golpes e fraudes” (<http://golpesefraudes.blogspot.com.br>);

- “Antispam” (<http://antispam.br/tipos/fraudes>, para fraudes pela internet);

- “Rede Nacional de Ensino e Pesquisa (RNEP)” (<http://www.rnp.br/servicos/ seguranca/catalogo-fraudes>);

- “Manual das fraudes” (site português, <http://fraudes.no.sapo.pt/pequenos% 20golpes%20populares.htm>);

- “Federação Brasileira de Bancos (Febraban)” (<http://www.febraban.org.br/Arquivo/Destaques/show.asp?id_destaque=629>).

Além dos golpes comuns, há aquelas situações que exploram as crendices, podendo levar as pessoas a tomar decisões erradas, as quais são igualmente exploradas pelo cibercrime, os quais são analisados em diversos sítios, como por exemplo:

- “E-farsas” (<http://www.e-farsas.com>);

- “Boatos.org” (<http://www.boatos.org>);

- “Quatrocantos.com” (<http://www.quatrocantos.com>); e

- “Ahduvido” (<http://ahduvido.com.br>).

Um dos golpes mais comuns atualmente é o chamado falso sequestro, que pode gerar, além de prejuízos financeiros, elevada carga de estresse psicológico. Nesse golpe, normalmente são feitas ligações telefônicas por presos de dentro de presídios, os quais ligam para as vítimas e dizem que sequestraram um parente. Colocam pessoas ao fundo chorando e gritando, pois sabem que é difícil reconhecer a voz de alguém chorando e a vítima tem certeza que é o seu parente. Com o susto, as próprias vítimas repassam detalhes pessoais aos falsos sequestradores. Geralmente, a quantia exigida no resgate é pequena, pois os criminosos ganham em escala. Assim, o tempo para que a pessoa que está sendo enganada recolha o dinheiro é mais rápido. Na maioria das vezes, as ligações são feitas aleatoriamente. Mas em alguns casos, os golpistas fazem uma pequena investigação para descobrir informações da família ou utilizam listagem de dados que adquirem no mercado negro.

Condutas proativas para evitar essa espécie criminosa podem incluir:

1) não atender ligações a cobrar, principalmente se for de madrugada;

2) desconfiar de ligações com o prefixo de outra área;

3) não se deixar impressionar por coincidências, perguntando pelo nome da pessoa ‘sequestrada’, sem dizer o nome dela,

trocando o nome, pois o bandido não vai confirmar ou vai desligar;

4) se pedirem para não desligar o telefone, isso é um sinal de que é falso sequestro, pois sequestradores não têm pressa e se for um sequestro real, entrarão em contato novamente; e

5) enquanto conversa com o pretenso sequestrador, pedir para alguém ligar para o parente ou buscar orientação da polícia, pelos números de telefone gratuitos 190 ou 147.

Outra séria incidência do cibercrime que causa verdadeiras tragédias é o tráfico de pessoas, tráfico humano ou tráfico de seres humanos (TSH). A conduta criminosa pode visar à exploração sexual comercial da vítima, sua submissão a trabalho escravo, o favorecimento da imigração e adoção ilegais, assim como a mutilação de parte de seu corpo para extração de órgãos para transplante. O tráfico de pessoas pode envolver contato presencial e mesmo só ele, mas a maioria é precedida de contato virtual, principalmente por meio das redes sociais. É importante não se deixar envolver por apelos supostamente inofensivos por essas redes sociais, como Facebook, Twitter e outras. Os traficantes são insidiosos, fazem-se passar por pessoas ricas, influentes e *bon vivants* (*playboys*). Muitos deles convencem os internautas, principalmente mulheres, a iniciar relacionamento virtual, que passa a presencial só para fins de convencerem as incautas a seguirem para o exterior, onde cairão nas garras dos exploradores. Inicialmente dão presentes caros, levam para jantares em restaurantes finos, enquanto preparam o bote. Enquanto isso, dão carinho e atenção, mantendo um relacionamento ‘amoroso’ que faz a vítima se apaixonar ingenuamente. A atitude preventiva, nesses casos, é não se deixar envolver por aparências. Às vezes a pessoa posta fotografias, vídeos e até se mostra como se fosse alguém de bela aparência, com bons relacionamentos, de boa formação, como se fossem empresários ou profissionais liberais bem sucedidos. A falta de relacionamentos afetivos sólidos ou confiáveis pode potencializar tais ataques, vez que nesses casos a vítima nem sempre tem a quem contar o que vem ocorrendo. As crianças, jovens e pessoas que vivem sozinhas são as potenciais vítimas, devendo ser objeto de monitoramento por parte dos responsáveis ou parentes.

1.3.9 – Classificação e proteção de dados governamentais e estratégicos

Passo importante no âmbito da proteção de documentos sensíveis foi dado pela Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI), "regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências".

Buscando equilibrar o interesse público e a necessidade de transparência da Administração Pública, estabelece critérios bastante liberais para o acesso do público às informações oficiais. Revogando norma anterior que dispunha sobre a matéria, de abrangência bem mais modesta, a Lei n. 11.111, de 5 de maio de 2005, altera a Lei n. 8.159, de 8 de janeiro de 1991, que "dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências". Foi regulamentada pelo Decreto n. 7.724, de 16 de maio de 2012, que "regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do *caput* do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição".

Outra norma que regula a informação classificada é o Decreto n. 7.845, de 14 de novembro de 2012, que "regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento". Revogou o Decreto n. 4.553, de 27 de dezembro de 2002, que "dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências"; e que por retrospectiva revogatória dos Decretos n. 2.134, de 24 de janeiro de 1997 e n. 2.910, de 29 de dezembro de 1998, atinge o Decreto n. 79.099, de 6 de janeiro de 1977, que aprovou o antigo "Regulamento para Salvaguarda de Assuntos Sigilosos".

Em que pese esse pretenso extenso arcabouço jurídico, notícia publicada no jornal *O Globo*, de 25/08/2015, na coluna Opinião, página 17, sob o título "Segurança cibernética", de autoria de Rubens Barbosa, revela que:

> No Brasil, engatinhamos na proteção da segurança das

> comunicações governamentais e privadas. O Centro de Defesa Cibernética – previsto na Estratégia Nacional de Defesa – criado no âmbito do Ministério da Defesa em 2010, continua afetado pela falta de recursos financeiros. A situação atual, descrita pelo ex-ministro Celso Amorim como "vulnerável", tem se agravado pela velocidade das mudanças e pela intensificação dos ataques cibernéticos em nossas redes de informação.

1.4 – PROCEDIMENTOS DE CRIAÇÃO DE CONTAS E DE PERFIS NA INTERNET

A identidade de usuários na internet nos dias de hoje é extremamente importante devido à miríade de serviços oferecidos pela grande rede e pelo alcance das informações. Com uma conta de e-mail válida compram-se produtos, ativam-se cadastros em redes sociais e habilitam-se aplicativos. Neste contexto, uma identidade virtual é até mais importante do que uma carteira de identidade. Quando analisados os crimes cibernéticos cometidos, na gênese do golpe muitas vezes encontram-se perfis falsos ou inválidos, o que dificulta, chegando a impossibilitar em inúmeros casos, a investigação criminal e a punição dos culpados.

Com base nessa constatação, esta CPI decidiu por realizar um procedimento de aferição dos métodos utilizados pelas principais empresas ponto com para a garantia da veracidade das informações de cadastro de seus usuários. Com a colaboração do Tribunal de Contas da União, foram verificados os procedimentos de criação de contas nos provedores de aplicações Gmail, Yahoo e Microsoft.

Constam nesse item as telas indicando os dados necessários para se criar uma conta de correio eletrônicos, assim como o passo a passo do procedimento adotado por cada um dos provedores de aplicações objeto desta auditoria.

1.4.1 Criação de conta no serviço de aplicação de correios eletrônico do GMAIL

O primeiro passo para se criar uma conta no Gmail é acessar o endereço eletrônico: www.gmail.com, que abrirá a seguinte tela:

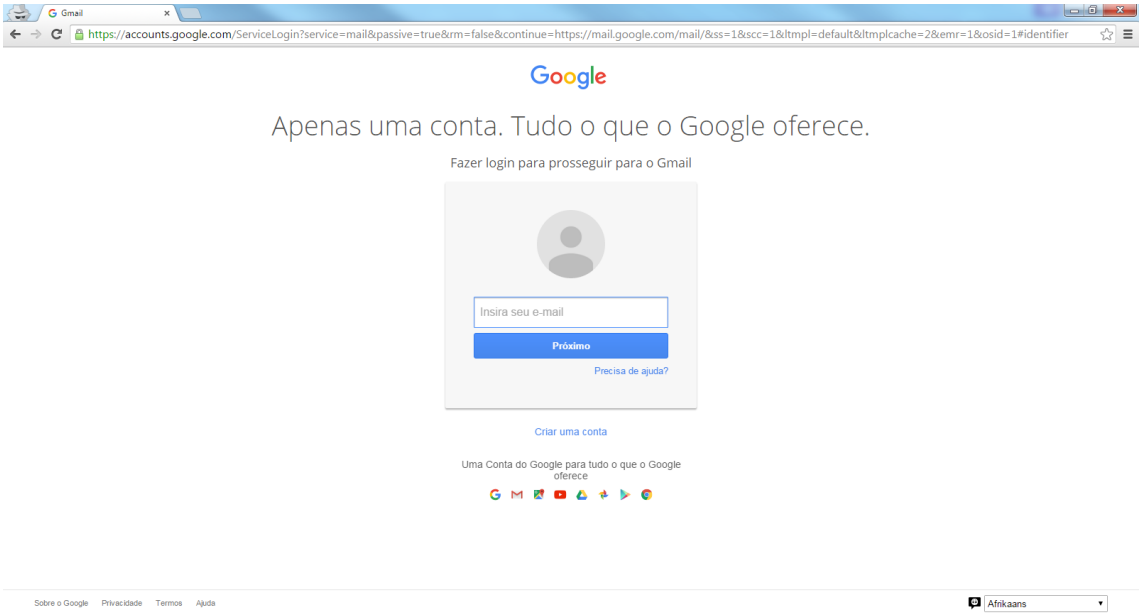


Figura 1 - Tela inicial de criação de conta no serviço de aplicação de correio eletrônico Gmail

Após clicar no ícone “Criar uma conta”, abrir-se-á a tela a seguir, na qual se solicita os seguintes dados: 1) Nome e sobrenome; 2)Escolha seu nome de usuário; 3) Criar uma senha; 4) Confirme sua senha; 5) Data de nascimento; 6) Sexo; 7) Celular; 8) Seu endereço de e-mail atual.

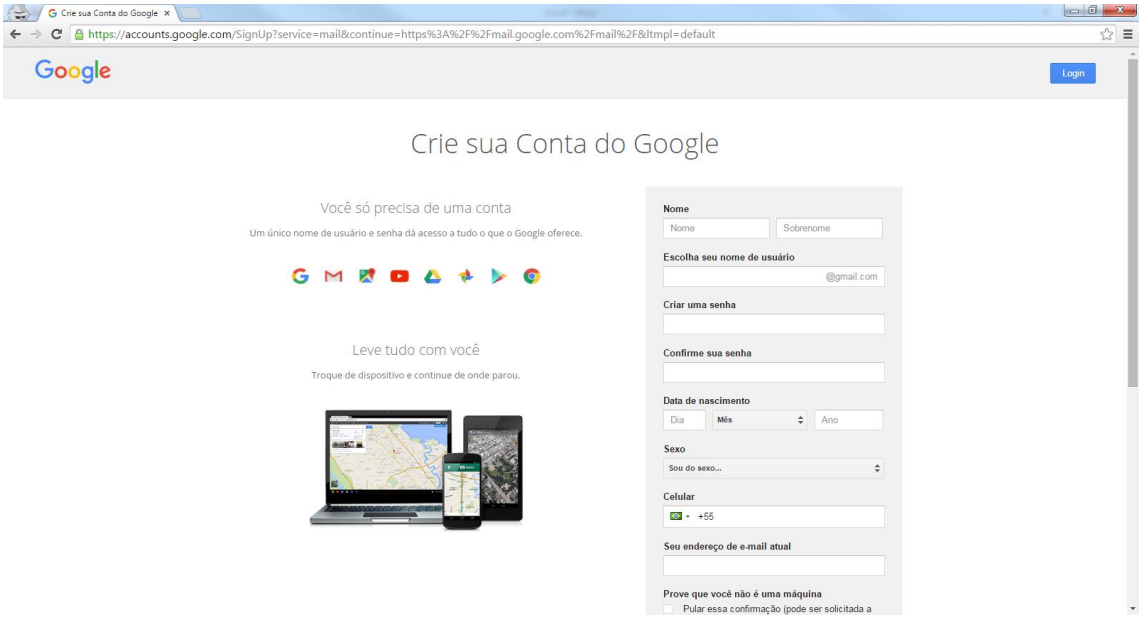


Figura 2 - Tela de solicitação de dados do serviço de aplicação de correio eletrônico Gmail

Para evitar a criação de contas por meio da utilização de programas de computador, o sítio utiliza o mecanismo de solicitar que o usuário digite o texto constante em uma imagem fornecida pelo serviço de aplicação.

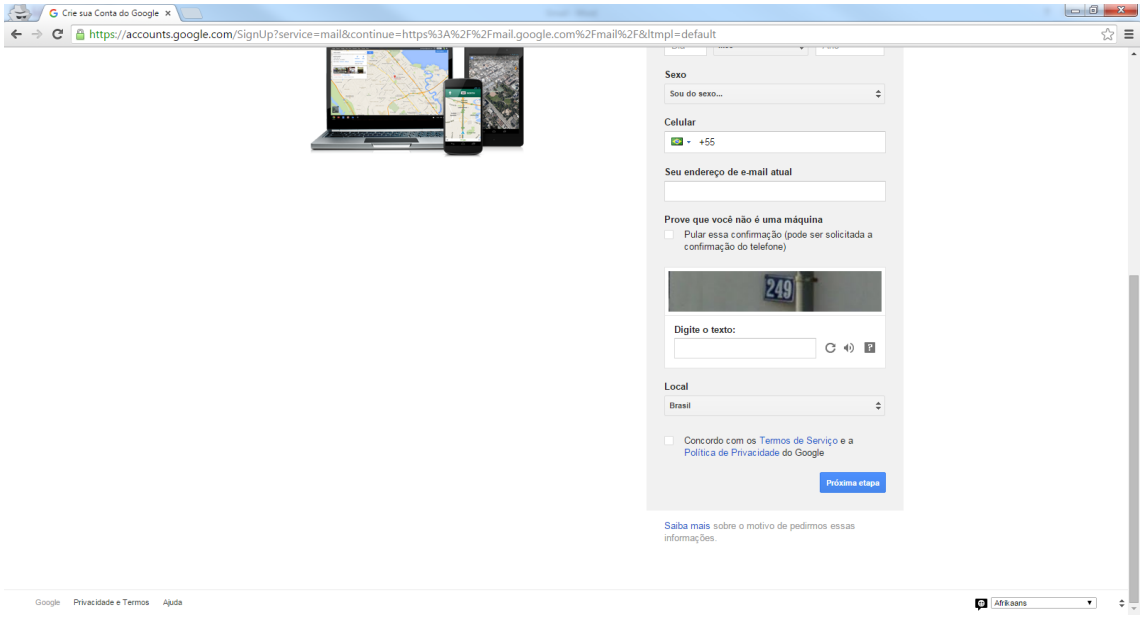


Figura 3 – Tela onde consta de a prova que o usuário não é uma máquina

Após o preenchimento dos dados, assim como a marcação de aceitação dos termos de usos, abre-se uma tela de verificação de conta, na qual se solicita o telefone do usuário para o serviço de aplicação enviar um código para o celular do indivíduo.

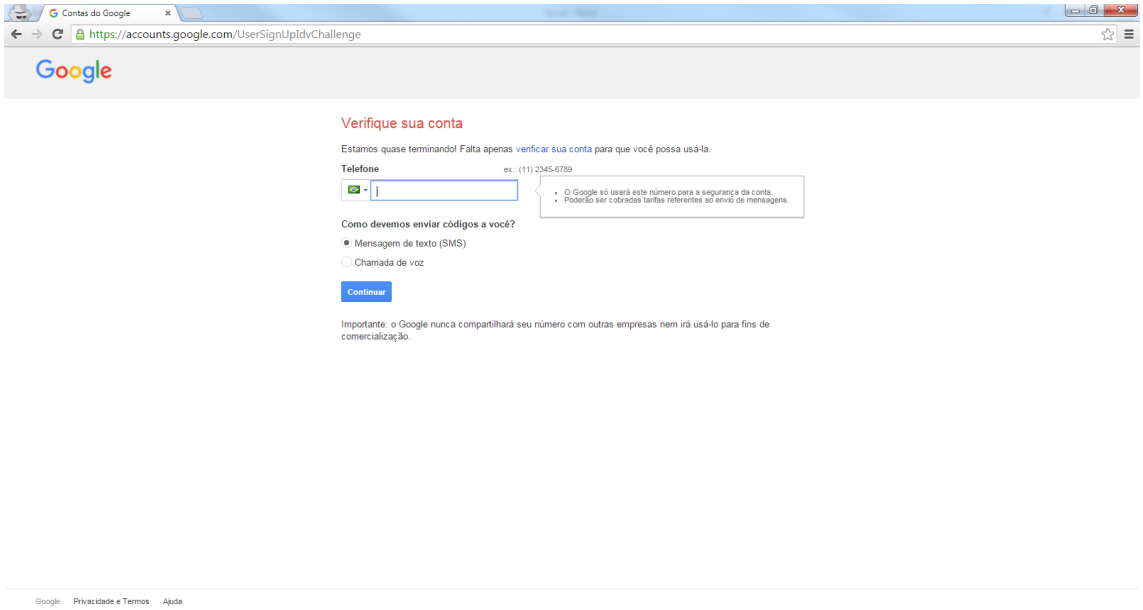


Figura 4 – Tela de verificação de usuário

Após essa etapa, abre-se uma tela na qual o usuário deve inserir o código verificador enviado pelo serviço de aplicação ao telefone informado na etapa anterior:

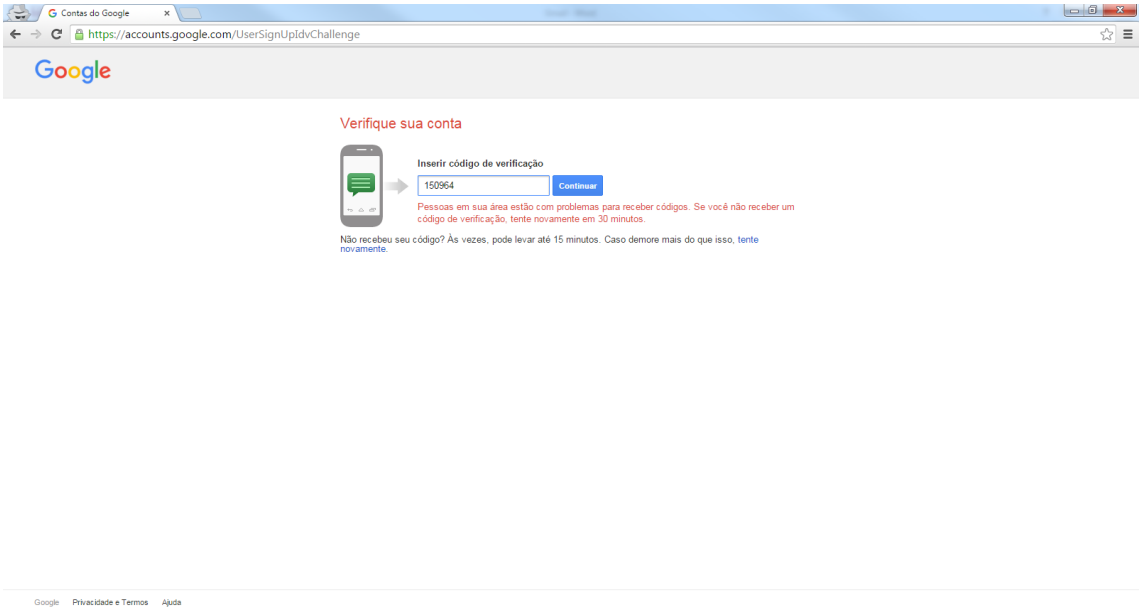


Figura 5 – Tela na qual o usuário deve inserir o código verificador fornecido pelo serviço de aplicação

Em seguida, caso o código de verificação esteja correto, a conta de correio eletrônico estará criada no serviço de aplicação de correio eletrônico.

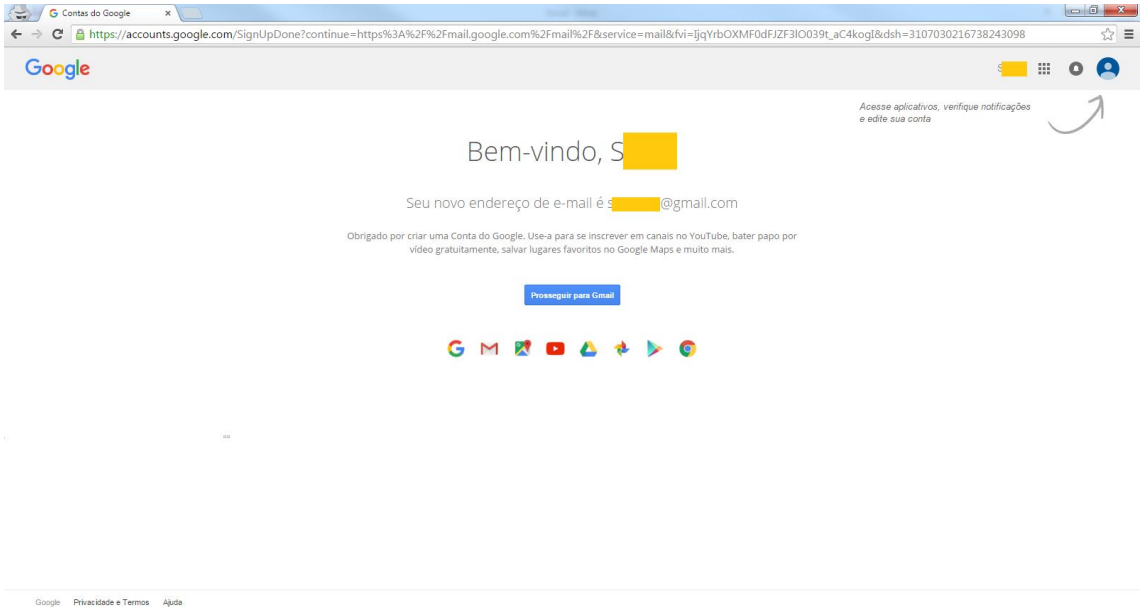


Figura 6 – Tela na qual informa que o procedimento de criação de usuário foi concluído

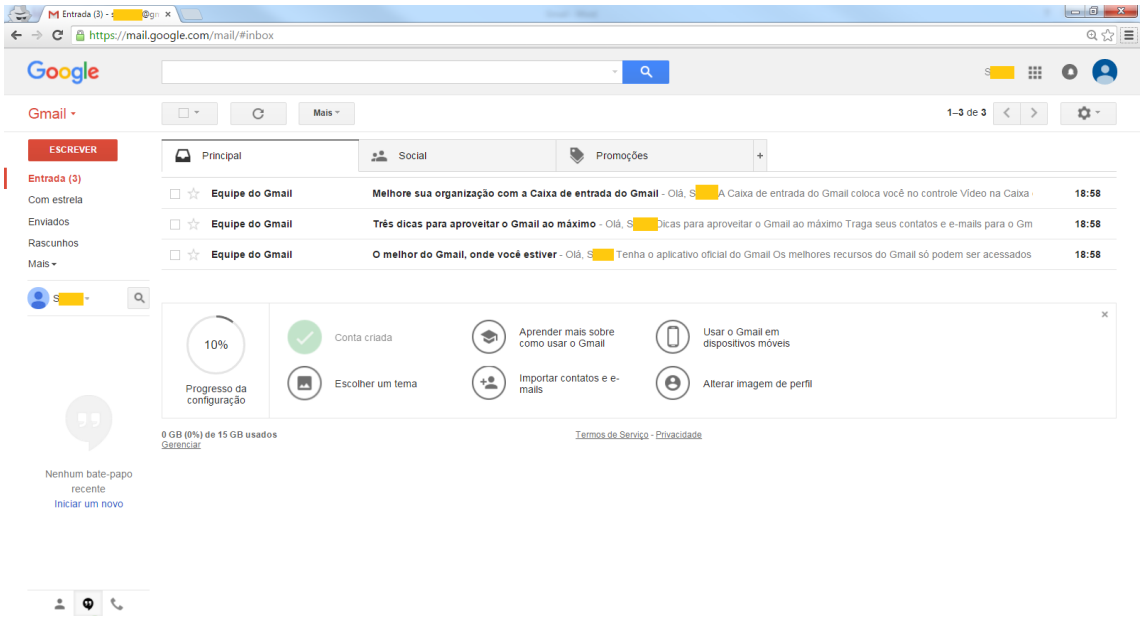


Figura 7 – Tela inicial da conta de correio eletrônico criada

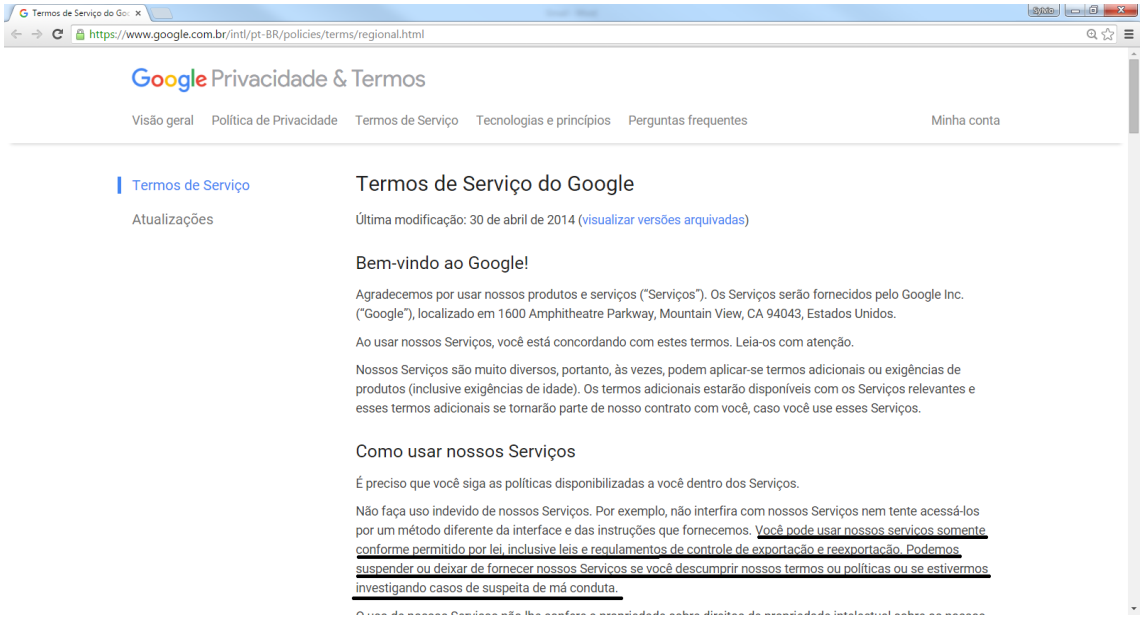


Figura 8 – Tela na qual consta os termos de usos do serviço de aplicação.

1.4.2 Criação de conta no serviço de aplicação de correios eletrônico do Hotmail

O primeiro passo para se criar uma conta no Hotmail é acessar o endereço eletrônico: https://signup.live.com/ que abrirá a seguinte tela:

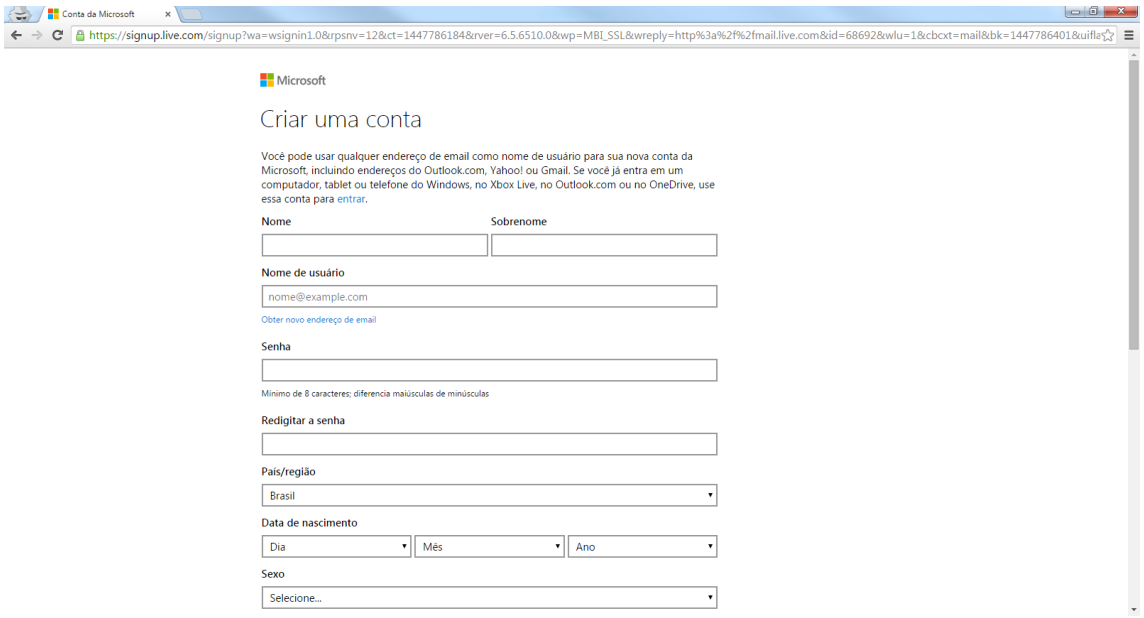


Figura 9 - Tela inicial de criação de conta no serviço de aplicação de correio eletrônico Hotmail

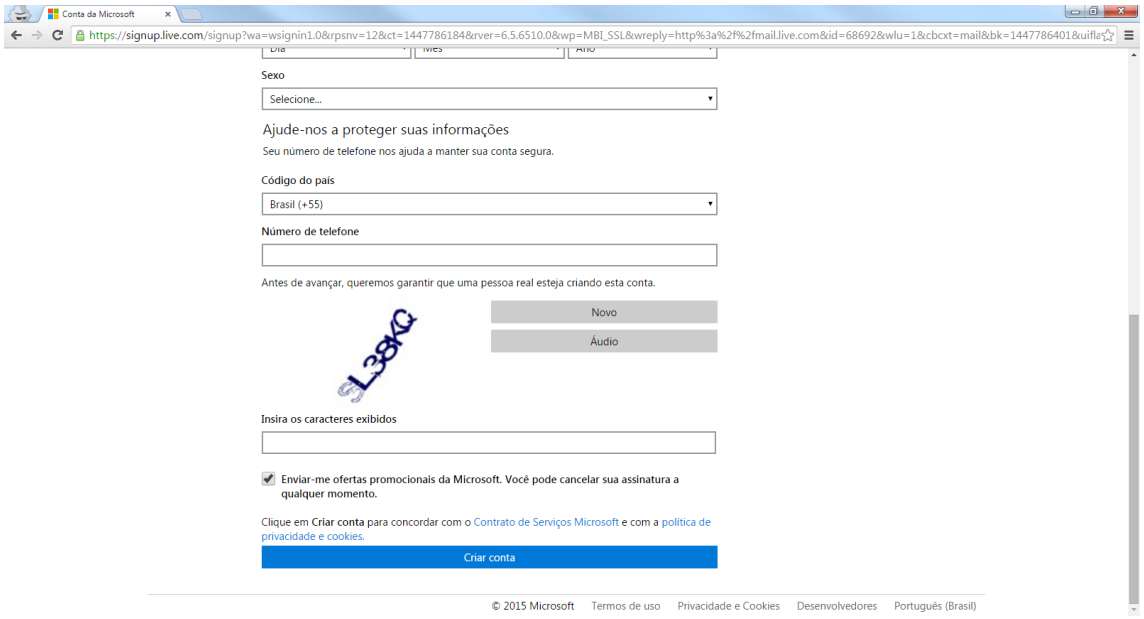


Figura 10 - Tela inicial de criação de conta no serviço de aplicação de correio eletrônico Hotmail

Para se criar uma conta no serviço de aplicação de correio eletrônico do Hotmail é necessário fornecer as seguintes informações de usuário: 1) Nome e Sobrenome; 2) Nome de Usuário; 3) Senha; 4) Redigitar a Senha; 5) País/região; 6) Data de Nascimento; 7) Sexo; 8) Código do País; 9) Número de telefone.

Para evitar a criação de contas por meio da utilização de programas de computador, o Hotmail utiliza o mecanismo de solicitar que o usuário digite o texto constante em uma imagem fornecida pelo serviço de aplicação.

Constatou-se que o perfil de usuário não é criado se não for fornecido um número de telefone.

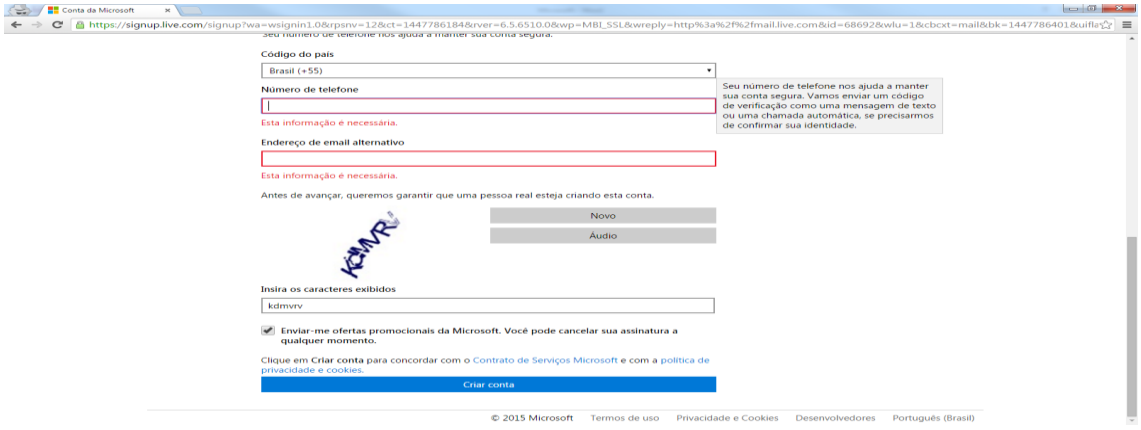


Figura 11 - Tela que informa que o número de telefone é obrigatório

Depois do preenchimento dos dados solicitados, e da correta inserção dos caracteres exibidos (verificação se o usuário não é uma máquina), a conta de correio eletrônico estará criada no serviço de aplicação de correio eletrônico.

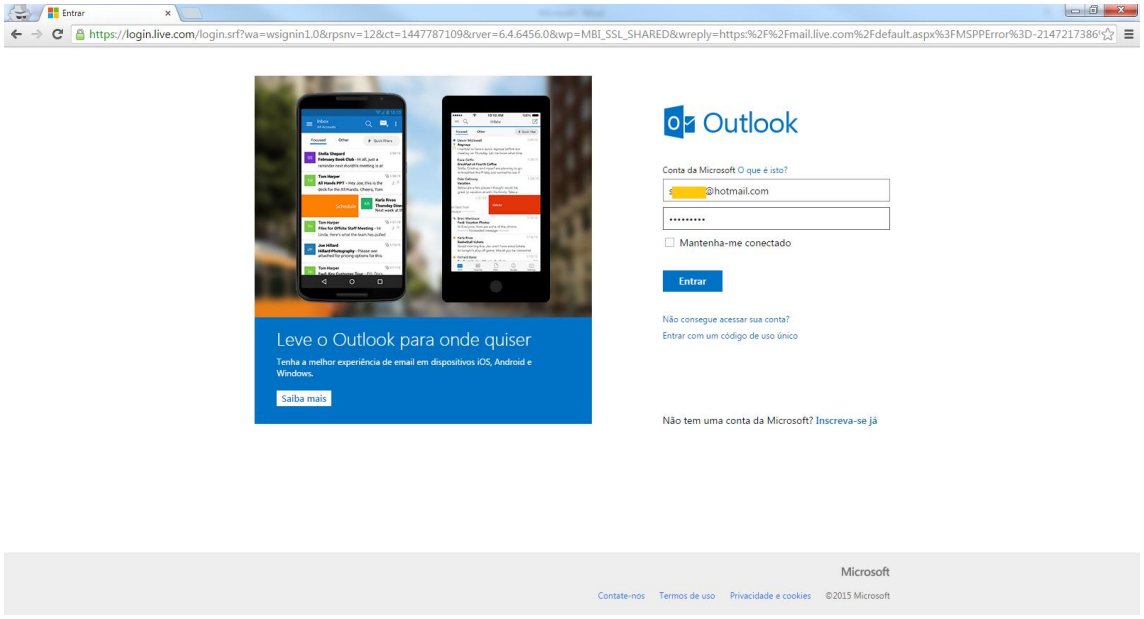


Figura 12 - Tela inicial que solicita o nome e usuário para entrar na conta de correio eletrônica

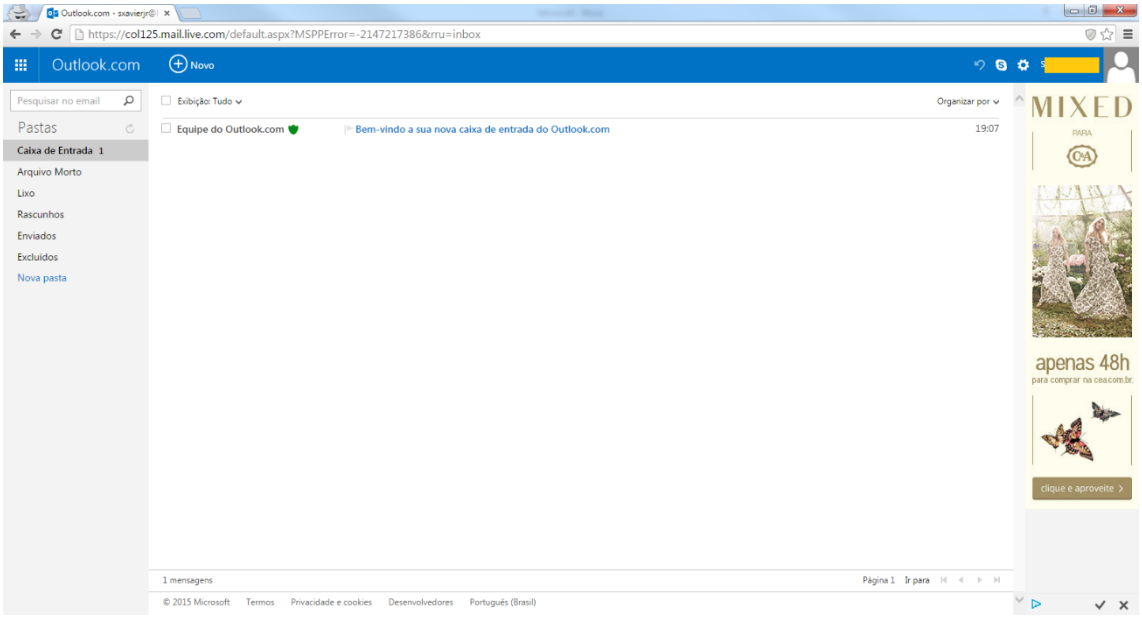


Figura 13 - Tela inicial da conta de correio eletrônico criada

1.4.3 Criação de conta no serviço de aplicação de correios eletrônico do Yahoo!

O servidor de aplicação de correio eletrônico Yahoo! solicita os seguintes dados para o usuário criar um perfil: 1) Nome e Sobrenome; 2) Usuário do Yahoo; 3) Senha; 4) Número de telefone celular; 5) Data de Nascimento; 6) Sexo e 7) Número de Recuperação (opcional).

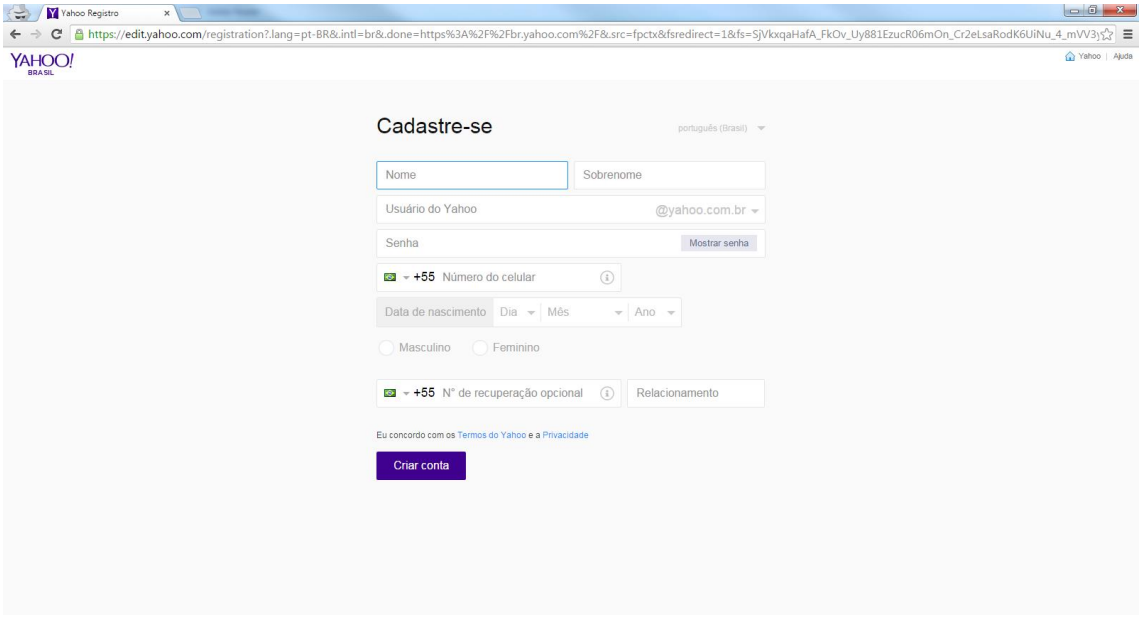


Figura 14 - Tela inicial da conta de correio eletrônico criada

Conforme se constata na figura abaixo, o número de telefone celular é obrigatório para se criar um perfil de usuário.

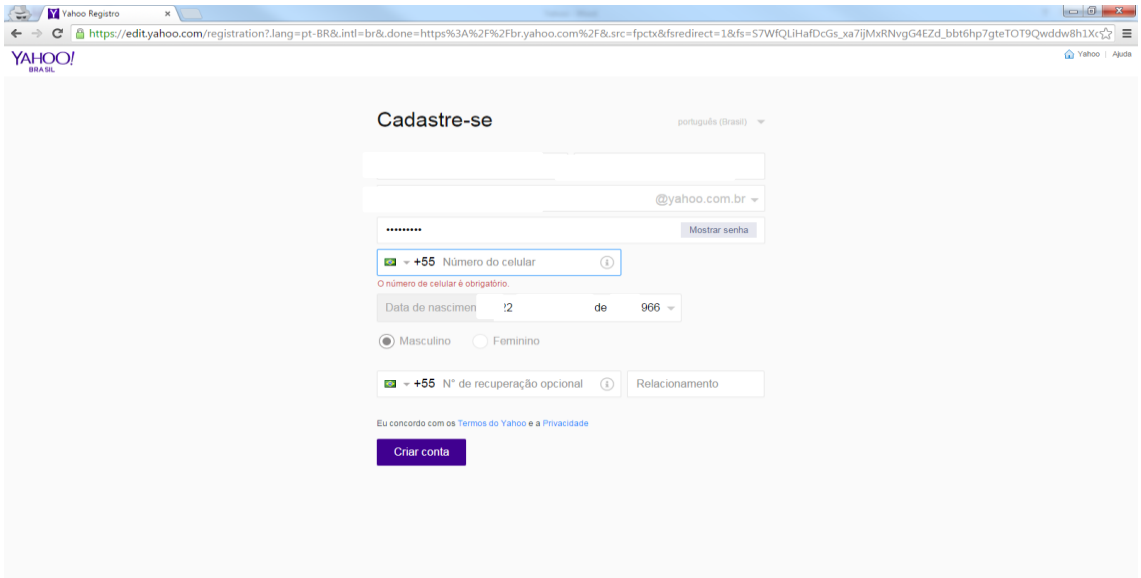


Figura 15 - Tela inicial que informa que o número de celular é obrigatório

Após o preenchimento dos dados, assim como a marcação de aceitação dos termos de usos, abre-se uma tela de verificação de conta, na qual o Yahoo! informa que enviará um código de verificador para o número de celular informado.

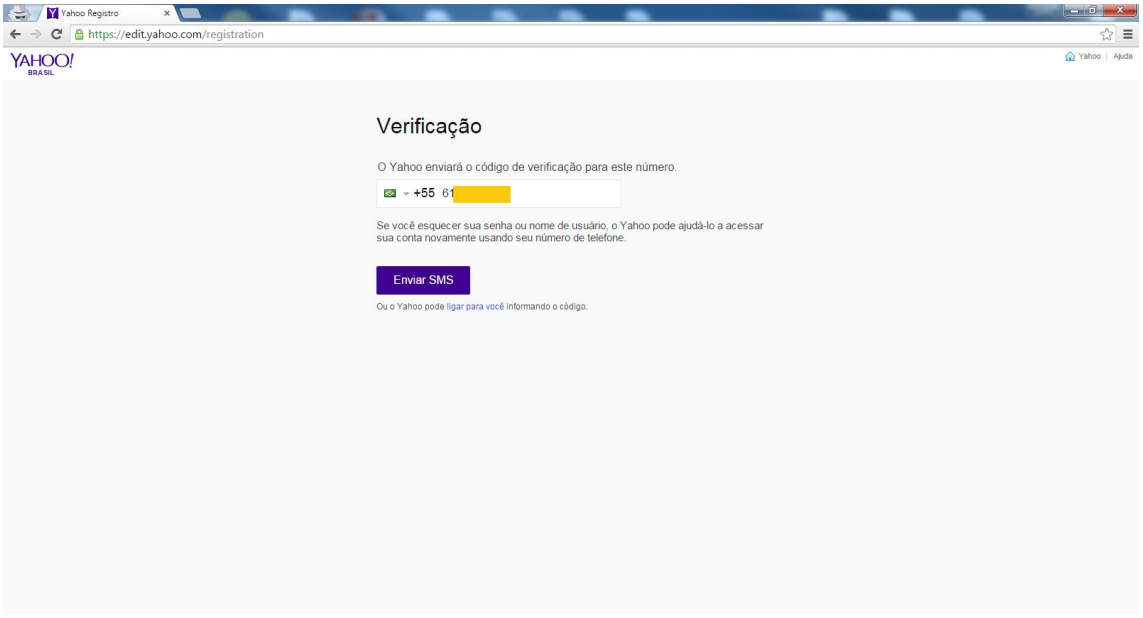


Figura 16 – Tela de verificação de usuário

Após essa etapa, abre-se uma tela na qual o usuário deve inserir o código verificador enviado pelo serviço de aplicação ao telefone informado na etapa anterior:

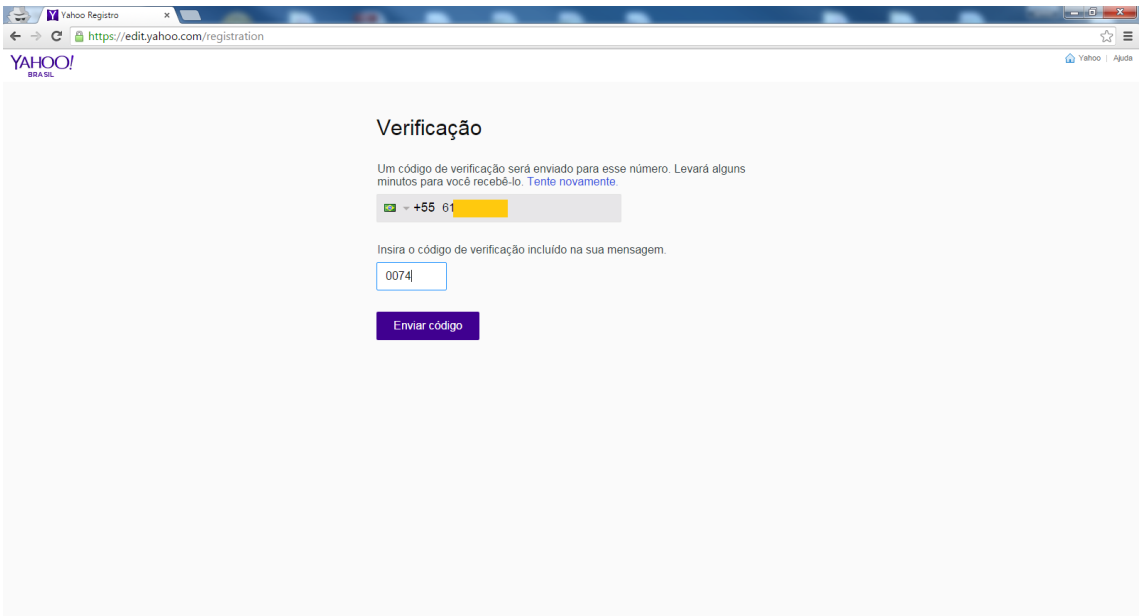


Figura 17 – Tela na qual o usuário deve inserir o código verificador fornecido pelo serviço de aplicação

Após realizado esse procedimento, está criada a conta de correio eletrônico.

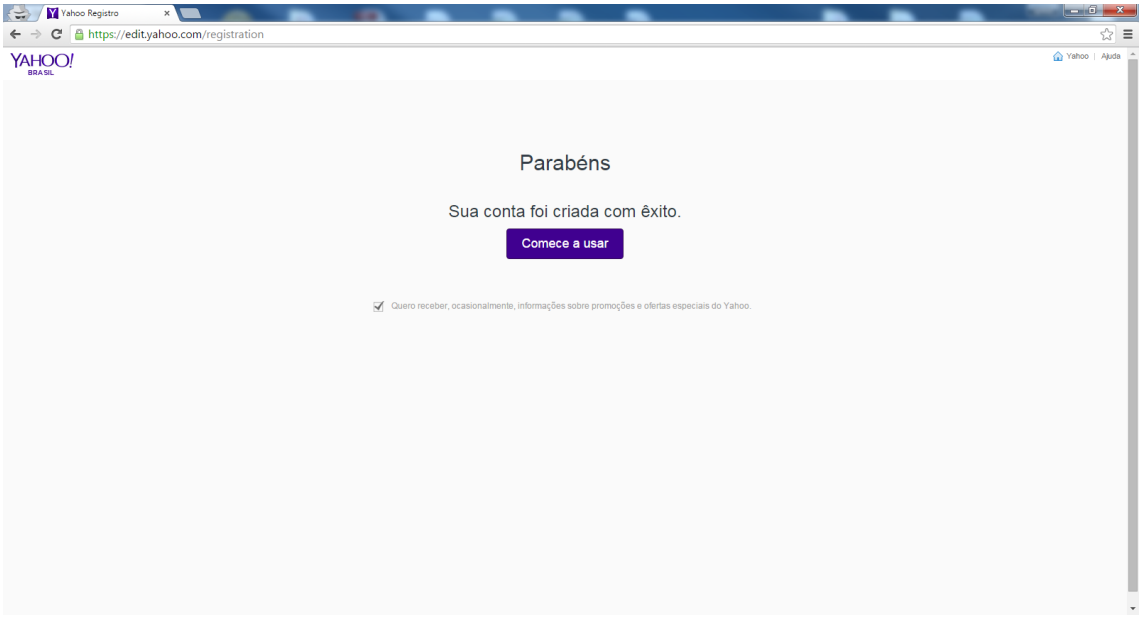


Figura 18 – Tela na qual informa o usuário que a conta foi criada

1.4.4 Considerações acerca dos procedimentos de cadastro

Foi possível evidenciar que pode ser criada uma conta qualquer (pertencente a pessoas verdadeiras ou fictícias) informando apenas um número de celular válido que serve para demonstrar que se trata de uma pessoa e não uma máquina.

Todos os três provedores adotam o procedimento de enviar um código via SMS para o número indicado na tela de cadastramento da conta, sendo que o usuário deve informar esse código para finalizar o procedimento. Além desse número de telefone, é necessário informar nome completo, sexo e data de nascimento, mas não existe procedimento para confirmar a veracidade dessas informações.

Deste exercício simplificado e não exaustivo com relação aos aplicativos analisados, depreende-se que a integridade e a veracidade dos dados informados dependem fundamentalmente da qualidade do cadastro da telefonia celular, isto é a correta identificação do titular da linha. Preocupa o fato

do cadastro do celular pré-pago ser bastante flexível e simplificado. Apesar da Lei nº 10.703/2003, que exige o cadastro dos usuários do pré-pago, é notório que os dados ali informados não são checados ou aferidos com o rigor necessário. O assunto do cadastro do pré-pago foi motivo de Audiência Pública específica no âmbito desta CPI e as conclusões daquele debate fazem parte das conclusões do Sub-Relator de Segurança Cibernética, que concluiu pelo oferecimento de uma Proposta de Fiscalização e Controle acerca do cadastro do pré-pago.

2 – CONSTATAÇÕES E INVESTIGAÇÕES DA CPI

2.1 – SUB-RELATORIA DE INSTITUIÇÕES FINANCEIRAS E COMÉRCIO VIRTUAL (SUB-RELATOR DEPUTADO SANDRO ALEX)

2.1.1 – Elaboração de Código de Boas Práticas na Publicidade Virtual e Assinatura de Termo de Ajustamento de Conduta

Dentre os inúmeros crimes praticados pela internet no âmbito das instituições financeiras e comércio virtual, encontra-se a difusão ilegal de conteúdos audiovisuais protegidos por direito autoral – os chamados sítios de conteúdos piratas. As investigações desta Sub-Relatoria identificaram diversos sítios que fazem esse tipo de veiculação, os quais são financiados mediante a veiculação de publicidade por meio de *banners*,

Com base em denúncia apresentada nesta CPI pelo Sub-Relator da área, em Audiência Pública no dia 08/10/15, com a presença do Sr. Edinho Silva, Ministro da Secretaria de Comunicação Social da Presidência da República, foi verificado que as entidades contratantes de serviços de publicidade e as agências de propaganda, em se tratando de veiculação de publicidade na internet, não possuem o controle final sobre quais sítios de internet efetivamente veiculam os anúncios contratados. Isso se deve a que algoritmos verificam quais sítios de internet possuem maior quantidade de acessos e automaticamente a essas páginas são direcionados os anúncios contratados.

Assim, como apresentado na denúncia, propagandas de empresas tradicionais e até do governo podem terminar sendo veiculadas em sítios utilizados para a prática de crimes cibernéticos, neste caso o *streaming* ilegal de filmes e de séries de televisão.

Pouco tempo após a denúncia apresentada, foi deflagrada a operação Barba Negra, da Polícia Federal, que resultou em prisões e na suspensão dos serviços do maior sítio de compartilhamento ilegal de filmes, o sítio Mega Filmes HD.

Como desdobramento da denúncia na CPI, em nova Audiência Pública em 04/04/2016, representante da empresa UOL, foi convidada para prestar esclarecimentos acerca das práticas de publicidade do grupo. A depoente informou que, em consequência ao conhecimento dos fatos denunciados à CPI, o grupo de comunicação disponibilizou em seu portal ferramenta para a denúncia de crimes cibernéticos.

O fato chama a atenção de que a CPI tem obtido logros na questão da transparência na gestão da contratação da publicidade ao longo dos elementos de sua cadeia. No entanto, verificamos que a transparência deva ser mais disseminada por todos os agentes, incluindo o setor público. Nesse sentido, chama a atenção a não entrega dos materiais solicitados ao Ministro da Secretária de Comunicação Social da Presidência da República, em 08/10/15. O material permitiria a esta CPI se debruçar sobre as práticas do setor e propor melhoramentos no sistema de contratação.

Dessa forma, esse tipo de derivação automática de publicidade nos leva a propor a criação de um **Código de Boas Práticas a ser adotado pelas entidades envolvidas com a publicidade no meio digital, para evitar a comercialização de espaço para anúncios publicitários em plataformas digitais que disponibilizem conteúdos ilícitos, pratiquem condutas ilegais e/ou fomentem a prática de tais condutas pelos seus usuários**. Esse Código de Boas Práticas poderá ensejar posterior assinatura de **Termo de Ajustamento de Conduta entre os principais sítios de internet, Conar, associações de mídia digital e Ministério Público Federal**. (Parte III, 5.e). Ademais o Ministro-Chefe da Secretaria de Comunicação Social declarou que encaminharia à Comissão “todo o ranqueamento [isto é, investimento em publicidade], assim como o ranqueamento das redes sociais para que a Comissão tenha todas as informações necessárias sobre o que é investido em publicidade, por meio da SECOM”. Ressaltamos que essas informações não foram encaminhadas até o encerramento dos trabalhos da CPI. Portanto, encaminhamos **Requerimento de Informações** solicitando esses dados.

2.1.2 – Aprofundamento das investigações sobre crimes cibernéticos contra a ordem tributária pelas empresas que veiculam publicidade na internet

No início de suas investigações sobre crimes cibernéticos, esta CPI convidou as companhias Google Brasil Internet Ltda., Microsoft do Brasil, Facebook Serviços Online do Brasil Ltda. e Twitter Brasil Rede de Informação Ltda, para prestarem depoimentos acerca de suas atividades no País. O convite tinha como objetivo colher informações das principais empresas de internet acerca de suas práticas para a proteção dos dados de seus clientes, sobre a sua participação no combate a crimes cibernéticos e sobre a segurança cibernética no Brasil, podendo, inclusive, trazer sugestões de aperfeiçoamento da legislação.

Durante a realização da Audiência Pública, levantou-se a possibilidade de que as empresas poderiam não estar recolhendo todos os tributos devidos no Brasil, o que motivou o envio de ofícios às empresas para que fossem prestados esclarecimentos adicionais.

Em resposta aos Ofícios encaminhados pela Presidência desta CPI, as empresas Facebook Serviços Online do Brasil Ltda., Twitter Brasil Rede de Informação Ltda. e Yahoo! do Brasil Internet Ltda. informaram que não estão sujeitas a recolher o Imposto Sobre Serviços de Qualquer Natureza (ISS) e nem o Imposto sobre Circulação de Mercadorias e sobre Serviços de Transporte Interestadual, Intermunicipal e de Comunicações (ICMS).

Quanto ao ISS, as empresas afirmam, em resumo, que a atividade por elas desenvolvida estaria enquadrada no item 17.07 (Veiculação e divulgação de textos, desenhos e outros materiais de propaganda e publicidade, por qualquer meio) originalmente previsto na Lei Complementar nº 116, de 31 de julho de 2013, mas objeto de veto presidencial.

Quanto ao ICMS, as empresas afirmam, em resumo, que a atividade por elas desenvolvida não se caracteriza como serviço de comunicação.

Em virtude da não ocorrência de fato gerador desses tributos estadual e municipal, as empresas informaram que não estão obrigadas à emissão de nota-fiscal.

Após a audiência pública realizada em 27 de agosto de 2015, o nobre Deputado Sandro Alex apresentou os Requerimentos n. 72 e 77/2015.

No primeiro, Sua Excelência solicitou a transferência do sigilo das empresas Google Brasil Internet; Facebook Serviços Online do Brasil; Twitter Brasil Rede de Informação e Yahoo! do Brasil Internet em virtude da suspeita, surgida durante a audiência pública mencionada, de que as citadas empresas não estariam recolhendo os tributos devidos no Brasil.

No segundo, Sua Excelência solicitou a convocação dos Diretores do Departamento de Tributação e Julgamento da Prefeitura de São Paulo em exercício atualmente, em exercício em 26 de novembro de 2009 e em exercício em 6 de fevereiro de 2013, assim como o Chefe da Coordenadoria da Administração Tributária da Secretaria da Fazenda do Estado de São Paulo.

O primeiro desses Requerimentos encontra-se pendente de apreciação, mas o último deles foi aprovado em reunião realizada em 20 de outubro de 2015, tendo ocorrido a oitiva dos servidores em reunião realizada em 17 de novembro de 2015.

Nessa reunião, constatou-se que o entendimento do Fisco de São Paulo parece ser o de que os serviços realizados pelas empresas se caracterizam como serviços de comunicação, o que atrairia a incidência do ICMS sobre tais receitas, desde que tais serviços sejam prestados no Brasil, entendimento esse corroborado pelo Tribunal de Justiça do Estado.

Apesar de tal entendimento aparentemente ainda não se encontrar pacificado na jurisprudência, haveria, no caso, uma questão de fato a ser solucionada, qual seja, a de saber se os serviços intermediados pelas empresas situadas no Brasil podem ser considerados aqui prestados ou se, ao contrário, seriam serviços de comunicação prestados em outros países e, portanto, não incluídos no campo de competências tributárias do Fisco estadual.

Quanto ao Fisco municipal, o entendimento é o de que a atividade das empresas se divide em duas partes. Uma delas seria a prevista no item 17.07 da Lei Complementar nº 116/2003, a qual foi objeto de veto presidencial, como já mencionado, o que afasta a competência tributária municipal.

Outra parte, todavia, diz respeito à intermediação, pelas empresas situadas no Brasil, de serviços prestados por empresas estrangeiras, serviços esses que se enquadram nos subitens 10.08 (agenciamento de publicidade e propaganda, inclusive o agenciamento de veiculação por quaisquer meios) e 10.09 (representação de qualquer natureza, inclusive comercial) da Lei Complemetnar nº 116/2003.

Constatou-se, inclusive, que a empresa Facebook Serviços Online do Brasil Ltda. formulou a Solução de Consulta nº 42/2013 à Prefeitura do Município de São Paulo, cuja resposta à consulente tem o seguinte teor:

> 6. Após a solicitação de documentos, a consulente apresentou novas informações acerca de suas operações.
>
> 6.1. Esclareceu que não desenvolve atualmente a atividade de locação de espaço publicitário, e sua principal atividade remunerada é a veiculação de publicidade online.
>
> 6.2. Considera que não presta serviços de intermediação entre o Facebook Ireland e os clientes anunciantes e que a Facebook Ireland não tem relação direta ou indireta com os clientes anunciantes brasileiros.
>
> 6.3. A consulente apresentou os seguintes documentos:
>
> Contrato de Veiculação de Anúncios firmado entre a Facebook Ireland Limited e a Facebook Serviços Online do Brasil Ltda., dois pedidos de inclusão de anúncios de empresas situadas no Brasil e o modelo dos Termos e Condições de Publicidade Facebook Ireland.
>
> 7. Dentre as condições estabelecidas no Contrato de Veiculação de Anúncios firmado entre a Facebook Ireland Limited, com sede na Irlanda, e a consulente estão:
>
> 7.1 A cláusula 2 nomeia a consulente como revendedora não exclusiva dos espaços publicitários aos clientes no território brasileiro.

7.2. A cláusula 3.1 estabelece que a consulente será responsável pelas comunicações com os clientes e clientes prospectivos, para fornecer informações sobre espaços publicitários, receber pedidos, faturar e cobrar pagamentos dos clientes, assim como por quaisquer assuntos administrativos com os clientes no território.

7.3. De acordo com a cláusula 3.4 a consulente deverá coletar e transmitir todos os dados de mercado disponíveis para a concessionária no território, incluindo, porém sem a isso se limitar, dados sobre potenciais anunciantes e seus requisitos, tendências do mercado no uso de redes sociais no território, e tendências sobre a publicidade de desempenho de marcas no território, todas as relevantes informações de anunciantes relativas às consultas, perguntas e reclamações de anunciantes.

7.4. Na cláusula 3.5 fica estabelecido que a consulente irá fornecer outros relatórios e informações relativas ao objeto do contrato, incluindo atividades de vendas, preços de mercado, produtos e estratégias de concorrentes, possíveis produtos novos, futuras necessidades de clientes, tendências de mercado e assuntos relacionados.

7.5. Nos termos da cláusula 5.1, em contrapartida da veiculação de publicidade aos clientes no território, a consulente deve pagar trimestralmente à empresa estrangeira uma quantia equivalente a 50% dos recebimentos brutos recebidos com relação à prestação de veiculação de publicidade aos clientes no território brasileiro.

8. Os serviços prestados pela consulente à Facebook Ireland Limited relativos a revenda de espaços publicitários na plataforma Facebook, nos termos descritos nos subitens 7.1 a 7.4, enquadram-se no subitem 10.09 da Lista de Serviços da Lei nº 13.701, de 24 de dezembro de 2003, referente ao código de serviço 06009 - representação de qualquer natureza, inclusive comercial, do Anexo 1 da Instrução Normativa SF/SUREM nº 08, de 18 de julho de 2011. Sobre estes serviços ocorre a incidência do ISS à alíquota de 5%,

nos termos do art. 14 da Lei nº 13.701, de 24/12/03, combinado com o art. 16 da mesma Lei, com a redação das Leis nº 14.256, de 29/12/06 e nº 14.668, de 14/01/08.

8.1 No caso em questão cabe ressaltar que, conforme descrito no item 7.5, o preço dos serviços de representação comercial prestados pela consulente corresponde a 50% (cinquenta por cento) dos recebimentos brutos relativos a veiculação de anúncios, que é a remuneração que lhe cabe em face do contrato apresentado.

8.2. Em relação a estes valores a consulente deve emitir Nota Fiscal de Serviços Eletrônica - NFS-e, de acordo com as disposições do Decreto nº 53.151, de 17 de maio de 2012.

8.3. A consulente deve também providenciar a inclusão do código 06009 em seu cadastro - CCM.

9. Sobre os serviços de veiculação prestados aos anunciantes no Brasil não ocorre a incidência do ISS. A atividade de veiculação de anúncios enquadrava-se no subitem 17.07 da lista de serviços constante do texto original da Lei Complementar nº 116, de 31 de julho de 2003. Todavia, os serviços de veiculação de anúncios foram excluídos do campo de incidência do ISS porque houve veto presidencial à inclusão de tais serviços na nova Lista de Serviços tributáveis.

Chama a atenção o fato de que a empresa não mencionou a esta CPI a Solução de Consulta nº 42/2013 formulada por ela, e a resposta a tal consulta deixa claro que a empresa Facebook Serviços Online do Brasil Ltda. deve pagar ISS sobre a contrapartida da veiculação de publicidade aos clientes no território nacional.

Dada a aparente similitude na estruturação negocial (empresas estrangerias constituindo sociedades limitadas no Brasil), é possível que a resposta se aplique por igual às empresas Twitter Brasil Rede de Informação Ltda. e Yahoo! do Brasil Internet Ltda., de modo que as três empresas estariam sujeitas ao recolhimento do ISS sobre receitas de intermediação, o que não vêm fazendo.

Do mesmo modo, a partir do cotejo entre as respostas fornecidas a esta CPI pelas empresas Google Brasil Internet Ltda.; Facebook Serviços Online do Brasil Ltda.; Twitter Brasil Rede de Informação Ltda. e Yahoo! do Brasil Internet Ltda. e as declarações do servidor da Administração Fiscal do Estado de São Paulo, é possível cogitar que todas as quatro empresas podem estar sujeitas ao ICMS sobre a parcela das receitas auferidas em território nacional não tributadas pelo ISS por se tratar, no caso de serviço de comunicação.

Esses dois fatos justificariam o aprofundamento das investigações e, inclusive, a transferência do sigilo das empresas apontadas.

Tendo em vista o término do prazo regimental para a conclusão dos trabalhos desta Comissão Parlamentar de Inquérito, não foi possível a realização de análises mais aprofundadas neste foro, nem a pretendida transferência do sigilo.

Por essa razão, concluímos pela apresentação de **Ofícios, em anexo, a fim de que as autoridades competentes aprofundem as investigações de modo a verificar se as aludidas empresas deixaram de recolher tributos devidos no território nacional, bem assim se houve a prática de crime contra a ordem tributária (Lei nº 8.137, de 27 de dezembro de 1990)** (Parte III, 4), mediante o uso da internet.

2.1.3 – Medidas para o combate a crimes cibernéticos contra o sistema financeiro

Na análise dos crimes cibernéticos cometidos contra o sistema financeiro nos deparamos com uma variedade de crimes sendo praticados. As contravenções são praticadas contra correntistas de bancos e usuários de entidades de crédito, assim como contra instituições solidamente estabelecidas. No estudo do caso, esta Sub-Relatoria realizou reunião de trabalho junto à Diretoria de Fiscalização do Banco Central, onde foram discutidas as ações de acompanhamento e de mitigação desses crimes por parte daquela instituição. A autoridade possui equipe especializada para receber denúncias e reclamações por parte de usuários e possui detalhado sistema de rankeamento das reclamações. Por outro lado, no que tange ao quantitativo de crimes digitais e

ao volume de recursos envolvidos, a Regulamentação exarada não possui como foco primário a informação específica das fraudes acometidas. Assim, os crimes cibernéticos são estimados como sendo uma fração de uma categoria geral conhecida no jargão técnico como “risco operacional”.

Tendo em vista que a publicização de informações referentes a crimes digitais efetuados contra instituições bancárias é extremamente sensível para a imagem das instituições e para a saúde do sistema financeiro como um todo, entendemos que essas informações devem ser trabalhadas com extrema cautela. Por outro lado, tanto correntistas quanto a autoridade reguladora devem possuir ferramentas transparentes que lhes possibilitem melhor avaliar os riscos envolvidos e tomarem as decisões que lhe cabem. Ademais, também julgamos que, em que pese o montante representar ínfima fração de recursos para o sistema financeiro, o total de recursos derivados do setor representam não só um ônus indevido aos correntistas, mas, também, uma fonte considerável de recursos para quadrilhas de diversos tamanhos e periculosidade.

Tendo feito esses reparos iniciais sobre o assunto, apresentaremos a seguir as principais conclusões desta Sub-Relatoria na questão dos crimes praticados contra correntistas de instituições financeiras.

2.1.3.1 Risco Operacional das instituições conforme o Banco Central

Na reunião realizada no Banco Central (Bacen) com representantes da área de fiscalização, em Dezembro de 2015, nos foi informado que a instituição não possui (e nem coleta) dados específicos relativos a crimes cibernéticos. No entanto, na ocasião foi sugerido que o risco operacional da instituição financeira, que é de informação obrigatória ao Bacen, englobaria as perdas ocasionadas por tais crimes. O indicador apresenta o grau de exposição de um banco e é derivado das características de seus negócios, por exemplo, dos tipos de créditos concedidos, perfil dos clientes, previsões devido a ações judiciais, crimes e sinistros sofridos, etc.

Para a obtenção de um Índice de Risco Operacional ponderado de acordo com o tamanho das instituições, o Bacen informou um procedimento para a sua extração, a partir das informações públicas constantes

do sistema Dados Selecionados de Entidades Supervisionadas - IF.data. Para a obtenção do índice relativo, basta dividir “Parcela do Risco Operacional” (representado pela sigla RWAOPAD no informe do Bacen) por “Risco Total Ponderado” (RWA).[25] Apresentamos a seguir os quocientes para os cinco bancos de varejo com maior RWA:

[25] As informações encontram-se disponíveis no sítio de internet do Bacen, no sistema Dados Selecionados de Entidades Supervisionadas - IF.data, sob o submenu Relatórios/Parcelas de Capital. Disponível em:

https://www3.bcb.gov.br/informes/relatorios?lingua=pt, acessado em 19/02/16.

Tabela - Índice de Exposição a Risco Operacional – Anualizado 2014/15 (4T14-3T15)

	dez/14			mar/15			jun/15			set/15			Média Anual
	RWA[1]	RWAOPAD[2]	Índice de Exposição	RWA	RWAOPAD	Índice de Exposição	RWA	RWAOPAD	Índice de Exposição	RWA	RWAOPAD	Índice de Exposição	Índice de Exposição
CEF	494	20,3	4,1%	533	33,6	6,3%	554,2	33,6	6,1%	564,9	40,4	7,2%	5,9%
Bradesco	597,2	31	5,2%	614,6	39,1	6,4%	607,2	38,1	6,3%	644	37,1	5,8%	5,9%
Santander	363,8	15,2	4,2%	379,2	18,6	4,9%	371,1	18,6	5,0%	389	17	4,4%	4,6%
Itau	768,1	36,8	4,8%	789	35,5	4,5%	736,6	35,5	4,8%	774,7	28,6	3,7%	4,5%
BB	786	39,7	5,1%	803,4	30,1	3,7%	791,1	30,2	3,8%	843,6	36,4	4,3%	4,2%

Nota: (1) RWA - Risco Total Ponderado e RWAOPAD - Parcela do Risco Operacional. Valores em R$ bilhões.

Fonte: Banco Central[26]

[26] Idem nota anterior.

O índice calculado apenas nas cinco maiores instituições de varejo aponta que, na média anualizada 2014/15, a Caixa e o Bradesco, proporcionalmente aos seus recursos, são os bancos que possuem maior risco operacional no período selecionado e o Banco do Brasil (BB), o menor. Cabe lembrar que os riscos operacionais envolvem todo e qualquer risco ao qual o banco está sujeito, desde a possibilidade de não pagamento de seus empréstimos, até os prejuízos causados por crimes cibernéticos. Em que pese essa ressalva, é correto dizer que a Caixa e o Bradesco são mais vulneráveis a riscos operacionais – de acordo com a natureza de seus negócios - do que o Itaú ou o Banco do Brasil.

2.1.3.2 Principais queixas dos consumidores de instituições financeiras relacionados a crimes cibernéticos, conforme o Bacen

O Banco Central disponibiliza o “Ranking de Instituições por Índice de Reclamações”. Nesse sistema, o Bacen permite ranquear as reclamações pelos tipos mais frequentes. Da análise dos dados, verificamos que o primeiro lugar da lista, “Irregularidades relativas à integridade, confiabilidade, segurança, sigilo ou legitimidade das operações e serviços”, é a mais afeita a crimes cibernéticos. A autoridade detalha que essa reclamação é “Para as situações em que há indícios de que a instituição financeira não assegurou integridade, confiabilidade, segurança ou o sigilo das transações realizadas, bem como a legitimidade das operações contratadas e dos serviços prestados." Expandindo esse item (o mais reclamado da lista) é apresentada a incidência por instituição. A seguir apresentamos a tabela resumo dessa reclamação para o segundo semestre de 2014 e primeiro de 2015, novamente apenas para os bancos que possuem maior risco operacional.

Tabela – Média do Índice de Reclamação Afeita a Crimes Cibernéticos(1) – Anualizado 2014/15 (4T14-3T15)

	2do. semestre de 2014			1ro. semestre de 2015			
	número de reclamações	milhões de clientes	índice da reclamação por milhão cliente	número de reclamações	milhões de clientes	índice da reclamação por milhão cliente	Média Anual. (2)
CEF	1001	73,7	13,6	1999	75,4	26,5	20,0
Santander	184	31,1	5,9	244	31,9	7,6	6,8
ITAU	147	56,9	2,6	318	58,5	5,4	4,0
Bradesco	249	74,1	3,4	330	75,4	4,4	3,9
BB	129	55,1	2,3	179	55,5	3,2	2,8

Nota: (1) Descrição do Bacen: “Irregularidades relativas à integridade, confiabilidade, segurança, sigilo ou legitimidade das operações e serviços.

(2) Média por milhão de clientes da instituição.

Fonte: Bacen[27]

Comparando a ordem desta última Tabela com aquela obtida no cálculo do índice de exposição ao risco operacional vê-se grande correlação entre os quesitos Índice de Exposição ao Risco Operacional e a Média do Índice de Reclamação Afeita a Crimes Cibernéticos. Enquanto na primeira a ordem era CEF, Bradesco, Santander, Itau e BB, nesta segunda relação a ordem é CEF, Santander, Itau, Bradesco e BB. Basicamente a alteração se deve ao fato de que o Bradesco, pelo fato de possuir muitos mais correntistas que os demais bancos (salvo a CEF), dilui a quantidade de reclamações, descendo no ranking. No entanto, a visão geral continua a mesma, os clientes da Caixa são mais propensos a serem vítimas de crimes cibernéticos, os do BB menos, e os das

[27] O ranking pode ser obtido em Perfis/Cidadão/Atendimento ao Público/ Reclamações contra instituições financeiras/Ranking de instituições por índice de reclamações. Disponível em: http://www.bcb.gov.br/?ranking, acessado em 19/02/16.

outras três instituições privadas encontram-se em posições intermediárias.

Todavia é preciso reconhecer que mais dados são necessários para elaborar um índice que avalie diretamente o risco a incidência a crimes cibernéticos de acordo com as instituições.

2.1.3.3 Projeto Tentáculos – Parceria Caixa e Polícia Federal

As operações da Polícia Federal na temática do crime cibernético são centralizadas pelo “Projeto Tentáculos”, capitaneado pelo Serviço de Repressão a Crimes Cibernéticos da Coordenação-Geral de Polícia Fazendária (SRCC/CGPFAZ), da Polícia Federal. Parte integrante do Projeto, o Banco Nacional de Fraudes Bancárias é um sistema que deveria centralizar as ocorrências desse tipo de fraudes, quando informadas pelas entidades participantes. O banco de dados e o projeto foram operacionalizados com a assinatura, em 2008, de um Termo de Cooperação Técnica com a Caixa Econômica Federal, sendo que em 2009 foi elaborado outro termo, desta feita com a Febraban, que prevê o repasse desses incidentes por parte das demais instituições financeiras. De acordo com informações da Polícia Federal, o projeto foi operacionalizado apenas com a Caixa.

Esta Subrelatoria recebeu o Despacho 43/2016 – SRCC/DICOR/DPF, da Polícia Federal, com o detalhamento dos crimes cibernéticos encaminhados pela Caixa, com base nesse Termo de Cooperação no âmbito do Projeto Tentáculos. Segundo o informe, desde o ano de 2009, a instituição repassou mais de meio milhão de processos de fraude com cartões de débito e internet banking para serem investigados, totalizando R$ 1,1 bilhão em montantes fraudados, conforme tabela abaixo.

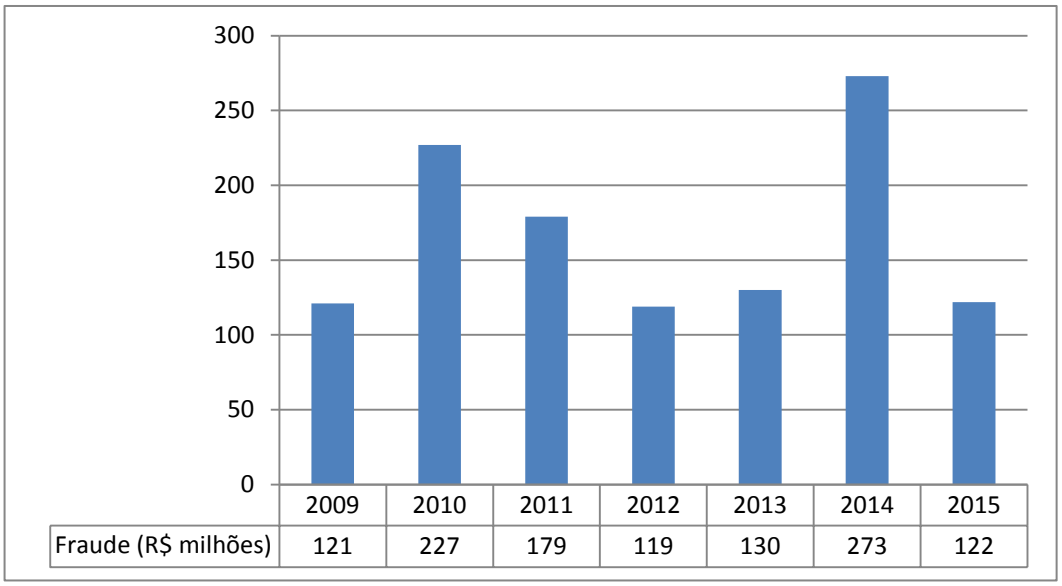


Gráfico - Fraudes de internet banking e clonagem de cartões comunicadas pela Caixa (R$ milhões)

Fonte: Despacho 43/2016 –SRCC/DICOR/DPF da Polícia Federal

As informações repassadas dão conta de que o pico dessas fraudes contra a instituição pública ocorreu em 2014, totalizando R$ 273 milhões somente naquele ano. Entretanto, não é possível verificar nenhuma tendência clara para o futuro próximo, o que indica que mais precisa ser feito pela Polícia Federal. Certamente, não é possível atacar o problema do crime cibernético contra instituições financeiras monitorando apenas a Caixa. As outras instituições financeiras também deveriam participar do Projeto Tentáculos e alimentar o seu banco de dados.

Nesse sentido, o Despacho encaminhado pela Polícia Federal também indica os bancos destinos das fraudes cometidas contra a Caixa. Como exarado no documento, “os criminosos cibernéticos fazem uso de todo o sistema bancário nacional nas transações fraudulentas”.

Tabela – Destino dos recursos fraudados da Caixa

Banco	**Valor [R$ milhões]**
Bradesco	15,6
Itaú	9,4

BB	5,6
Santander	3,0
HSBC	0,8
BNB	0,6
BrB	0,3

Fonte: Despacho 43/2016 –SRCC/DICOR/DPF da Polícia Federal

A análise da tabela anterior indica que os principais bancos de varejo são utilizados pelos criminosos como ferramentas para consecução dos crimes perpetrados contra a Caixa.

2.1.3.5 Conclusão e ações a serem tomadas

Em primeiro lugar é importante salientar que não pudemos comprovar e nem encontrar a fonte primária da informação de que ocorrem no Brasil R$ 900 milhões anuais em fraudes bancárias cibernéticas. Todavia, para o caso da Caixa é possível calcular a proporção dos crimes cibernéticos na Parcela do Risco Operacional da instituição, por conta dos dados encaminhados no citado Despacho.

Tendo em conta que o total anual desse tipo de fraudes na Caixa em 2015 foi de R$ 122 milhões e anualizando o total de “Parcela de Risco Operacional” trimestral daquela instituição para o mesmo ano de 2015 (20,3+33,6+33,6+40,4 = R$ 127,9 bilhões), determinamos que a contribuição dos crimes cibernéticos para o risco operacional da instituição é de, aproximadamente, 0,1%.

Para efeitos de se estimar o total de crimes cibernéticos praticados no País e na inexistência de outros dados informados pelas instituições financeiras, consideraremos que todos esses principais bancos possuem essa mesma preponderância de crimes cibernéticos: 0,1% do risco operacional da instituição. Faremos essa inferência, apesar de já termos salientado o fato de que as instituições possuem perfis e ativos e passivos distintos. Todavia, é importante ressaltar também que, conforme os termos do Despacho, os dados “não contemplam as fraudes cometidas com cartões de crédito”. Portanto, mesmo

considerando que os crimes cometidos contra a Caixa são maiores e mais numerosos do que contra as demais instituições, existe uma gama muito ampla de golpes cibernéticos que não foram totalizados pelo Banco Nacional de Fraudes Bancárias. Assim, a estimativa de 0,1% do risco operacional pode ser considerada como sendo conservadora.

Com base em nossa projeção de 0,1% da Parcela de Risco Operacional fornecemos a tabela abaixo que contempla nossa estimativa anual para os crimes cibernéticos acometidos contra as principais instituições do país.

Tabela – Estimativa mínima de crimes cibernéticos nas principais instituições em 2015

Instituição	**Estimativa Crime Cibernético Anual [R$ milhões]**
CEF	127,9
Bradesco	145,3
Santander	69,4
Itau	136,4
BB	136,4
Total	**615,4**

Nota: Estimou-se em 0,1% da Parcela do Risco Operacional anual das instituições

Em que pese essa taxa percentual de 0,1% do risco operacional seja baixa comparado com o tamanho do sistema financeiro, deve ser considerado que essas fraudes abastecem organizações criminosas com vultosas quantias. Conforme estimado na Tabela anterior, mais de R$ 600 milhões são drenados das principais instituições financeiras e abastecem o submundo do crime. Cabe ressaltar que nossa estimativa, conservadora, se aproxima no valor propalado por diversas vezes na CPI e na imprensa de que os crimes cibernéticos beiram os R$ 900 milhões anuais. Nas palavras da Polícia Federal:

"Os expressivos números... demonstram também o alto poder lesivo deste crime, gerando um grande impacto para a sociedade e, por consequência, financiando a cibercriminalidade organizada." (Despacho 43/2016 –SRCC/DICOR/DPF da Polícia Federal)

Por fim, o citado Despacho aponta para algumas soluções legais de auxílio ao combate ao crime cibernético, sobre as quais faremos um rápido comentário. Dentre as sugestões que não tinham sido vislumbradas por esta CPI encontra-se a necessidade de regulamentação do inciso VI, do art. 1º da Lei nº 10.446/02, *Lei das Infrações Federais*. A normatização deverá exigir dos bancos a notificação compulsória desse tipo de ocorrência. Isso se faz necessário para permitir a repressão uniforme em todo o país das fraudes bancárias. Também como forma de dar maior uniformidade e celeridade ao tratamento desses crimes, verificou-se a necessidade da criação de Varas Judiciais Especializadas em Crimes Eletrônicos. Mediante esses organismos seria possível a criação e a especialização de equipes também no âmbito da justiça. Por fim, observou-se que os criminosos possuem vultosos bens que poderiam ser perdidos em favor do Estado como forma de reparação pelos danos causados e utilizados em favor da repressão a esses mesmos tipos de crimes. Tal medida seria mais uma ação coercitiva e teria o amparo constitucional constantes nos incisos XLV e XLVI, do artigo 5º da Constituição Federal.

Desta análise concluímos pelo encaminhamento das seguintes ações que deveriam ser implementadas pelas autoridades mencionadas:

1. **Determinar ao Bacen a contabilização, por separado, em seu sistema de atendimento ao público Reclamações contra Instituições Financeiras as fraudes cibernéticas;** (Parte III, 3.2)

2. **Indicar ao Ministério da Justiça a necessidade de regulamentação do inciso VI, do art. 1º da Lei nº 10.446/02, *Lei das Infrações Federais*, assim como ao Bacen, por intermédio do Ministério da Fazenda, o estabelecimento de regulamentação que obrigue as instituições financeiras a notificar a ocorrência de fraudes cibernéticas;** (Parte III, 3.2

e 3.3)

3. **O Bacen e a DPF deverão estabelecer entendimentos para o compartilhamento das informações e a manutenção de um Banco (de Dados) Nacional de Fraudes Bancárias;** (Parte III, 3.2 e 3.3)

4. **Oferecimento de Projeto de Lei permitindo o perdimento de bens de criminosos;** (Parte III, 1.1)

5. **Oferecimento de Indicação para a criação de Varas Judiciais Especializadas em Crimes Eletrônicos.** (Parte III, 3.4)

2.1.4 Violação de direitos autorais na internet

Quanto à violação de direitos autorais na internet, esta CPI não teve tempo hábil para se debruçar sobre a legislação específica do tema. Todavia, entendemos que a legislação vigente é insuficiente, uma vez que não prevê qualquer mecanismo efetivo que permita à autoridade judicial bloquear junto às operadoras o acesso a sítios de internet que distribuam conteúdos protegidos distribuídos de maneira ilegal, os chamados “sites de conteúdos piratas”.

Esta comissão de inquérito deu uma grande contribuição para a mitigação desse tipo de crime com o oferecimento da denúncia sobre o qual já relatamos aqui no item anterior e que culminou com a operação Barba Negra. No entanto, entendemos que há um vácuo legal que deve ser preenchido. Aqueles sítios de internet que veicularem majoritariamente conteúdo protegido por direito autoral devem ter seu acesso possível de ser bloqueado junto às operadoras de conexão à internet mediante ordem judicial.

Cumpre notar que essa questão já vem sendo tratada, por exemplo, no âmbito da União Europeia, com a aprovação da Regulação (EU)

2015/2120 no Conselho e no Parlamento europeus, em 25 de novembro de 2015. A referida Regulação prevê, no artigo 23, intitulado “Liberdade para prover e dispor de acesso à internet aberta e gerenciamento razoável de tráfego”, a possibilidade de restrição de acesso a conteúdo específico mediante ordem judicial.

Ressalte-se, porém, que se encontra em andamento nesta Casa Legislativa a Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 3.968, de 1997, e na qual os temas atinentes aos direitos autorais, em todas as suas nuances, estão sendo amplamente debatidos.

Por tanto, sugerimos a apresentação de Projeto de Lei **que possibilita a adoção de medidas que poderão chegar até ao bloqueio, por ordem judicial, de aplicações de internet consideradas ilícitas, quando ofertadas no exterior por empresas sem representação no país**. Ressalte-se que esse projeto foi elaborado em conjunto com as demais Sub-Relatorias.

2.2 – SUB-RELATORIA DE CRIMES CONTRA A CRIANÇA E O ADOLESCENTE (SUB-RELATOR DEPUTADO RAFAEL MOTTA)

2.2.1 – Educação para o uso seguro da internet

No âmbito das investigações desta Sub-Relatoria, foram realizadas importantes audiências públicas, com representantes de diversas entidades governamentais e não governamentais, personalidades e estudiosos do tema. Dentre os ouvidos, contamos com a presença do senador Magno Malta (PR-ES), que presidiu as investigações da CPI da Pedofilia do Senado Federal.

Todos os participantes dessas audiências, em especial aqueles cuja atuação está direta ou indiretamente ligada à área da Educação, foram unânimes em afirmar a necessidade do aumento da proteção a crianças e adolescentes no uso da internet. Diante da recorrência de depoimentos nesse sentido, observou-se a importância de se incluir o uso seguro da internet no conteúdo curricular dos ensinos Fundamental e Médio.

Argumentando em favor dessa constatação, dados apresentados pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (Unesco) revelam que 38% dos adolescentes brasileiros entre 11 e 17 anos costumam adicionar pessoas que não conhecem à lista de amigos nas redes sociais. A mesma pesquisa da Unesco mostra que apenas 8% dos pais acham que os filhos dessa faixa etária possam ser alvo de assédio ou de outro tipo de constrangimento na internet.

Esses números reforçam a necessidade de se trabalhar a educação digital com crianças e adolescentes, a partir de um planejamento sério, elaborado e que abranja todo o país.

Nesse particular, o Ministério Público Federal já despertou para a necessidade de implementar ações efetivas de educação dos internautas, especialmente os mirins. A Portaria PGR/MPF nº 753/15, instituiu projeto “Ministério Público pela Educação Digital nas Escolas” preparando os jovens internautas no uso seguro da internet.

Durante audiência pública desta CPI realizada em Natal-RN, no início do mês de outubro de 2015, por proposição do nosso mandato, o depoimento do professor especialista em Segurança de Redes e Perícia Forense Computacional do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN), Ricardo Kleber Martins Galvão, tornou ainda mais clara a necessidade de instrução quanto ao uso da internet por esse público. O especialista destacou, em sua fala, que geralmente crianças e adolescentes acessam o mundo virtual sem qualquer orientação em casa ou no ambiente escolar, tornando-se vulneráveis e vítimas em potencial para crimes cibernéticos.

Da mesma opinião compartilha o juiz federal Mario Azevedo Jambo, da 2ª Vara Federal do nosso Estado, que também foi ouvido no encontro realizado em Natal. O magistrado apontou a necessidade de discussão aberta com as crianças e os adolescentes por parte da família e, principalmente, das escolas, expondo os riscos reais da internet, para que haja uma considerável conscientização por parte desses usuários.

O ideal, portanto, seria viabilizar a segurança digital como conteúdo perene e obrigatório em sala de aula, tanto nas escolas públicas quanto privadas do Brasil, configurando-se uma importante política de prevenção. O artigo 26 do Marco Civil da Internet, aliás, prevê que “o cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico”. Nesse sentido, o Projeto de Lei nº 2801/2015, do Deputado JHC é extremamente acertado, pois considera fundamental a educação digital de crianças e de jovens.

Porém, tendo em vista que a Comissão de Educação da Câmara dos Deputados possui a Súmula de Recomendações aos Relatores de número 1, de 2013, que determina que a criação de disciplina ou qualquer alteração curricular deve ser encaminhada exclusivamente via Indicação, julgamos mais conveniente propor duas medidas:

i) a **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, o Ministério Público Federal e Poder Executivo, no sentido de promover ações educativas para o uso seguro da internet por crianças e adolescentes nas escolas, em consoante com os objetivos da Portaria PGR/MPF nº 753/15,. (Parte III, 5.e)

ii) o envio de **Indicação ao Ministério da Educação para a oferta obrigatória de noções de educação digital nas escolas públicas e privadas** de ensino fundamental e médio, assim como para incluir expressamente a promoção da educação digital como uma das diretrizes do Plano Nacional de Educação (PNE). (Parte III, 3.5)

2.2.2 – Inclusão no rol de crimes hediondos dos crimes relacionados à exploração sexual de crianças ou adolescentes mediante o uso da internet

Esta CPI tem a consciência de que a internet e as redes sociais amplificam os danos causados por mensagens, imagens e vídeos veiculados com o intuito de denegrir, manchar a honra ou violar a privacidade e a intimidade de pessoas. Essa amplificação se dá pela facilidade da replicação infinita dos conteúdos digitais sem custo, pela impossibilidade de erradicação definitiva dos materiais e pela consequente incapacidade de qualquer possibilidade de direito ao esquecimento.

Esses acontecimentos são ainda piores quando se trata de crianças e adolescentes. Foram inúmeros os relatos de autoridades policiais e de entidades a esta CPI acerca das nefastas consequências para as crianças e suas famílias quando imagens de pedofilia são veiculadas na internet. Foram relatados, inclusive, casos de suicídio e de abandono de lar e de escola, em decorrência da circulação de conteúdo desse tipo.

Esta CPI entende que uma das razões para a proliferação desse mal digital é a impunidade. Por isso, **apoiamos a aprovação do Projeto**

de Lei 1.776/15, em tramitação, que tornam crimes hediondos delitos ligados à pedofilia. (Parte III, 3)

2.2.3 – Previsão de bloqueio, por meio de decisão judicial, dos sites que disponibilizam conteúdos ilícitos.

A internet, como se sabe, desde o seu surgimento, trouxe enormes benefícios à sociedade, com destaque para a multiplicação das fontes de conhecimento, a dinamização das relações sociais e o encurtamento de distâncias. Porém, infelizmente, da mesma forma que a internet pode ser usada – e de fato o é – para a realização de coisas boas, essa ferramenta também vem sendo utilizada como ambiente para a prática de diversos crimes, até mesmo contra crianças e adolescentes, conforme amplamente demonstrado nesta CPI.

Inclusive, não é novidade para usuários da rede mundial de computadores do Brasil a existência de sites voltados quase que exclusivamente à disponibilização e compartilhamento de conteúdo ilícito, violando a legislação nacional. Dentre os quais, registre-se, sítios com imagens e vídeos com conteúdo pedófilo ou com mensagens cujo teor representa declarada apologia à pedofilia.

Dessa forma, mostra-se importante inserir no Marco Civil da Internet uma exceção à regra geral de neutralidade de rede que ratifique ao Poder Judiciário brasileiro a possibilidade de determinar aos provedores de conexão medidas técnicas de bloqueio de tráfego, como já acontece em outras democracias ocidentais, a exemplo de países da União Europeia, Estados Unidos e Chile.

Assim, ainda que não se consiga fazer com que o hospedeiro estrangeiro apague o conteúdo que afronta a legislação brasileira de seus servidores, o acesso a qualquer provedor de conteúdo ilícito será prejudicado pela medida técnica implementada por provedores brasileiros de conexão. Por essa razão, **apresentamos um projeto de lei nesse sentido,** com o objetivo de tornar a internet um ambiente mais seguro e livre da ilegalidade (Parte III, 1.7).

2.3 – SUB-RELATORIA DE CRIMES CONTRA A HONRA E OUTRAS INJÚRIAS (SUB-RELATOR DEPUTADO DANIEL COELHO)

2.3.1 – Retirada de conteúdos infringentes repetidos

Na questão da remoção de conteúdos atentatórios, o estudo do assunto e as oitivas realizadas pela CPI nos indicam que as disposições do MCI dificultam a manutenção da exclusão de conteúdos criminosos quando estes são replicados. Uma vez que no texto legal (§1º, do artigo 19) há a menção expressa à "localização inequívoca do material", alguns dos principais aplicativos de internet tem procedido apenas a remoções de endereços específicos apontados em decisões judiciais. Assim, quando os mesmos conteúdos são postados em outra página, ou por outro usuário, os responsáveis pelo sítio têm exigido nova ordem judicial apontando esse novo endereço a ser removido. Essa prática é extremamente danosa para a vítima, pois as facilidades inerentes aos meios digitais, relatados anteriormente, tornam a prática do crime ininterrupta.

Assim, o sistema atual é injusto com a vítima, pois as disposições do MCI obrigam a vitima a entrar na justiça contra cada ocorrência do conteúdo. Essa metodologia tem consequências nefastas para vítimas, pessoas comuns, celebridades, ou pessoas investidas de cargo público ou político.

No caso específico do processo eleitoral, tendo em vista os prazos exíguos das campanhas, os ataques pelas redes sociais são impossíveis de serem coibidos em tempo hábil, sendo o dano eleitoral irreparável, com graves consequências para o processo democrático.

No estudo da matéria foram sugeridas diversas propostas para regulamentar o assunto. Após profícuo debate com Parlamentares, instituições e membros da sociedade organizada, entendemos que o CGI.br apresentou contribuição que mais se aproxima do entendimento por parte dos membros desta Comissão e será, portanto, acatada em sua quase totalidade. Assim, como é o entendimento desta Sub-Relatoria, a proposta determina que conteúdos idênticos devem ser retirados após notificação por parte do usuário. No entanto, a sólida instituição técnica indica que essa retirada também deva se dar

em casos de conteúdos “que contenham parte majoritária e que reproduza a infração decorrente do conteúdo removido por ordem judicial”. As discussões salientaram o fato de que a introdução de elementos de subjetividade poderia levar ao uso extremado de retiradas como medida de precaução por parte dos provedores de aplicação e seria, consequentemente, danoso para o desenvolvimento saudável da internet. Portanto, não consideramos a melhor solução essa extensão. Por outro lado, o CGI.br não estabelece prazos para a retirada, o que entendemos ser deletério para a manutenção da proteção dos usuários.

Por isso, sugerimos apresentar um Projeto de Lei para que a retirada de conteúdos replicados seja feita em 48 horas, a pedido do usuário, no caso em que decisão judicial já tenha reconhecida a infringência do conteúdo.

Por fim, constatamos que tramitam, nesta Casa Legislativa, alguns projetos de lei que, pela pertinência do tema neles tratados, merecem ser amplamente discutidos. São eles:

a) Projeto de Lei nº 5555/2013 e seus apensados, que tratam da divulgação não autorizada de imagens íntimas das vítimas. Essa conduta, que tem se tornado comum no meio virtual, realmente demanda uma atuação mais enérgica por parte do Estado, razão pela qual manifestamos apoio a estas proposições;

b) Projeto de Lei nº 3686/2015, que “*tipifica o crime de intimidação sistemática (Bullying), prevendo causa de aumento se a conduta for realizada por meio da internet (Cyberbullying)*”;

c) Projeto de Lei nº 7544/2014, que tipifica a conduta de incitação virtual ao crime;

d) Projeto de Lei nº 1755/2015 e apensados, que tratam da criminalização da divulgação indevida, na internet, de informações pessoais.

2.3.2. – Sobre o acesso ao endereço IP utilizado para a geração de conteúdo específico objeto de investigação criminal

Esta Sub-Relatoria verificou, também, que as autoridades de investigação (autoridade policial e Ministério Público) têm encontrado dificuldades para obter o endereço IP utilizado para a geração de determinado conteúdo criminoso, objeto de investigação.

Mediante a sistemática atual, para se obter o usuário que se encontra por trás de determinado endereço IP é necessário recorrer a mandado judicial e realizar o processo de quebra em três etapas. Primeiro junto ao aplicativo, segundo, junto à autoridade de registro da internet e, terceiro, junto à operadora de telefonia. Diversas autoridades indicaram a demora desses processos por diversos motivos. Desde a recusa no atendimento a solicitações por parte de empresas de internet que possuem suas bases de dados no exterior, até a falta de disponibilidade de juízes de plantão para emissão de ordens judiciais que autorizem a quebra do sigilo nas diversas etapas.

Para alterar essa realidade, seria necessário que as autoridades de investigação obtivessem acesso, independentemente de ordem judicial, do endereço IP utilizado para a geração de determinado **conteúdo criminoso, objeto de investigação**. Essa ótica vislumbra franquear o acesso a autoridades de investigação a dados de internauta que tenham publicado **conteúdo criminoso** na internet e que já sejam objeto de investigação.

Fundamental destacar nesta sistemática que, processos de investigação criminal são todos remetidos ao Ministério Público, o que por si só já garantiria a verificação de supostas irregularidades ou mau uso de prerrogativas. Nesse particular, eventuais utilizações indevidas das informações recebidas seria considerado crime. Dessa maneira, internautas que não tivessem acometido nenhum tipo de crime possuiriam a garantia de manutenção de sua intimidade. Já aqueles que se utilizarem da internet para o acometimento de crimes seriam identificados mais rapidamente.

Importante ressaltar nesta discussão que o endereço IP do dispositivo utilizado é um dado de identificação distinto de conteúdo e sua

requisição não deve ser confundida com interceptação de comunicações telemáticas.

Aliás, a legislação brasileira já autoriza a requisição direta, por parte do Ministério Público e da autoridade policial, de dados cadastrais (art. 15 da Lei nº 12.850/13 – Lei das Organizações Criminosas, art. 17-B da Lei nº 9.613/98 – Lei da Lavagem de Dinheiro, e art. 10, § 3º, da Lei nº 12.965/2014 – Marco Civil da Internet). Dessa forma, a autoridade de investigação pode, por exemplo, pedir a uma empresa telefônica, sem a necessidade de ordem judicial, a qualificação pessoal (nome, nacionalidade, naturalidade, data de nascimento, estado civil, profissão, número da carteira de identidade , etc.), a filiação e o endereço de um cliente que esteja sendo investigado.

Uma das possíveis críticas a essa possível nova sistemática de investigação diz respeito a possíveis abusos cometidos por autoridades. De acordo com contribuição recebida por esta CPI do Instituto Beta, Coding Rights e Intervozes, dados da Ouvidoria de polícia de São Paulo, entre 1998 e 2014, indicam a investigação de 591 delegados, a partir de denúncias na Ouvidoria, que resultaram em 144 punições. Houve também 10 investigações contra agentes de telecomunicações, com quatro policiais punidos. Esses são dados alarmantes que devem ser levados em consideração por parte dos legisladores. Assim, projetos nesse sentido devem determinar claramente que a utilização indevida de endereço IP configurará crime.

Esta discussão do acesso ao endereço IP por autoridade de investigação é matéria de elevado interesse no Congresso Nacional. Em 18/04/16, portanto durante o tramo final dos trabalhos desta CPI, o Senado Federal aprovou o PLS 730/2015 (PL 5074/2016), de autoria do Senador Otto Alencar. A proposição permite o acesso aos dados cadastrais associados a determinado endereço IP, limitando essa obtenção apenas à qualificação pessoal, filiação e endereço do suspeito de prática de crime por intermédio da internet.

Entendemos que o Senado Federal obteve o tempo necessário para madurar uma proposta concreta que regulamente a requisição de dados de internauta de forma célere, em casos de investigação criminal. Por isso, esta Casa poderá aprimorar a solução oferecida e concluir por uma peça legal consistente, moderna, que respeita as garantias individuais, mas que possa, também, tornar a internet um lugar mais seguro..

Pelos motivos expostos e com o objetivo geral de aumentar a eficácia das investigações, propomos a análise do **Projeto de Lei do Senado 730, de 2015 (que recebeu, na Câmara, o nº 5074/2016), que dispõe sobre investigação criminal e a obtenção de meios de prova de crimes praticados na internet**. Ressaltamos que a recomendação aqui expressa não significa que estamos propondo sua aprovação, apenas que reconhecemos a importância da matéria e a necessidade de posicionamento do Parlamento brasileiro. Ademais a análise deve levar em consideração os princípios emanados no Marco Civil da Internet.

2.3.3 – Elaboração de tipo penal específico para a divulgação de fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima

Outro ponto que foi bastante criticado por diversas autoridades que prestaram esclarecimentos a esta CPI (sobretudo na audiência pública realizada no Dia Internacional da Mulher) diz respeito à brandura com que a legislação penal atual tem tratado a gravíssima conduta de divulgação não autorizada de material de conteúdo sexual (a popularmente conhecida "pornografia de vingança" ou "vingança pornô"). É importante compreender que esse tipo de crime, quando praticado pela internet, incorre em dano continuado e de muito maior alcance do que pelos meios tradicionais. Pelo fato da mídia digital ser invasiva, onipresente e praticamente indelével, as vítimas são acossadas por esse tipo de prática de maneira muito mais intensa. Por isso, a questão da vingança pornô já vem sendo tratada de maneira específica em diversos países. Nos Estados Unidos, vários estados da federação aprovaram recentemente leis específicas.

No Brasil, porém, conforme esclarecido, esses casos são enquadrados, hoje, no crime de injúria, cuja pena máxima é de seis meses de detenção, e que se processa mediante ação penal privada (ou seja, se a vítima quiser processar criminalmente o agressor, terá que contratar um advogado para apresentar a queixa-crime). Ocorre que, pelas razões expostas acima, o alcance da injúria pela internet é infinitamente maior do que aquela causada à pessoa

pelos meios previstos originalmente no Código Penal, de 1940.

A gravidade desse crime, portanto, demanda uma atuação mais rigorosa por parte do Estado nos dias de hoje.

Por essa razão, inclusive, já existem diversos projetos em andamento nesta Casa que tratam do assunto (Projeto de Lei nº 5555/2013 e seus apensados). Dessa forma, neste particular, **sugerimos o apoio à aprovação do PL 5555/2013 e apensados, após, evidentemente, sua ampla discussão pelo Parlamento**.

2.4 – SUB-RELATORIA DE SEGURANÇA CIBERNÉTICA NO BRASIL (SUB-RELATOR DEPUTADO RODRIGO MARTINS)

2.4.1 – 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, **oferecemos Projeto de Lei aperfeiçoando a redação do tipo penal em comento,** em grande parte inspirado no projeto do novo Código Penal brasileiro, ainda em trâmite no Senado Federal**.** (Parte III, 1.2)

2.4.2 – Guarda dos registros de conexão por todos os provedores de internet e migração para o IPv6 ou tecnologia similar

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[28].

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 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

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

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;** (Parte III, 5) **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 ou de tecnologia similar no país**. (Parte III, 3.6)

2.4.3 – 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, o Ministério Público Federal e Poder Executivo, no sentido de promover ações educativas continuadas para o uso seguro da internet por adultos.** (Parte III, 5.e)

2.4.4 – 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, e obteve as seguintes respostas:

Unidade Federativa	*Resposta*	*Data*
Acre	A CPI não obteve resposta até o fechamento do Relatório.	
Alagoas	A CPI não obteve resposta até o fechamento do Relatório.	
Amapá	Não dispõe de Delegacia de Combate aos Crimes Cibernéticos, por isso não há como fornecer as informações solicitadas. Ressalta-se que está prevista a criação de Delegacia de Combate aos Crimes Cibernéticos, logo que for possível a	14/04/2016

	realização de concurso público.	
Amazonas	Não há setores e equipes especializados no combate a crimes cibernéticos. Existe uma proposta de reestruturação da Polícia Civil para ampliar a atuação da atual Delegacia Interativa e transformá-la em Delegacia Interativa e Especializada em Crimes Cibernéticos - DIECC. O mínimo para o funcionamento desta Delegacia seria de um delegado, 2 escrivães e 6 investigadores. No momento, não há estrutura disponível. Não há treinamento específico e a Delegacia Interativa não realiza procedimentos policiais, por isso não há procedimentos instalados referentes à criminalidade cibernética.	12/04/2016
Bahia	A CPI não obteve resposta até o fechamento do Relatório.	
Ceará	A CPI não obteve resposta até o fechamento do Relatório.	
Distrito Federal	Não há unidade, setor ou equipes especializadas no combate à ação dos crimes cibernéticos, pois a Seção de Investigação de Crimes de Alta Tecnologia, da Divisão de Inteligência Policial da Polícia Civil do DF, foi extinta pelo Decreto Distrital nº 33.483, de janeiro de 2012. Os demais esclarecimentos foram prejudicados em decorrência deste fato.	14/04/2016
Espírito Santo	A CPI não obteve resposta até o fechamento do Relatório.	
Goiás	A CPI não obteve resposta até o fechamento do Relatório.	
Maranhão	Atualmente há uma equipe composta por um Delegado, um Escrivão, 3 Investigadores e um	19/04/2016

	Administrativo, quantidade que necessitaria ser maior com o ideal de 2 Delegados, 2 Escrivães, 10 Investigadores(com conhecimento em TI, especificamente em software de relacionamento) e 2 Administrativos. A unidade de combate ao crime cibernético é denominada Departamento de Combate ao Crime Tecnológico e encontra-se em uma sala no prédio da Superintendência Estadual de Investigações Criminais e dispondo de 2 computadores, 4 mesas, 2 armários, um telefone celular, 2 aparelhos de ar condicionado e 4 viaturas. O ideal seria a instalação em um prédio independente com estrutura de Delegacia Especializada, melhorias das técnicas e meios de investigação e redimensionamento do efetivo. Há treinamento uma vez por ano como o Curso previsto de Investigação Cibernética e Crime Organizado, mas há necessidade de mais cursos e maior disponibilidade de vagas. Em 2015, foram instaurados 5 inquéritos e 4 TCOs. Em 2015, até março, foram lavrados 4 TCOs. O índice de solução é de 100%.	
Mato Grosso	A CPI não obteve resposta até o fechamento do Relatório.	
Mato Grosso do Sul	A equipe é composto de 1 Delegado de Polícia, 1 Investigador de Polícia, apoiados quando necessário por mais de 9 Investigadores de Polícia (atuam no suporte técnico de Sistema Integrado de Gestão Operacional). Tanto a quantidade de servidores quanto a estrutura disponível, são adequadas para a demanda atual. Além da formação policial inicial, participaram do "Curso de atualização do sistema SIGO", em junho de 2015. Sobre os inquéritos policiais, se faz necessário estabelecer um lapso temporal	25/04/2016

	inicial e final.	
Minas Gerais	A CPI não obteve resposta até o fechamento do Relatório.	
Pará	A CPI não obteve resposta até o fechamento do Relatório.	
Paraíba	Não dispõe de setores ou equipes especializadas no combate à ação de crimes cibernéticos, não possuindo, desta maneira, profissionais ou estrutura. Informaram que já ocorreram 5 edições do Curso de Técnica de Investigação em Crimes Cibernéticos na Academia de Ensino da Polícia, entre 2009 a 2015, não periódicos. A Polícia Civil não consta com sistema informatizado para levantamento do número de inquéritos instaurados referentes a crimes cibernéticos. Sendo uma pesquisa manual, o lapso temporal para resposta foi insuficiente para o fornecimento dos dados.	19/04/2016
Paraná	Existe, desde 2005, o Núcleo de Combate aos Cibercrimes – NUCIBER. A equipe é composta por um Delegado, 4 Escrivães, 10 Investigadores, 3 Estagiários acadêmicos de Direito e um Estagiário de nível médio. Parte deste quadro integram equipes específicas no combate à pedofilia e outros crimes de alta complexidade, visando dinamizar as investigações. O atual contingente do quadro necessitaria ser quadriplicado, para atender o atual volume das demandas. Recomenda-se a implantação de divisões específicas para facilitar os tramites administrativos e otimizar a comunicação com as unidades federativas. A sede está localizada em um prédio alugado, compartilhado com outras unidades da Polícia	14/04/2016

	Civil. Possui 4 viaturas, 3 delas descaracterizadas, com mais de 8 anos de uso. Também, desktops e notebooks, alguns adquiridos pelo Estado, outros doados pela Receita Federal, em 2013. Não possui softwares específicos. Sugere-se que a estrutura fosse fortalecida com pelo menos mais 4 viaturas descaracterizadas; maletas forenses do tipo "Cellebrite"; maletas duplicadoras de HDs; impressoras a laser coloridas; Softwares de análise forense; softwares de análise de vínculos em investigações; sistema "guardião" para operacionalização de interceptações telefônicas; drones; binóculos e furgão. Também sugere-se a criação de subunidades em cidades polos do Paraná, projeto que já foi apresentado à Secretaria de Segurança Pública. No quadro há policiais com formações em Direito; Engenharia Elétrica, com ênfase em Eletrônica e Telecomunicações; Ciências da Computação; Processamento de Dados; Informática e Sistemas de Informação. Os policiais, esporadicamente, frequentam cursos ofertados pela ABIN e Secretaria Extraordinária de Segurança para Grandes Eventos do Ministério da Justiça – SESGE/MJ. Entretanto os cursos não contemplam a totalidade dos policiais e são esporádicos. Ressalta-se que devido às restrições de acesso a informações essenciais para a investigação cibernética, como ordem judicial para obter logs de acesso de um usuário, reforça-se a necessidade de cursos específicos e *hackerismo*(dentro da legalidade). Os número atuais de procedimentos são 3865 inquéritos, sento 316 na Delegacia e 3549 na Justiça; 4440 TCIPs; 541 apoios e 385 investigações	

	preliminares. O índice de elucidação gira em torno de 90%, sendo que os 10% de insucesso decorrem da negativa de prestação de informações por operadoras de telefonia, provedores de acesso, provedores de aplicação; desinteresse das vítimas em dar continuidade as investigações e a utilização de recurso denominado NAT (network addres translation), que muitas vezes impossibilita a identificação do usuário.	
Pernambuco	A CPI não obteve resposta até o fechamento do Relatório.	
Piauí	A CPI não obteve resposta até o fechamento do Relatório.	
Rio de Janeiro	A CPI não obteve resposta até o fechamento do Relatório.	
Rio Grande do Norte	A CPI não obteve resposta até o fechamento do Relatório.	
Rio Grande do Sul	Há setor especializado, Delegacia de Repressão aos Crimes Cibernéticos – DRCI, ligada ao Departamento Estadual de Investigações Criminais – DEIC, com a atribuição de combate ao crime informático. Existem 5 policiais civis lotados da DRCI/DEIC e um delegado. Entende-se que seriam necessários, devido a demanda, ao menos 14 policiais civis. Também seria importante, ao menos um analista se sistemas/analista forense computacional e de redes, para pareceres técnicos e instrução qualificada de inquéritos. A estrutura disponível atende as necessidades básicas de hoje, com o aumento do quantitativo de policiais civis seriam necessários o aumento do espaço e de	14/04/20106

	equipamentos. Como treinamento existe o Curso EAD/SENASP/MJ, que traça diretrizes básicas a respeito de investigação e instrução de procedimentos criminais, em se tratando de crimes informáticos, disponibilizados anualmente. Eventualmente existem outros cursos na área. Sugere-se convênios com escolas especializadas na área bancária e escolas de informática especializadas em forense computacional e de redes. Existem hoje 258 inquéritos na DRCI. Não há estatística de índice de solução. Descrevem como dificuldade a necessidade de "autorização judicial" para praticamente todo e qualquer ato investigatório. Tem-se a remessa média elucidada de 45% com autoria conhecida (ref. 2010 a 2015).	
Rondônia	A estrutura do Núcleo de Tecnologia da Gerência de Estratégia e Inteligência - GEI é a mesma utilizada para outras demandas de instalação, manutenção e assistência técnica. Não dispõe de equipes especializadas no combate aos crimes cibernéticos. Quatro servidores participaram de um único treinamento do Curso de Inteligência Cibernética, pela SENASP. Em outro ofício enviado posteriormente, informaram que não há equipes especializadas no combate à ação dos Crimes Cibernéticos e que a implementação exige a criação de cargo específico ou cursos de formação, o que exige ampliação orçamentária. Também informou que, devido ao prazo exíguo, não há filtros para colher a quantidade de inquéritos policiais instaurados relacionados a criminalidade cibernética.	07/04/2016

Roraima	Não há Delegacia ou Núcleo ou Setor especializado em Crimes Cibernéticos. No entanto, o Setor de Perícias em Material Audiovisual e Eletrônico – SEPAEL, subordinado ao Instituto de Criminalística, supri de alguma forma a demanda. Entretanto não há previsão da SEPAEL para combate a crimes cibernéticos, sendo necessária, assim, a criação de uma Delegacia Especializada, ainda sem previsão. A SEPAEL é composta por 2 peritos, 2 agentes, um chefe e um adjunto (peritos) e 2 auxiliares (agentes). Seriam necessários, para uma Delegacia Especializada, uma equipe composta por 5 pessoas, sendo um chefe de setor, um auxiliar direto e 3 profissionais capacitados em Crimes Cibernéticos. Não há estrutura disponível e seriam necessárias 3 salas, sendo uma delas com equipamentos e softwares necessários. Não há treinamentos específicos promovidos pelo governo estadual. Houve cursos promovidos pela SENASP/MJ, genéricos, voltados para os peritos, e um específico de Inteligência Cibernética. A plataforma EAD/SENASP disponibiliza o Curso de Combate a Crimes Cibernéticos. Não foi possível obter, devido ao curto prazo, nas várias delegacias do Estado, o número de inquéritos instaurados sobre o tema.	13/04/2016
Santa Catarina	Não possui Delegacia especializada em crimes cibernéticos e, apenas em determinados casos, um Agente de Polícia com conhecimentos técnicos da Diretoria Estadual de Investigações – DEIC é designado para a investigação. Seriam necessários um Delegado, um Escrivão e 4 agentes de polícia. A Academia de Polícia Civil já realizou 2 cursos de investigação por meio eletrônico, mas há necessidade de realização de cursos específicos para qualificação dos policiais. Foram instaurados 5 inquéritos para	08/04/2016 e 14/04/2016

	apurar crime de pedofilia, 2 concluídos e as autorias identificadas e 3 em andamento; um para apurar crime de racismo; 16 procedimentos investigatórios relacionados a fraudes e crimes contra a honra e outros 23 inquéritos foram concluídos, relacionados a fraudes praticadas por meio eletrônico, com uma resolução de aproximadamente 70% dos casos.	
São Paulo	A CPI não obteve resposta até o fechamento do Relatório.	
Sergipe	A CPI não obteve resposta até o fechamento do Relatório.	
Tocantins	A CPI não obteve resposta até o fechamento do 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.

Neste contexto, o FNSP - Fundo Nacional de Segurança Pública (criado pela Lei nº 10.201/01), que possui provisão legal específica para o apoio a projetos que tratem de reequipamento das polícias, estabelecimentos de sistemas de informações e outros, surge como a opção mais óbvia. Ocorre, no entanto, que este Fundo possui recursos insuficientes e parca execução orçamentária. Segundo o sistema de acompanhamento de execução orçamentária da Câmara dos Deputados, em 2013, pouco mais de R$200 milhões foram liquidados de uma previsão orçamentária de R$ 640 milhões. Em 2014, repetiu-se essa realidade. Em 2015, menos ainda: apenas R$ 190 milhões foram liquidados de uma previsão orçamentária de R$ 930 milhões. Certamente, com esses valores, o fundo não poderá encampar todas as suas atribuições e também promover projetos para a investigação dos crimes cibernéticos. Essa realidade levou esta CPI a buscar fontes alternativas para o financiamento desses tipos de investigações.

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 telecomunicações, gera mais recursos do que os efetivamente utilizados na fiscalização dessas atividades. É notório 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. Tais recursos têm 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 não utilizada do Fistel, isto é aquela já transferida para o Tesouro Nacional, para a estrutura de combate ao crime tem o potencial de diminuir essas perdas. Lembrando que grande parte dos recursos roubados são drenados de entidades públicas. Assim, o descontingenciamento de recursos voltaria ao caixa da Administração na forma de maior eficiência em suas instituições.

Por esses motivos, esta CPI conclui por:

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;** (Parte III, 1.3) **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.** (Parte III, 3.3)

2.4.5 – 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.

Outro assunto conexo que expõe a fragilidade do cadastro, pela Lei atual a estrangeiros estariam vedados a adquirirem linhas pré-pagas no Pais. Por isso, muitas vezes os próprios agentes de vendas, imbuídos de boa fé, possuem a prática de habilitar aparelhos com CPFs indevidos. Nesse contexto, é importante cessar essa prática, permitindo a aquisição de linhas por estrangeiros, o que aumentaria a confiabilidade do cadastro.

Por esses motivos, **oferecemos 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**. (Parte III, 2.1) Ademais, manifestamos nosso apoio à discussão célere do Projeto de Lei nº 2315/15, do Dep. Enio Verri que trata do cadastro da telefonia pré-paga.

2.4.6 – Apoio a discussão aprofundada acerca de proposições que tratam da 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 seria de que a autoridade policial notificasse o juiz a

cada caso de quebra e este, ao analisar os casos, verificaria se houve excesso, determinando as penas cabíveis, caso necessário.

Esse entendimento 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, tenho o entendimento pessoal de que a metodologia excepcional deve ser adotada para os casos extremos de risco iminente de vida. Todavia, não desconhecendo que a questão envolve direitos fundamentais constitucionalmente garantidos, somos do entendimento que **as Comissões pelas quais tramitar o PL 6.726/10, sobretudo a Comissão de Constituição e Justiça e Cidadania, devem debater com urgência essa proposição**, inclusive avaliando a possibilidade de ampliar o seu escopo, para permitir a quebra das comunicações e não apenas da localização.

2.4.7 – 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.[29] 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.

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."*[30]

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

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

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

Acórdão 3.117/14, “Levantamento de Governança de TI 2014”,[31] 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.

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.

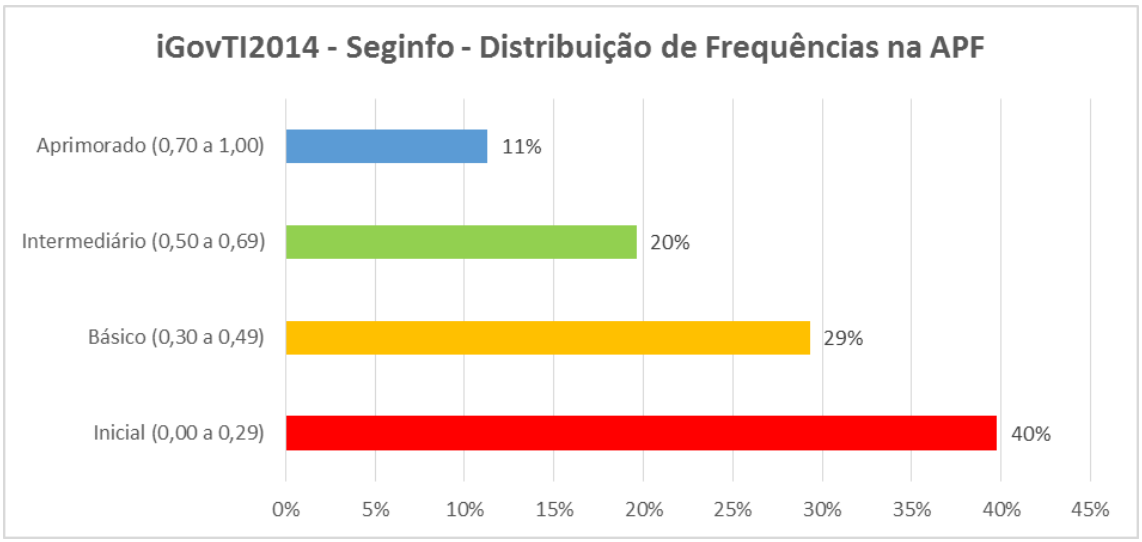


Figura – Índice SegInfo

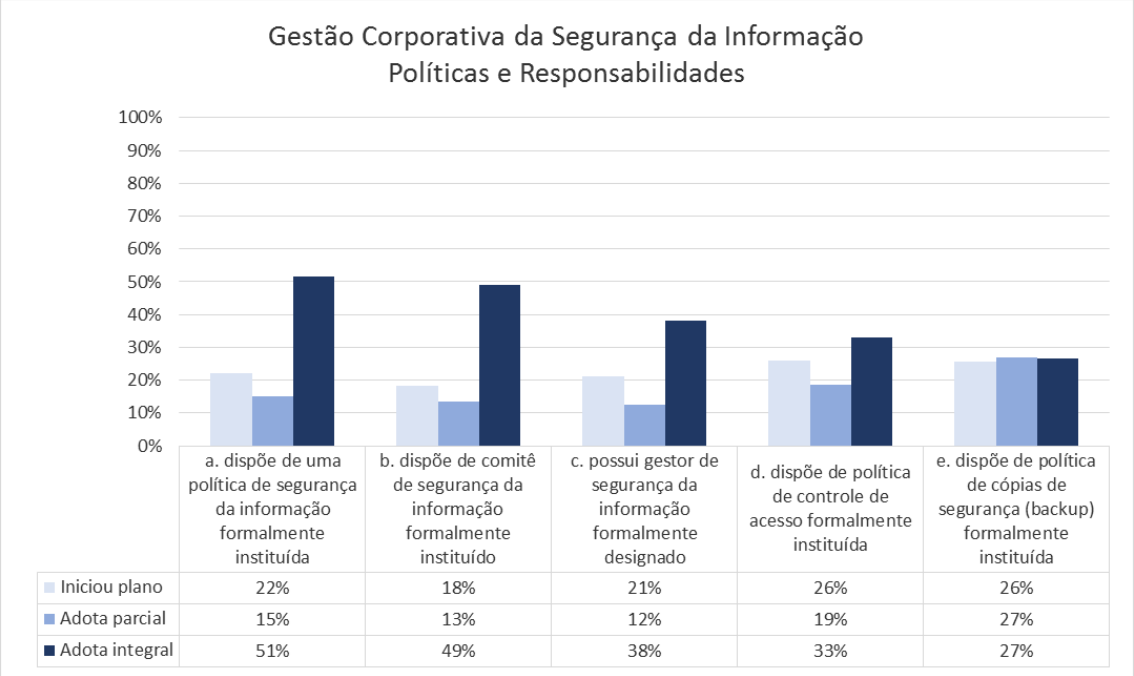
Fonte: Elaborado com base em dados fornecidos pelo TCU coletados no âmbito do iGovTI2014

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

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

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, os quais foram baseados em normas e boas práticas de segurança da informação, como as normas complementares do DSIC/GSI/PR e norma técnica ABNT NBR ISO/IEC 27002:2013.[32]



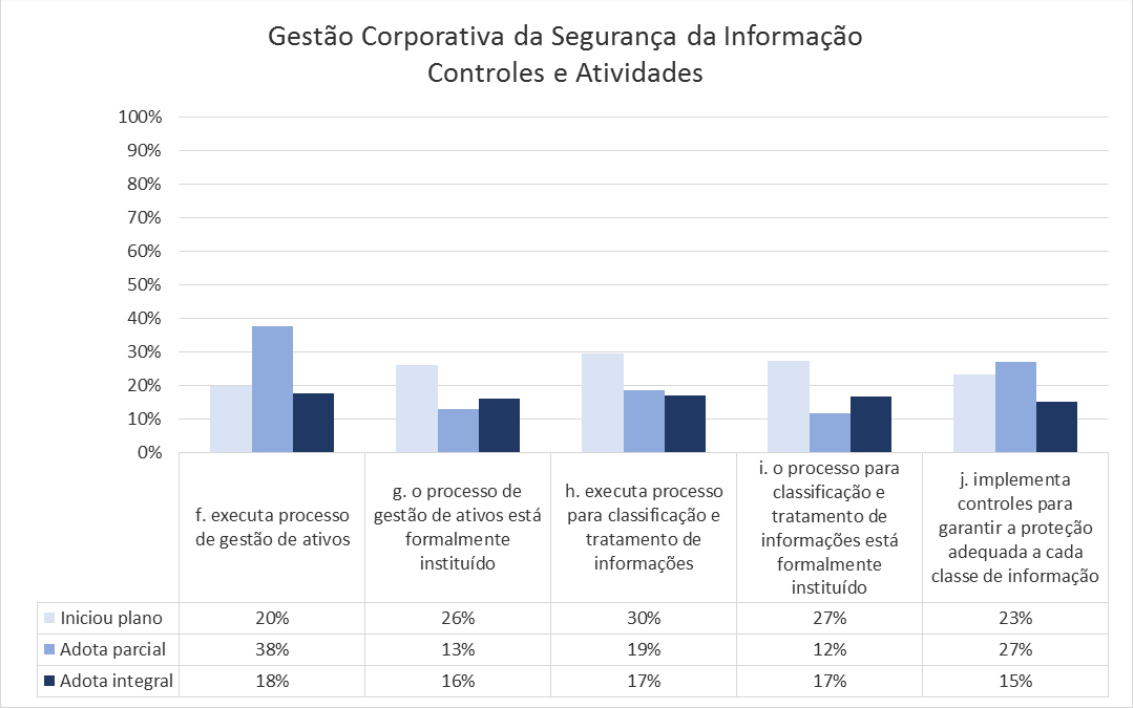
	a. dispõe de uma política de segurança da informação formalmente instituída	b. dispõe de comitê de segurança da informação formalmente instituído	c. possui gestor de segurança da informação formalmente designado	d. dispõe de política de controle de acesso formalmente instituída	e. dispõe de política 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 de forma integral uma política formal de segurança da informação, apenas 27% adota integralmente uma política formal de backups de seus dados. Ademais, apenas um terço das instituições avaliadas controla integralmente quem possui acesso às suas informações.

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

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 ativos. A figura próxima detalha as ações nesse sentido.

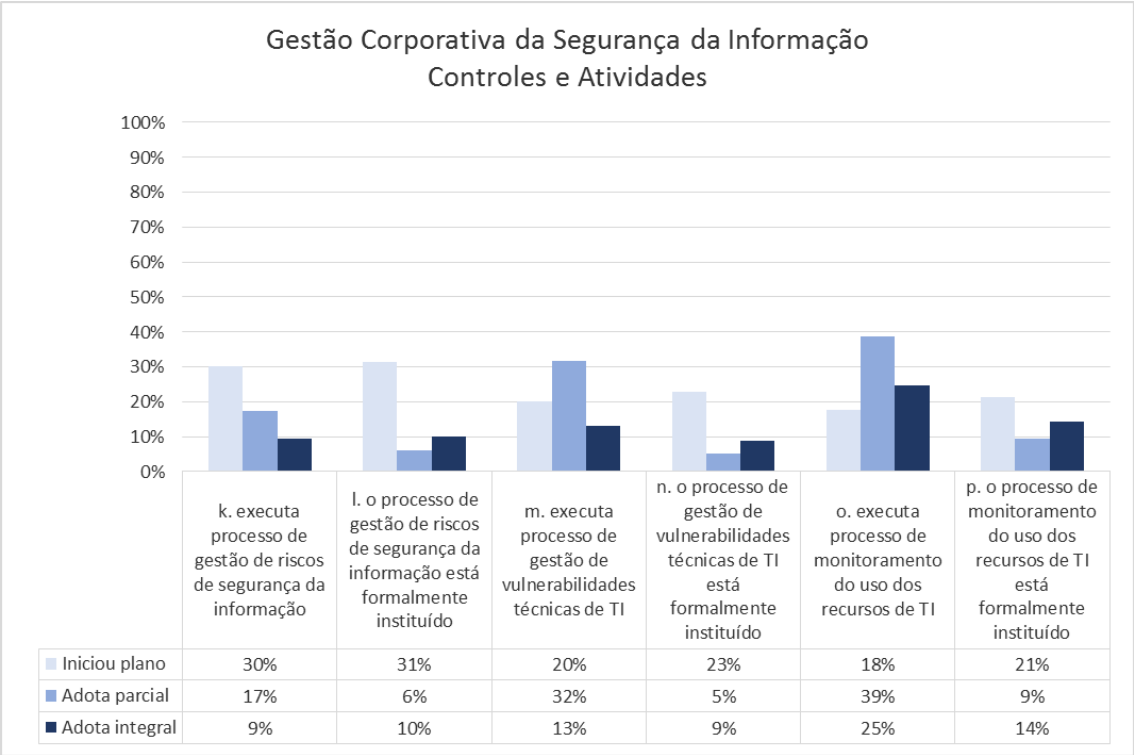


	f. executa processo de gestão de ativos	g. o processo de gestão de ativos está formalmente instituído	h. executa processo para classificação e tratamento de informações	i. o processo para classificação e tratamento de informações está formalmente instituído	j. implementa controles para garantir a proteção 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 informação e no processo de classificação e tratamento das informações, indica práticas ainda mais frágeis. 44% das instituições não executam nenhum tipo de gestão de ativos de informação e apenas 15% do universo auditado implementam de forma integral controles para garantir proteções específicas para cada classe de informação.

Dando prosseguimento à gestão de ativos e dos dados das instituições, a próxima figura detalha a existência de processos de controle de riscos de segurança da informação e da área de TI.



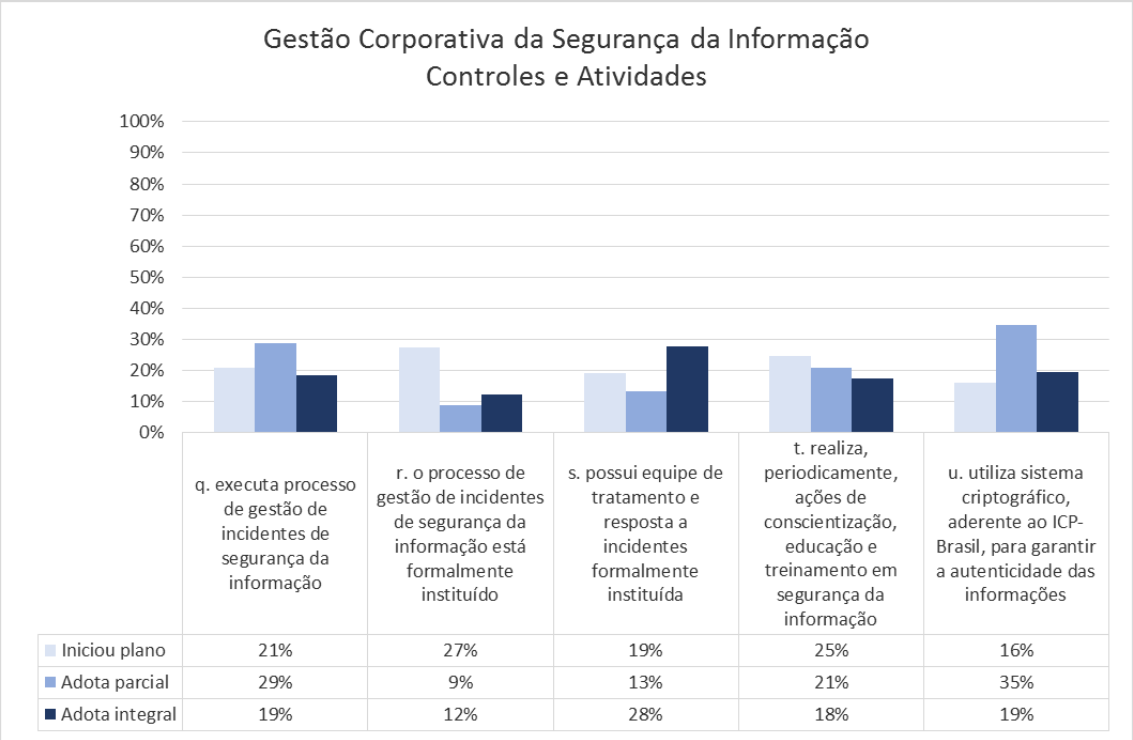
	k. executa processo de gestão de riscos de segurança da informação	l. o processo de gestão de riscos de segurança da informação está formalmente instituído	m. executa processo de gestão de vulnerabilidades técnicas de TI	n. o processo de gestão de vulnerabilidades técnicas de TI está formalmente instituído	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 apenas 26% das instituições executa algum processo de gestão de riscos de segurança da informação e que 55% procura identificar de maneira sistemática riscos e vulnerabilidades técnicas em suas infraestruturas de TI.

A próxima figura apresenta o desempenho das instituições públicas em caso de ocorrência de incidentes de segurança da informação

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 de ocorrência de incidentes na área de TI nas instituições, as respostas indicam que esse assunto não tem sido tratado com a devida relevância. Apenas um terço das instituições já possuem equipes formalmente instituídas para responder a incidentes (item ‘s’) e 12% possui procedimento integralmente implementado a ser seguido (‘r’).

Além do estágio incipiente na gestão de incidentes, outro aspecto preocupante é que apenas metade das instituições está atuando de alguma forma na prevenção, com ações de conscientização, educação e treinamento em segurança 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.

Certos de que o desenvolvimento da tecnologia modifica padrões de maneira constante, temos a compreensão de que apenas focar em boas práticas não garantirá o melhor resultado em termos de segurança de TI. Portanto, entendemos que tais medidas deverão focar, também, na redução de riscos e na limitação dos eventuais danos decorrentes de sinistros na área.

Por último, nessa avaliação e sugestão de práticas deve igualmente ser considerada a questão do incentivo e da adoção preferencial de tecnologias, padrões e formatos abertos e livres. Sabe-se que a adoção desse tipo de programas possui o potencial de aumentar a segurança e diminuir os riscos em ambientes de TI, pois possui a facilidade da auditoria dos códigos.

Pelos motivos expostos, esta CPI julga oportuno o oferecimento de Indicação determinando à Administração Pública Federal (APF), direta e indireta, no âmbito de cada entidade, que: i) adote guia de boas práticas em segurança da informação; ii) implemente processo de gestão de riscos de segurança da informação; iii) avalie a possibilidade da adoção de tecnologias, padrões e formatos abertos e livres no estabelecimento de controles de segurança da informação; iv) realize auditoria em sua infraestrutura pública de TI; v) celebre instrumentos de cooperação técnica entre autoridades públicas de segurança cibernética e entidades privadas; vi) direcione esforços para a consecução dos objetivos propostos na Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF, em especial instituir modelo de governança sistêmica de SIC e de SegCiber.

(Parte III, 3.1)

2.4.8 – 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*".[33]

[33] 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.

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 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.

Cabe ressaltar que essa batalha pela abertura de aplicativos e dispositivos não ocorre somente no Brasil. Recentemente no episódio do atentado terrorista de San Bernardino, de dezembro de 2015, nos EUA, o FBI (a Polícia Federal daquele país) solicitou a quebra da segurança de um telefone *Iphone* do suposto terrorista pelo seu fabricante, a Apple. Mediante a quebra o órgão esperava acessar as mensagens ali gravadas e colher mais informações acerca do atentado. Após a negativa do fabricante em cooperar e a querela pública decorrente que incluiu ameaças de ações judiciais de ambos os lados, o FBI desistiu de obter cooperação e anunciou que tinha conseguido o desbloqueio por conta própria. O episódio serve para mostrar que a quebra do sigilo em sistemas de comunicações, hoje em dia, reveste-se de vital importância para o sucesso de investigações. Como segunda conclusão da análise dos episódios no Brasil e nos EUA, concluímos que, aparentemente, a polícia daquele país encontra-se melhor aparelhada.

Apesar da controvérsia que ocorreu no Brasil com relação ao pedido de "espelhamento" do aplicativo, os diversos depoimentos nesta CPI 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, **oferecemos 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.** Cabe ressaltar que esta proposição é parte integrante do Projeto de Lei proposto pelo Sub-relator Deputado Daniel Coelho para a retirada de conteúdos que atentem contra a honra, proposto no Anexo 1.4.(Parte III, 1.5)

2.4.9 – 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.

2.5 – ASSUNTOS CORRELATOS INVESTIGADOS

Com o andamento das investigações e das Audiências Públicas realizadas, esta CPI recebeu diversas reclamações sobre assuntos correlatos relacionados ao mau uso da internet. A análise indicou que as temáticas não eram atinentes a nenhuma Sub-Relatoria em especial, nem tampouco poderiam ser relacionadas nos objetivos precípuos desta Comissão. Entretanto, como as problemáticas apontadas tangenciam a temática da CPI e suas resoluções contribuirão para uma prestação mais efetiva dos serviços de telecomunicações e de informática, assim como propiciarão uma internet mais segura para todos os cidadãos, esta CPI decidiu incluir um tópico específico sobre esses assuntos correlatos.

2.5.1 – Consumo da franquia de dados da internet

Durante os trabalhos da CPI seus integrantes receberam diversas indicações de descontentamento por parte dos usuários com os serviços prestados pelas operadoras de telecomunicações, em especial no que diz respeito ao consumo de dados nos planos de banda larga da telefonia móvel.

Possivelmente motivadas pelo vertiginoso crescimento da telefonia móvel no País, e incapazes de expandir suas próprias redes a um ritmo tão acelerado, as empresas prestadoras resolveram, de forma mais ou menos coordenada, acabar com a possibilidade do usuário continuar desfrutando da internet móvel, mesmo que com velocidade reduzida, após superada a franquia de dados contratada. Essa decisão das prestadoras evidenciou ainda mais uma dúvida que já era um dos grandes motivos de reclamação dos assinantes, qual seja, saber se a prestadora mede o consumo de dados corretamente.

A preocupação da sociedade com o assunto é tão evidente que, atualmente, já tramitam nessa casa os PLs 418 e 4.470, de 2015, ambos no sentido de proibir as prestadoras do Serviço Móvel Pessoal (nome técnico do serviço) de interromper o acesso a internet para o usuário que exceder a franquia de dados contratada.

De particular interesse para esta Comissão é o fato de que o corte após o uso da franquia de dados contratada pode levar os usuários a deixarem de atualizar aplicativos e diretivas de segurança como forma de economizar seu pacote de dados. Assim, a segurança dos dispositivos fica comprometida. Neste particular, entendemos que a mudança dos planos permitindo a desconexão de usuários quando atingem a franquia contratada é potencialmente nociva para a segurança cibernética.

Em que pese a regulamentação específica exarada pela Anatel,[34] esta CPI não tem conhecimento de nenhuma atividade de controle ou fiscalização por parte do órgão regulador na questão da medição do consumo da internet móvel. Este é, certamente, um campo em que o Poder Público precisa se debruçar. Até para se chancelar as boas práticas das operadoras de telefonia, é mister avaliar as práticas de bilhetagem, especificamente na questão do consumo de dados. Uma internet segura, livre de crimes, mas também justa e de qualidade é de fundamental importância para o exercício pleno da cidadania nos dias atuais. Por estas razões, a CPI dos Crimes Cibernéticos, acatando sugestão de sua Presidente, Deputada Mariana Carvalho, **apresenta Proposta de Fiscalização e Controle para que, com o apoio do Tribunal de Contas da União, possa-se verificar como a Anatel, tem realizado o acompanhamento e o controle da tarifação dos pacotes de dados da telefonia móvel**.

2.5.2 – Seminário Segurança Cibernética para as Olimpíadas Rio 2016

Outra questão muito relevante, e que foi levantada pelo Dep. Delegado Eder Mauro em algumas audiências da CPI, diz respeito à preparação do país para receber as Olimpíadas de 2016, tendo em vista o receio de que tal evento esportivo seja utilizado como palco para ataques terroristas, que podem ser praticados ou organizados, inclusive, por meios cibernéticos.

Em que pese essa temática não ter recebido o tratamento que merecia devido à importância e à premência do evento, esta CPI reservou um

[34] Resolução n.º 632, de 7 de março de 2014,da Anatel, que dispõe, no art. 62, que as prestadoras deverão disponibilizar aos assinantes, entre outras, as seguintes informações: *"VII – o volume diário de dados trafegados; VIII - os limites estabelecidos por franquias e os excedidos; ...; X - o valor da chamada, da conexão de dados ou da mensagem enviada, explicitando os casos de variação horária;"*.

espaço especial em sua agenda e realizou Seminário específico tendo convidado as principais autoridades a cargo da segurança cibernética do grande evento. No Seminário, resultado de requerimento dos Deputados Delegado Eder Mauro e Silas Freire, foi apresentado o arcabouço institucional desenvolvido para o acompanhamento do evento e as principais ações em andamento, além das ferramentas que serão utilizadas durante os jogos. Entretanto, os depoimentos indicaram que a questão é extremamente intrincada, envolve recursos tecnológicos complexos e humanos intensivos. Ademais, o potencial de dano é altíssimo, ainda mais em se considerando os atuais acontecimentos de terrorismo internacional, como as ações do Estado Islâmico. Dessa forma, recomendamos à **Comissão de Segurança Pública e Combate ao Crime Organizado que crie uma Subcomissão Especial para acompanhar essa questão**.

2.5.4 – Acolhimento por parte do Cedes de estudo sobre *bigdata*

Durante o andamento da CPI, o Dep. Paulo Henrique Lustosa salientou o fato de que a massificação da internet, a proliferação de sistemas automatizados, assim como a crescente adoção da internet das coisas, gera uma quantidade de dados acerca de informações, hábitos e preferências dos cidadãos, sem precedentes na história da humanidade.

Na verdadeira indústria de dados pessoais que se criou nos dias de hoje cunhou-se a frase "*data is the new oil*" – dados são o novo petróleo, tal a importância dessas informações. Verdadeiros impérios faturam bilhões de dólares mediante a monetização dos dados, exemplos mais notórios as quatro grandes Google, Facebook, Microsoft e Apple.

Diversas são as questões derivadas do processamento maciço de informações de cidadãos. Preocupam-se não apenas ativistas sociais e o terceiro setor, majoritariamente focados com os impactos sobre a privacidade e a intimidade das pessoas, mas também concorrentes e empresas de menor poder econômico, assim como governos. Em síntese, a questão do *bigdata* transcende a esfera da internet e reveste-se de importância nevrálgica para o desenvolvimento econômico de nações, assim como tem a capacidade de ditar os caminhos futuros da vida em sociedade.

Por esses motivos, consideramos acertada a sugestão

apresentada pelo Dep. Paulo Henrique Lustosa de que o Cedes – Centro de Estudos e Debates Estratégicos – adote a temática como futuro objeto de estudos. Nesse sentido, **recomendamos o envio de Ofício ao Centro de Estudos e Debates Estratégicos para que desenvolva estudo sobre o impacto e a necessidade de regulação na questão do *bigdata***.

2.5.5 – Sugestão de criação de força tarefa para a eleição Municipal

Os crimes cibernéticos quando aplicados no processo eleitoral possuem efeito devastador no estado democrático e de direito. Como bem lembrado em contribuição dada a esta CPI pelo Segundo-Secretário da Câmara dos Deputados, Deputado Felipe Bournier, o baixo custo do uso da internet e a sua capacidade de difusão das informações podem transformar a internet em “um veículo de gerrilha eleitoral”. Para coibir esse mau uso e diminuir os seus efeitos deletérios sobre o processo democrático, encampamos a sugestão dada pelo nobre Segundo-Secretário.

Por esses motivos, incluímos em nosso relatório **Indicação ao Presidente do Superior Tribunal Eleitoral** para que tome as providências necessárias para a criação de força tarefa, no âmbito de cada Tribunal Regional Eleitoral, com membros da Polícia Federal, Ministério Público e tribunais, visando a célere apuração de cibercrimes eleitorais.

3 – PROPOSIÇÕES LEGISLATIVAS EM TRAMITAÇÃO NA CÂMARA CUJA DISCUSSÃO SE MOSTRA IMPORTANTE

Conforme apontado pelos Sub-Relatórios, verifica-se que existem algumas proposições legislativas já tem trâmite nesta Casa e que podem auxiliar na resolução dos problemas atinentes aos crimes cibernéticos e que, por isso, devem ser amplamente discutidas por esta Casa. São eles:

a) Projeto de Lei nº 1776/15 (de autoria do Deputado Paulo Freire), que "*inclui no rol de Crimes Hediondos os Crimes de Pedofilia*";

b) Projeto de Lei nº 3237/15 (de autoria do Deputado Vinícius Carvalho), que "*altera o Marco Civil da Internet, Lei no 12.965, de 23 de abril de 2014, dispondo sobre a guarda dos registros de conexão à internet de sistema autônomo*";

c) Projeto de Lei nº 5555/2013 (de autoria do Deputado João Arruda) e apensados, que tratam da divulgação não autorizada de imagens íntimas das vítimas;

d) Projeto de Lei nº 3686/2015 (de autoria do Deputado Ronaldo Carletto), que "*tipifica o crime de intimidação sistemática (Bullying), prevendo causa de aumento se a conduta for realizada por meio da internet (Cyberbullying)*";

e) Projeto de Lei nº 7544/2014 (de autoria do Deputado Ricardo Izar), que tipifica a conduta de incitação virtual ao crime;

f) Projeto de Lei nº 1755/2015 (de autoria do Deputado Raul Jungmann) e apensados, que tratam da criminalização da divulgação indevida, na internet, de informações pessoais;

g) Projeto de Lei nº 6726/2010 (de autoria do Deputado

Arnaldo Faria de Sá), que dispõe sobre o acesso de autoridades às informações relativas à localização de aparelhos de telefonia celular;

h) Projeto de Lei nº 2315/15 (de autoria do Dep. Enio Verri), que trata do cadastro da telefonia pré-paga;

i) Projeto de Lei nº 2801/2015 (de autoria do Dep. JHC), que altera a Lei Federal nº 9.394/1996 - que Estabelece as diretrizes e bases da educação nacional, para acrescentar finalidade ao Ensino Médio no sentido de incluir a necessidade de educação quanto aos meios telemáticos de comunicação e comportamento e tecnologia.

4 – CONCLUSÕES DO RELATOR (DEPUTADO ESPERIDIÃO AMIN)

A CPI contou com a excelente condução por parte da Presidente do colegiado, Deputada Mariana Carvalho, que procurou colocar em pauta, da forma mais abrangente possível, todos os aspectos que envolvem a prática de crimes pela internet, assim como soube de maneira extremamente hábil colocar em discussão, de maneira imparcial, as quatro temáticas em que foi dividida esta CPI.

Por sua vez, os Sub-Relatores Sandro Alex, Rafael Motta, Daniel Coelho e Rodrigo Martins também souberam explorar suas temáticas de maneira exemplar e brindaram-nos com extraordinárias e profícuas colaborações e indicações de oitivas para Audiências Públicas. Ademais, conduziram investigações próprias com extrema desenvoltura. Nesta parte, gostaríamos de salientar também o clima de cordialidade e de cooperação que predominou entre os pares integrantes desta CPI ao longo das investigações, que se mostraram válidas e eficazes.

No curso dos inquéritos, esta CPI realizou cerca de trinta Audiências Públicas e ouviu depoimentos de mais de 100 convidados e convocados. Prestaram contribuições e esclarecimentos autoridades regulatórias, de investigação das polícias Estaduais e Federal, dos Ministérios Públicos Estaduais e Federal, assim como entidades diversas, tais como de defesa de crianças e adolescentes, de representação de classe e de defesa do consumidor. Também foram ouvidos especialistas em diversas áreas do direito, principalmente na incipiente área do direito digital. Também de fundamental importância para o entendimento da internet e para a compreensão de como os crimes cibernéticos são cometidos, chamamos as principais empresas da internet, de telecomunicações e de segurança na grande rede.

Com base nesses depoimentos, conseguimos realizar uma proveitosa fase de instrução nesta CPI que nos permitiu fazer um *raio-X* pormenorizado do setor, entendendo o papel de cada instituição nessa infindável cadeia de valores em que se traduz a internet.

Como era o objetivo desta CPI, fomos instruídos nas práticas nefastas de crimes digitais que ocorrem na grande rede e verificamos,

através dos depoimentos e das investigações, as agruras pelas quais passam as vítimas e, também, as autoridades de investigação. Soou uníssono nos depoimentos a necessidade de melhorar alguns tipos penais, certos dispositivos legais, procedimentos de investigação, o aparelhamento de nossas autoridades de investigação e, também, a educação dos internautas.

Desafortunadamente, a finalização dos trabalhos desta Comissão não nos possibilitou aprofundar em diversas questões que surgiram nas discussões e que merecem, sem lugar a dúvidas, aprofundamentos.

Todavia, diversos também foram os temas tratados. Cabe enumerar alguns principais, nestas conclusões ao relatório:

1. De maneira concomitante ao andamento das investigações conduzidas pelo Sub-Relator afeito à área de publicidade, Deputado Sandro Alex, a Polícia Federal deflagrou a operação Barba Negra que resultou no fechamento de sítio de internet que oferecia ilegalmente filmes e outros conteúdos audiovisuais. A denúncia apresentada nesta CPI pelo Deputado Sandro Alex, desencadeou, também, mudanças nos procedimentos de alocação de publicidade governamental na internet. Conforme se evidenciou na audiência pública realizada, no dia 08/10/2015, com o Ministro Edinho Silva, da Secretaria de Comunicação Social da Presidência da República, propagandas de empresas tradicionais e até do governo estavam sendo veiculadas em sítios utilizados para a prática de crimes cibernéticos, tais como o *streaming* ilegal de filmes e de séries de televisão. Na ocasião o Ministro declarou que encaminharia à Comissão “todo o ranqueamento [isto é, investimento em publicidade], assim como o ranqueamento das redes sociais para que a Comissão tenha todas as informações necessárias sobre o que é investido em publicidade, por meio da SECOM”. Ressaltamos que essas informações não foram encaminhadas até o encerramento dos trabalhos da CPI. Portanto, encaminhamos Requerimento de Informações solicitando esses dados. Portanto, as sugestões desta CPI de **elaboração de um Código de Boas Práticas na Publicidade da Internet e assinatura de TAC (Termo de Ajustamento de Conduta) entre o Ministério Público Federal e associações de mídia digital, assim como da necessidade de**

inclusão de dispositivo que permita o bloqueio desse tipo de sítios de conteúdo pirata diretamente pela Comissão de Direito Autoral, já em andamento, são extremamente necessárias. No entanto, ficou evidente que essas medidas representam apenas o começo das ações necessárias. É preciso continuar nas investigações dos sítios de internet que comercializam e oferecem produtos e serviços ilegais com o auxílio da grande rede. É preciso, também, que a Polícia Federal e o Ministério Público continuem as investigações relacionadas à operação Barba Negra, com o intuito de chegar àqueles que verdadeiramente financiam esses sites que oferecem conteúdo ilícito;

2. O **comércio eletrônico** é uma grande categoria de práticas criminosas em que não foi possível realizar investigações. Sabemos que, no Brasil, par e passo o crescimento do comércio eletrônico, multiplicam-se as modalidades de crimes relacionados a esse tipo de transações. Faz-se imprescindível entranhar-se nessas práticas, dimensionar prejuízos e verificar as melhores práticas para mitigar esse mais novo dreno na economia brasileira;

3. As investigações sobre possíveis crimes à ordem tributária praticados por empresas de internet - e mediante o uso da internet - revelou a necessidade de aprofundamento das investigações na temática. A tributação dos serviços prestados pela internet é de difícil conceituação e perpassa o arranjo federativo e até as fronteiras do País. As oitivas evidenciaram entendimentos e práticas tributárias contraditórias que salientam a necessidade de atuação na área. Tendo em vista a importância crescente da internet na economia de modo geral, é evidente que a temática precisa ser melhor esclarecida. **É necessário que as autoridades tributárias e o Parlamento continuem as investigações sobre as práticas fiscais e o recolhimento de impostos por parte das empresas de internet**;

4. Na questão dos crimes praticados contra o sistema financeiro, esta CPI obteve significativo avanço com a colaboração do Banco Central e da Polícia Federal. Tomando-se como parâmetro, conservador, de que 0,1% do risco operacional da Caixa seja devido à incidência de

crimes cibernéticos, foi possível estimar que esse tipo de fraudes desvia, no mínimo, R$ 600 millhões de correntistas. Contudo, o estudo da Sub-Relatoria indicou a necessidade de aprofundamento das investigações por parte do Congresso Nacional. **As Indicações ao Banco Central e Polícia Federal no sentido de melhorar e compartilhar as informações, à esfera Judicial para a criação de Varas Especializadas e o Projeto de Lei permitindo o perdimento de bens desses criminosos são medidas acertadas propostas por este colegiado;**

5. Ficou claro nesta CPI, e os depoimentos apenas reforçaram o entendimento do setor, que a primeira barreira na segurança da internet são os próprios usuários. Por isso, os Sub-Relatores desta CPI concluíram pela sugestão de **elaboração de Termo de Cooperação para a educação de internautas, a ser celebrado pelas principais entidades atuantes na internet**. Ressaltamos que o Ministério Público Federal já possui importante programa de educação digital nas escolas, estabelecido pela Portaria PGR/MPF nº 753/15. Nesse contexto esta CPI propõe dois Termos de Cooperação. O primeiro, com o objetivo de **promover a educação de crianças e adolescentes nas escolas, levando em consideração o programa já em desenvolvimento pelo Ministério Público Federal**. O segundo, **voltado para a educação de adultos.** Ainda na questão da educação de crianças e adolescentes, o Sub-Relator Dep. Rafael Motta sugere o envio de **Indicação ao Ministério da Educação** para que seja incluída **a oferta obrigatória de noções de educação digital nas escolas públicas e privadas** de ensino fundamental e médio. Em que pese essas medidas busquem mitigar o desconhecimento da população com as melhores práticas para o uso seguro da internet, as investigações indicam que uma melhor discussão dos procedimentos e das ações a serem promovidas devem ser objeto de maior estudo por parte do Congresso. Ressaltamos que essa preocupação é também do objeto do Projeto de Lei nº 2801/2015, do Deputado JHC, razão pela qual apoiamos a sua discussão nesta Casa;

6. Desafortunadamente, a distribuição de conteúdos pedófilos é uma execrável prática que ficou facilitada de sobremaneira pela internet, como constatado no relatório do Sub-Relator Rafael Motta. Por isso, **apoiamos a discussão do Projeto de Lei 1.776/15, em tramitação, que torna crimes hediondos os delitos ligados à pedofilia**;

7. Verificou-se, também, a necessidade de coibir oferta de conteúdos criminosos, extremamente deletérios à sociedade. A indisponibilização de serviços ilegais prestados a partir de provedores de hospedagem localizados em território brasileiro pode ser bastante simples, uma vez que basta ao juiz determinar ao provedor em território brasileiro a retirada de conteúdos que violam direitos de qualquer gênero. O mesmo não se verifica para serviços ilegais hospedados para fora da jurisdição do Estado Brasileiro. Nesses casos, conforme apontado pelos Sub-Relatores Deputados Sandro Alex e Rafael Motta, o bloqueio ao acesso ao conteúdo criminoso é a única forma, em certos casos extremos em que já foram esgotadas alternativas cabíveis, de se garantir a proteção efetiva dos usuários. Por isso, após o recebimento de frutíferas contribuições de diversas entidades e autoridades, **propomos Projeto de Lei que possibilite, em casos extremos, o bloqueio a conteúdos ou, em último caso, aplicações de internet ofertadas no exterior e que não possuam representação no País e que sejam consideradas criminosas por ordem judicial e que cuja pena mínima cominada for igual ou superior a dois anos**. Optamos por essa delimitação, pois nesses casos a atuação de autoridade judicial brasileira depende de atuação de órgão de justiça internacional, o que dificulta a cessação da oferta. Nesse rol encontrar-se-iam enquadrados aqueles sítios que veiculam conteúdos que violem direito autoral com o intuito de lucro (cuja pena mínima é de 2 anos), crimes ligados a pedofilia (3 anos), medicamentos proibidos (10 anos) e terrorismo (12 anos), os quais foram objeto de grande preocupação durante os trabalhos desta CPI, Em contrapartida, ofensas menores como **crimes contra a honra não estariam ao alcance do dispositivo**, sendo outras as medidas cabíveis já prescritas em Lei.

8. A abordagem de bloquear conteúdos ou aplicações, apenas em último caso e somente quando a autoridade brasileira não tem outra forma de atuação célere, guarda paralelo em muitos outros países democráticos. A lei chilena, por exemplo, que trata a neutralidade da rede de forma extremamente ampla, veda o bloqueio e garante o acesso apenas a serviços ou a aplicações legais (Ley 20.453, art. 24H).. A Regulação 2120, de 2015, do Conselho e do Parlamento da Europa, em seu art. 3º, garante aos usuários o acesso a conteúdos e serviços, desde que estes sejam legais, permitindo o seu bloqueio para o cumprimento de leis ou ordens judiciais. Da mesma forma, nos Estados Unidos a Resolução de Proteção e Promoção da Internet Aberta, de 13/04/2015 e o Código de Regulações Federais (CFR, Título 47, Capítulo I, Subcapítulo A, Parte VIII, Seção 8.5), determina que os provedores de internet não podem bloquear conteúdos legais. No entanto, na Seção 8.9 do Código, é determinado que não são proibidos esforços razoáveis por provedores de acesso com o intuito de resolver infrações a direito autoral ou a outras atividades ilegais. Outrossim, é mister ressaltar que, assim como divulgado por diversas associações ligadas à proteção de direitos autorais, nos mais variados campos, esse tipo de proteção existe em países com democracias solidamente estabelecidas, entre elas Reino Unido, Austrália, Espanha, França, Coreia do Sul, Bélgica, Dinamarca, Alemanha, Suécia, Holanda e Itália.

9. A retirada da fronteira física entre as pessoas, a facilidade de uso, a ubiquidade e a gratuidade das redes sociais teve como efeito colateral o aumento de ataques pessoais e da postagem de conteúdos ofensivos. Entendemos que, conforme assinalou o Sub-Relator Deputado Daniel Coelho, a legislação deveria ser atualizada no sentido de que os conteúdos considerados infringentes e já retirados mediante ordem judicial, continuem indisponíveis em caso de repetições nas mesmas aplicações. Por isso, oferecemos **Projeto de Lei alterando o Marco Civil da Internet, determinando que as aplicações de internet retirem conteúdo infringentes em casos de replicação, quando notificados pelo usuário.** Destacamos que esta proposta se beneficiou de valorosa contribuição do CGI.br.

Entendemos que esta variante é adequada, pois evita a necessidade de policiamento contínuo por parte das aplicações de internet, o que seria dificultoso para entidades de menor envergadura econômica e, por isso, não é deletério para a inovação na rede ou a atração de investimentos. Ressaltamos, no entanto, que a proposta da entidade incorre na problemática de considerar idêntico aquele conteúdo "que contenha parte majoritária e que reproduza a infração decorrente de conteúdo removido por ordem judicial anterior", tal como previsto em sua contribuição. Entendemos que esta extensão gera subjetivismo e, portanto, não a acolhemos. Por fim nesta temática, aponte-se que a medida proposta é distinta de uma implementação pura e simples de NOTICE AND STAY DOWN, uma vez que inclui o aviso ao provedor de aplicação por parte do usuário. A medida possui equivalentes internacionais, por exemplo na corte alemã para o caso do aplicativo Rapidshare, em 2012. O assunto também é objeto de estudo nos Estados Unidos onde se encontra em Consulta Pública a alteração à Seção 512 do Digital Millennium Copyright Act.

10. Com relação a conteúdos atentatórios contra a honra, esta CPI buscou incessantemente convidar personalidades atacadas por essa mazela que contamina a internet. Foram diversos requerimentos aprovados para convidar vítimas a prestarem depoimento, mas todas elas declinaram por se tratar de assunto extremamente doloroso e pessoal. Essa recusa é um forte indicativo do grave transtorno que acarreta ser alvo desses comentários e ações continuadas. O estudo da matéria, entretanto, mostrou que a solução regulamentar para coibir esse tipo de ataque é extremamente complexa. Entendemos que é necessário encontrar formas para a proteção a cidadãos comuns de ataques pessoais pela internet (tais como ameaças, e cyberbulling) sem a necessidade de acionar a justiça. O Parlamento deve dar uma resposta à excessiva judicialização de direitos, tão criticada em um país de tantas desigualdades sociais como a brasileira, em que o acesso à justiça não se dá da mesma maneira para todos os cidadãos.

11. A multiplicação de serviços oferecidos pela internet, aliada à facilidade na criação de perfis e ao alto alcance dos aplicativos de

internet, em especial das redes sociais, fazem com que usuários estejam cada vez mais expostos a ataques e malfeitores tenham mais opções para a prática de crimes. Nesse sentido, a rápida identificação de agressores é de fundamental importância para limitar os danos causados. Pela sistemática introduzida pelo Marco Civil da Internet, a identificação dos autores de malfeitos na internet precisa necessariamente passar por três fases. A primeira junto à empresa de aplicação para a obtenção do IP (*Internet Protocol*), a segunda, junto à autoridade de certificação para obtenção da empresa que utiliza aquele IP e a terceira com a operadora responsável pela conexão do internauta para a obtenção do nome e endereço. Considerando que o endereço IP é um dado imprescindível para a célere investigação da autoria de conteúdos criminosos, entendemos que permissão de acesso ao endereço IP à autoridade de investigação, independentemente de ordem judicial, facilitaria a identificação do autor, o que diminuiria os tempos de atuação e aumentaria a eficácia no combate aos crimes digitais. Entretanto, entendemos que essa proposta é extremamente controversa, pois há diversos setores da sociedade organizada que entendem que essa previsão vai de encontro aos preceitos constitucionais de respeito às garantias e liberdades individuais. Por esses motivos, acolhemos a proposta do Deputado Daniel Coelho de apoiar o debate em torno do **Projeto de Lei do Senado 730, de 2015 (que recebeu, na Câmara, o nº 5074/2016), de autoria do Senador Otto Alencar, que dispõe sobre investigação criminal e a obtenção de meios de prova de crimes praticados na internet, aprovada naquela Casa em 18/04/2016**. Consignamos que, assim como ressaltado pelo Deputado Leo de Brito, essa análise deve levar em consideração os princípios, garantias, direitos e deveres constantes no Marco Civil da Internet.

12. A melhor tipificação do crime de invasão de dispositivo informático é importante contribuição desta CPI, conforme extensamente debatido pelo Deputado Rodrigo Martins. O **Projeto de Lei oferecido retira a questão da motivação e determina que a invasão, com ou sem vantagem pessoal, é criminalizada, desde que haja exposição dos dados informatizados a risco de divulgação ou de utilização**

indevida. Aponte-se neste particular, que não se está alterando a ação penal relacionada ao tipo, que continua sendo condicionada à representação, a não ser em casos específicos como contra a Administração. Dessa forma, invasões em que o proprietário particular ou vítima, não vislumbrar a necessidade de dar início a investigação criminal, isso não ocorrerá.;

13. Foi verificado que grande parte dos usuários navega na internet sem a devida guarda dos respectivos registros, em que pese a intenção do Marco Civil da Internet para tal. O PL 3237/15 preenche corretamente uma lacuna legal ao melhor especificar as diversas categorias de provedores de acesso. Ademais, a CPI e em especial a Sub-Relatoria do Deputado Rodrigo Martins verificaram que a adoção do protocolo IPv6 contribuiria para resolver essa questão do anonimato. Portanto, declaramos nosso **apoio ao PL 3.237/15 assim como o oferecimento de Indicação à Anatel para a implantação do IPv6 ou de tecnologia similar**;

14. A falta de estrutura específica para o combate aos crimes cibernéticos nas polícias estaduais e a necessidade de um maior desenvolvimento desta na Polícia Federal ficaram evidentes nos depoimentos a esta CPI em diversas Audiências. Esta investigação tomou conhecimento de estruturas formalmente constituídas para o combate e estes tipos de crimes apenas nos Estados da Bahia, Maranhão, Mato Grosso do Sul, Paraná e Rio Grande do Sul. O Fundo Nacional de Segurança Pública (FNSP), que deveria suprir os recursos necessários para o desenvolvimento de projetos de combate aos crimes cibernéticos possui parcos recursos e execução orçamentária. Nesse sentido, consideramos acertada a constatação do Sub-Relator Rodrigo Martins que conclui pela necessidade de oferecimento de **Projeto de Lei autorizando que 10% das receitas do Fistel (Fundo de Fiscalização das Telecomunicações) transferidas para o Tesouro Nacional possam ser utilizadas para o financiamento das estruturas de combate a crimes cibernéticos. Ressalte-se que não está se propondo retirar recursos do setor ou da agência do setor, a Anatel. O projeto dá nova destinação aos recursos já recolhidos ao Tesouro e não**

aplicados pela Lei Orçamentária na fiscalização do setor. Nesse mesmo segmento, oferecemos Indicação para que sejam estabelecidos convênios para o uso conjunto desses recursos entre as esferas Federal e Estadual. Além disso, **propõe-se que a investigação dos casos de crimes cibernéticos que possuam repercussão interestadual ou internacional e que demandem uma repressão uniforme fique a cargo da Polícia Federal**;

15. Assim como a internet abriu uma nova modalidade de crimes praticados contra a sociedade, o uso da telefonia celular, em especial a pré-paga, contribui em grande escala para o acometimento destes. Esta CPI identificou que as operadoras são omissas quanto à integridade do cadastro obrigatório por lei, assim como verificou que o número de celular é informação fundamental para a obtenção de cadastro nas principais aplicações de internet. Por isso malfeitores se aproveitam dessa falha nos cadastros para praticarem crimes no anonimato. Para intentar estancar essa situação, **encampamos sugestão do Sub-Relator Deputado Rodrigo Martins de Proposta de Fiscalização e Controle para que, com auxílio do Tribunal de Contas da União, sejam verificadas quais ações foram tomadas pela Anatel na fiscalização da integridade do cadastro do pré-pago;**

16. A prática do *cyberbullying* tem resultado em graves danos, principalmente em crianças e adolescentes, e esta CPI constatou a infelicidade da ocorrência de mortes decorrentes dessas práticas. Em face desse problema, esse Parlamento, inclusive, já teve a oportunidade de aprovar a Lei nº 13.185, de 2015, que entrou em vigor no início do presente ano e institui o Programa de Combate à Intimidação Sistemática (*Bullying*). Por se tratar de uma norma recente, porém, ainda não foi possível avaliar sua eficácia e suas eventuais falhas.

17. A auditoria do TCU em 30 instituições e o levantamento de Governança de TI em 372 organizações governamentais indicaram que a segurança das redes públicas está aquém do desejado. Ademais, os depoimentos das autoridades de inteligência ligadas à Presidência da República indicaram que os ataques cibernéticos são

ameaças reais e constantes. Nesse contexto, a CPI conclui pela necessidade, apontada pela Sub-Relatoria do Deputado Rodrigo Martins, do Poder Público adotar, de maneira resumida: **i) guia de boas práticas em segurança da informação; ii) medidas concretas para o reforço e a correta implantação de plano nacional de segurança cibernética; iii) medidas concretas de auditoria em sua infraestrutura pública de TI, e; iv) celebração de instrumentos de cooperação técnica entre autoridades públicas de segurança cibernética e entidades privadas;**

18. O fenômeno crescente de aplicativos de mensageria, tais como o Whatsapp e o Viber, representam não só uma mudança no modelo de negócios no setor de telecomunicações, mas um novo paradigma de segurança que precisa ser melhor equacionado. Esses serviços são criptografados, na maioria das vezes não possuem representação no país e veiculam todo tipo de conteúdo, legal e ilegal. É preciso encontrar uma solução que equacione liberdade, inovação e livre iniciativa à segurança. É inadmissível que quadrilhas se utilizem desses aplicativos para praticar crimes e que as autoridades não tenham acesso a esses sistemas. Ao mesmo tempo, porém, essas são ferramentas indissociáveis da vida moderna. Os recentes casos de bloqueio do Whataspp em todo o Brasil e da prisão do vice-presidente do Facebook na América Latina colocaram em evidência esse conflito. Todavia, esta não é uma realidade apenas brasileira. Nos Estados Unidos ocorreu pugna semelhante entre o FBI e a Apple, quando a autoridade de investigação daquele país solicitou ao fabricante a quebra da segurança de um telefone *Iphone* de suposto terrorista. Em que pese a existência do conflito, o FBI conseguiu, por fim, acessar o dispositivo. Já no caso brasileiro, as investigações ficam rotineiramente prejudicadas, possivelmente devido a falta de disponibilidade de tecnologia por parte das autoridades de investigação. Os episódios indicam que medidas precisam ser tomadas. Nesse sentido, e como forma de melhor balizar as decisões judiciais e o atendimento à legislação brasileira por parte das empresas estrangeiras com atuação no País, a CPI acolhe a proposta do Sub-Relator Deputado Rodrigo Martins que oferece

Projeto de Lei incluindo novo parágrafo ao artigo 22 do MCI, para esclarecer, definitivamente, que filial, sucursal, escritório ou estabelecimento situado no País respondem solidariamente pelo fornecimento de dados requisitados judicialmente de empresas com atuação no país e cuja matriz esteja situada no exterior;

19. A CPI avançou ainda em outros assuntos que embora afeitos à temática dos crimes cibernéticos, fugiam ao escopo inicial das investigações. No entanto, estas indicaram que a CPI deveria se posicionar sobre esses aspectos. Em primeiro lugar, a CPI recebeu diversas reclamações acerca de práticas de tarifação e de bilhetagem das operadoras de telefonia, em especial no que diz respeito ao pacote de dados da internet móvel. Para dirimir a questão, a CPI acolhe sugestão de nossa **Presidente Deputada Mariana Carvalho de oferecer Proposta de Fiscalização e Controle para que, com o apoio do Tribunal de Contas da União, possa-se verificar como a Anatel tem realizado o acompanhamento e o controle da tarifação dos pacotes de dados da telefonia móvel**. Esta medida reveste-se de renovada atualidade em face à recente polêmica do possível corte da conexão à internet de usuários que tiverem excedido a franquia, por parte das operadoras de telefonia. Em segundo lugar, a CPI ouviu representantes da Volkswagen para discutir o escândalo do software que burla a legislação ambiental. Certos da necessidade de aprofundar essas investigações, a CPI acolhe a sugestão do **Deputado JHC de sugerir a continuidade das investigações acerca da introdução de códigos maliciosos com as demais montadoras de veículos em colegiado específico**. Em terceiro lugar, ouvimos as inquietudes acerca da segurança nacional e da possibilidade de ataques terroristas durante os Jogos Olímpicos. Sensibilizados com a temática, os membros desta CPI também acolhem sugestão dos **Deputados Delegado Eder Mauro e Silas Freire para sugerir o aprofundamento das implicações de eventuais atentados terroristas por colegiado específico**. Em quarto e último lugar, a CPI acolhe sugestão do **Dep. Paulo Henrique Lustosa no sentido de encaminhar proposta ao Centro**

de Estudos e Debates Estratégicos para que desenvolva estudo sobre o impacto e a necessidade de regulação na questão do *bigdata*.

20. Em diversos outros assuntos a CPI não dispôs de tempo hábil para investigar, dentre os quais desejamos destacar os mais importantes. Em primeiro lugar, a ***deep web***. Em verdade, o colegiado foi apenas alertado da existência, mas não pôde avançar no seu entendimento. Questões como quais sítios hospedam conteúdos da *deep web* no Brasil, quem são os usuários e como se financiam os pontos de acesso à rede profunda são alguns dos pontos que devem ser esclarecidos e que possuem grande importância na mitigação dos crimes cibernéticos. Uma segunda temática que merece maior aprofundamento é relativa aos ***bots*** (*robots*, *internet bots* ou *web robots*), que simulam a ação humana de forma repetitiva e padronizada no meio digital, podendo, por exemplo, aumentar a visualização de um site de forma indevida, o que pode acarretar em fraude no pagamento de visualizações e publicidade na internet. Esses são alguns dos tópicos em que maiores e mais profundos estudos são necessários.

21. Também não houve tempo hábil para avançar em investigações relacionadas a agências de comunicação na internet que podem estar ligadas a esquemas de financiamento ilegal de campanhas. Nesse particular, todavia, foi divulgado recentemente que a dona da Pepper Interativa assinou acordo de colaboração premiada na Operação Acrônimo, o que evidencia que os órgãos competentes já estão investigando essas supostas irregularidades.

22. Com relação aos Projetos de Lei em tramitação, os Sub-Relatores indicaram quais proposições podem levar ao aperfeiçoamento da legislação brasileira acerca do tema, após, claro, sua ampla discussão nessa Casa. A saber: os PLs: i) 1776/15 (de autoria do Deputado Paulo Freire), que inclui no rol de crimes hediondos os crimes de pedofilia; ii) 3.237/15 (de autoria do Deputado Vinícius Carvalho), que dispõe sobre a guarda dos registros de conexão à internet de sistema autônomo; iii) 5555/2013 (de autoria do Deputado João Arruda) e apensados, que tratam da divulgação não

autorizada de imagens íntimas das vítimas (a vingança pornô); iv) 3686/2015 (de autoria do Deputado Ronaldo Carletto), que “tipifica o crime de intimidação sistemática (Bullying), prevendo causa de aumento se a conduta for realizada por meio da internet (Cyberbullying)”; v) 7544/2014 (de autoria do Deputado Ricardo Izar), que tipifica a conduta de incitação virtual ao crime; vi) 1755/2015 (de autoria do Deputado Raul Jungmann) e apensados, que tratam da criminalização da divulgação indevida, na internet, de informações pessoais; vii) Projeto de Lei nº 6726/2010 (de autoria do Deputado Arnaldo Faria de Sá), que dispõe sobre o acesso de autoridades às informações relativas à localização de aparelhos de telefonia celular; viii) Projeto de Lei nº 2801/2015 (de autoria do Dep. JHC), que altera a Lei Federal nº 9.394/1996 - que Estabelece as diretrizes e bases da educação nacional, para acrescentar finalidade ao Ensino Médio no sentido de incluir a necessidade de educação quanto aos meios telemáticos de comunicação e comportamento e tecnologia, e; ix) Projeto de Lei do Senado 730, de 2015 (que recebeu, na Câmara, o nº 5074/2016), de autoria do Senador Otto Alencar, que dispõe sobre investigação criminal e a obtenção de meios de prova de crimes praticados na internet.. Todos esses projetos merecem um debate aprimorado neste Parlamento, que certamente possui melhoramentos a oferecer.

23. Uma das conclusões mais naturais que advém dos trabalhos desta CPI foi a sua incapacidade de exaurir as investigações, os temas e as propostas atinentes ao mundo dos crimes cibernéticos, Por esses motivos, acolhemos a sugestão do Deputado Silas Freire, para que a Comissão de Ciência, Tecnologia, Comunicações e Informática, crie Subcomissão para tratar do tema dos crimes cibernéticos de maneira perene.

24. Os crimes cibernéticos, quando aplicados no processo eleitoral, possuem efeito devastador no estado democrático de direito. Como bem lembrado em contribuição dada a esta CPI pelo Segundo-Secretário da Câmara dos Deputados, Deputado Felipe Bornier, o baixo custo do uso da internet e a sua capacidade de difusão das informações podem transformar a internet em “um veículo de

> guerrilha eleitoral". Para coibir esse mau uso e diminuir os seus efeitos deletérios sobre o processo democrático, encampamos a sugestão dada pelo nobre Segundo-Secretário. Incluímos em nosso relatório Indicação ao Presidente do Superior Tribunal Eleitoral para que tome as providências necessárias para a criação de força tarefa, no âmbito de cada Tribunal Regional Eleitoral, com membros da Polícia Federal, Ministério Público e respectivos tribunais, visando a célere apuração de cibercrimes eleitorais.

Esses foram os principais temas que, em maior ou menor grau, esta CPI abordou.

Portanto, concordando com as propostas apresentadas pelos Sub-Relatores, Deputados Sandro Alex, Rafael Motta, Daniel Coelho e Rodrigo Martins, conclamo os nobres pares à aprovação do presente Relatório Final da CPI dos Crimes Cibernéticos.

PARTE III – PROPOSIÇÕES E RECOMENDAÇÕES

1 – PROJETOS DE LEI

1.1 – PROJETO DE LEI QUE PERDA DOS INSTRUMENTOS DO CRIME DOLOSO DESTINADOS À PRÁTICA REITERADA DE CRIMES.

(Decorrente da Constatação item 2.1.3)

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)

Estabelece a perda dos instrumentos do crime doloso destinados à prática reiterada de crimes.

O Congresso Nacional decreta:

Art. 1º Esta Lei estabelece a perda dos instrumentos do crime doloso destinados à prática reiterada de crimes.

Art. 2º O inciso II do art. 91 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, passa a vigorar acrescido da seguinte alínea “c”:

“Art. 91. .....

.....

II - .....

.....

c) dos instrumentos do crime doloso, ainda que de origem lícita, quando demonstrado que sua utilização destinava-se à prática reiterada de crimes.” (NR)

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

JUSTIFICAÇÃO

Tradicionalmente, quando se fala em repressão ao crime, a primeira medida que vem à cabeça diz respeito à privação da liberdade daqueles que delinquem.

Todavia, essa mentalidade vem mudando nos últimos tempos, pois outras medidas – como o perdimento de bens, por exemplo – têm se mostrado como um importante instrumento de combate à criminalidade. Afinal, o confisco de bens e valores acaba promovendo a asfixia econômica de certos crimes ou grupos criminosos.

Por essa razão, propõe-se que os instrumentos do crime doloso, mesmo que de origem lícita, sejam perdidos em favor da União, quando utilizados reiteradamente para a pática de crimes, ressalvado o direito do lesado ou de terceiro de boa-fé. Aponte-se que, na sistemática atual do Código Penal, se determinado indivíduo utiliza de um aparato de origem lícita (computadores, por exemplo) para a prática reiterada de crimes cibernéticos, esse bem, após periciado, será restituído ao criminoso.

Entendemos, porém, que os instrumentos que o indivíduo utiliza intencionalmente para a prática reiterada de crimes não podem lhe ser restituídos. Tal medida, além de ser uma pena eficaz contra a prática de delitos, impede que o mesmo instrumento seja novamente utilizado para práticas ilícitas.

Aponte-se, por fim, que tal medida encontra amparo no texto constitucional, ao assentar que uma das penas que pode ser adotada pela lei é exatamente a “*perda de bens*” (art. 5º, inc. XLVI, alínea “b”).

Ressalte-se, por fim, que autoridades de investigação afirmaram a esta CPI que essa medida pode aprimorar, por exemplo, o combate às fraudes bancárias eletrônicas, que, nos últimos anos, gerou prejuízo de bilhões de reais às instituições financeiras e, por consequência, aos seus correntistas.

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

1.2 – 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.

(Decorrente da Constatação item 2.4.1)

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, expondo os dados informatizados a risco de divulgação ou de utilização indevidas:

Pena - detenção, de três meses a um ano, 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 - obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, arquivos, senhas, informações ou outros documentos ou dados privados;

III - controle remoto não autorizado do dispositivo acessado:

Pena – detenção, de seis meses a dois 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 um a quatro anos, e multa.

§ 4º 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 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. A proposta determina que, caso os dados informatizados acessados indevidamente sejam

expostos a risco de divulgação ou de utilização indevida, a conduta será criminalizada.

Ressalte-se que a conduta continua a ser punida apenas em sua forma dolosa, ou seja, quando há a intenção de acessar sistema informatizado contra a vontade de quem de direito. A modalidade culposa apenas pode ser punida quando há expressa previsão legal (art. 18, inciso II, parágrafo único, do Código Penal), o que não é o caso do tipo penal em questão.

O que se propõe é, apenas, que não se exija um dolo específico para a configuração do delito (ou seja, a finalidade específica de "obter, adulterar ou destruir dados ou informações" ou de "obter vantagem ilícita", como consta da atual redação). Isso porque o acesso indevido, independentemente da finalidade, já viola os direitos relacionados à intimidade e à privacidade da vítima. Ademais, conforme aponta a doutrina, "*com essa previsão de elemento subjetivo específico, percebe-se que o tipo penal fez uma restrição temerária ao horizonte de abrangência da norma. É possível que nessas invasões despretensiosas (em que a satisfação da conduta restringe-se a conseguir violar a segurança de determinado sistema computacional, mesmo sem a intenção de obter, adulterar ou destruir dados), o primeiro autor deixe aberta as portas para que um segundo criminoso, sem qualquer ajuste entre os dois, agora com a intenção de obter informações, por exemplo, atue livremente, chegando ao extremo de nem mesmo responder pelo crime, já que ele não violou indevidamente a segurança, pois esta já estava violada*"[35].

Com este Projeto, busca-se suprimir do tipo, também, a necessidade de que haja a violação de mecanismo de segurança. Afinal, repita-se, o acesso indevido, por si só, já viola os direitos relacionados à intimidade e à privacidade da vítima. Faz-se um paralelo com o crime de invasão de domicílio, que não exige, para a sua configuração, que a porta da residência esteja trancada.

A proposta exige para a configuração do delito, porém, que os dados informatizados sejam expostos a risco de divulgação ou de utilização

[35] BRITO, Auriney. Direito penal informático. São Paulo: Saraiva, 2013, p. 71.

indevidas, o que afasta a tipicidade de condutas que não possuem qualquer ofensividade, como a simples violação de “termos de uso”, por exemplo.

Aponte-se por fim, que não se está alterando a ação penal relacionada ao tipo, que continua sendo condicionada à representação, a não ser em casos específicos como contra a Administração. Dessa forma, invasões em que a vítima não vislumbrar a necessidade de dar início a investigação criminal, isso não ocorrerá.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

1.3 – 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.

(Decorrente da Constatação item 2.4.4)

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. De fato apenas os Estados da Bahia, Mato Grosso do Sul, Maranhão, Paraná e Rio Grande do Sul, responderam positivamente aos Ofícios desta CPI indagando acerca da existência de órgãos especializados para o combate a esses crimes como dita a Lei de 2012.

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.

Neste contexto, o FNSP - Fundo Nacional de Segurança Pública (criado pela Lei nº 10.201/01), que possui provisão legal específica para o

apoio a projetos que tratem de reequipamento das polícias, estabelecimentos de sistemas de informações e outros, surge como a opção mais óbvia. Ocorre, no entanto, que este Fundo possui recursos insuficientes e parca execução orçamentária. Segundo o sistema de acompanhamento de execução orçamentária da Câmara dos Deputados, em 2013, pouco mais de R$200 milhões foram liquidados de uma previsão orçamentária de R$ 640 milhões. Em 2014, repetiu-se essa realidade. Em 2015, menos ainda: apenas R$ 190 milhões foram liquidados de uma previsão orçamentária de R$ 930 milhões. Certamente, com esses valores, o fundo não poderá encampar todas as suas atribuições e também promover projetos para a investigação dos crimes cibernéticos. Essa realidade levou esta CPI a buscar fontes alternativas para o financiamento desses tipos de investigações.

Nessa busca por novas fontes de recursos, a CPI deparou-se com o Fistel – Fundo de Fiscalização das Telecomunicações -, que constituiu-se, na prática, em fonte de financiamento do Governo Federal para as mais distintas tarefas. Instituído pela Lei nº 5.070/66, o fundo foi criado para, dentre outras finalidades, o "aperfeiçoamento da fiscalização dos serviços de telecomunicações existentes no País".

Entretanto, o fundo já possui a previsão na Lei que o instituiu para que parte de seus recursos possam ser transferidos para o Tesouro Nacional. A rubrica arrecada aproximadamente R$ 2 bilhões anuais e, como amplamente noticiado na imprensa, seus recursos são sistematicamente repassados ao Tesouro, principalmente para fins de superávit fiscal. Apenas algo em torno de R$ 400 milhões são utilizados para a fiscalização do setor.

Devido a essa sistemática histórica adotada pelo Governo Federal, entendemos que a destinação de parte dos recursos já derivados para o Tesouro Nacional poderiam ser reaplicados na estruturação das polícias judiciárias para o combate aos crimes cibernéticos. Essa aplicação guardaria total paralelismo com o principal objetivo do fundo, quer seja a fiscalização no bom uso dos sistemas de telecomunicações, uma vez que essa é a infraestrutura de suporte aos dados que navegam pela rede mundial de computadores.

Por esses motivos, propomos que apenas 10% dos recursos repassados ao caixa central da União, aproximadamente R$ 160 milhões, e que, portanto, o Governo decidiu em Lei Orçamentária por não utilizar diretamente na

fiscalização do setor, 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

1.4 – PROJETO DE LEI QUE INCLUI OS CRIMES PRATICADOS CONTRA OU MEDIANTE COMPUTADOR, CONECTADO OU NÃO A REDE, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO OU DE TELECOMUNICAÇÃO NO ROL DAS INFRAÇÕES DE REPERCUSSÃO INTERESTADUAL OU INTERNACIONAL QUE EXIGEM REPRESSÃO UNIFORME, QUANDO HOUVER INDÍCIOS DA ATUAÇÃO DE ASSOCIAÇÃO CRIMINOSA EM MAIS DE UM ESTADO DA FEDERAÇÃO OU NO EXTERIOR.

(Decorrente da Conclusão do Relator item 4.12)

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)

Inclui os crimes praticados contra ou mediante computador, conectado ou não a rede, dispositivo de comunicação ou sistema informatizado ou de telecomunicação no rol das infrações de repercussão interestadual ou internacional que exigem repressão uniforme, quando houver indícios da atuação de associação criminosa em mais de um Estado da Federação ou no exterior.

O Congresso Nacional decreta:

Art. 1º Esta lei inclui os crimes praticados contra ou mediante computador, conectado ou não a rede, dispositivo de comunicação ou sistema informatizado ou de telecomunicação no rol das infrações de repercussão interestadual ou internacional que exigem repressão uniforme.

Art. 2º O artigo 1º da Lei nº 10.446, de 8 de março de 2002, passa a vigorar acrescido do seguinte inciso VII:

"Art. 1º.....

.....

VII – crimes praticados contra ou mediante computador, conectado ou não a rede, dispositivo de comunicação ou sistema informatizado ou de telecomunicação, quando houver indícios da atuação de

associação criminosa em mais de um Estado da Federação ou no exterior.

....." (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.

Uma questão que chamou a atenção, por exemplo, diz respeito à ausência de uma norma específica no que tange à competência para a investigação desses delitos. Assim, os casos envolvendo crimes praticados na internet – que geralmente possuem repercussão interestadual ou, até mesmo, internacional – continuam sendo, na maioria das vezes, de competência investigativa das policias civis estaduais.

Entendemos, porém, que esses delitos, quando necessitarem de uma repressão uniforme, devem ficar a cargo da Polícia Federal sempre que houver repercussão interestadual ou internacional e houver indícios da atuação de associação criminosa em mais de um Estado da Federação ou no exterior.

É com esse intuito que apresentamos o presente projeto de lei.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

1.5 – PROJETO DE LEI DETERMINANDO A INDISPONIBILIDADE DE CÓPIA IDÊNTICA DE CONTEÚDO RECONHECIDO COMO INFRINGENTE, SEM A NECESSIDADE DE NOVA ORDEM JUDICIAL E DÁ OUTRAS PROVIDÊNCIAS.

(Decorrente da Constatação item 2.3.1)

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 a indisponibilidade de cópia idêntica de conteúdo reconhecido como infringente, sem a necessidade de nova ordem judicial e dá outras providências.

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 a indisponibilidade de cópia idêntica de conteúdo reconhecido como infringente, sem a necessidade de nova ordem judicial e dá outras providências.

Art. 2º A Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet, passa a vigorar acrescida dos seguintes dispositivos:

"Art. 20-A O provedor de aplicação deverá indisponibilizar, no âmbito e nos limites técnicos dos seus serviços, no prazo de 48 horas após o recebimento de notificação pelo interessado ou representante legal, conteúdo infringente idêntico ao objeto de ordem judicial anterior, hipótese na qual não poderá ser responsabilizado pelas consequências da eventual falta de correspondência entre os conteúdos.

§1º. A remoção de conteúdo prevista no *caput* dependerá de notificação que deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como

infringente, a conferência da validade da ordem judicial em questão e a verificação da legitimidade para apresentação do pedido.

§2º: Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere este artigo, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à sua indisponibilização, possibilitando que ingresse em juízo para assegurar o seu direito à liberdade de expressão e a responsabilização por abuso de direito ou pelo dano causado por retirada decorrente de notificação indevida.

.....

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

Nossa Carta Magna garante, no seu artigo 5º, a todos os brasileiros e residentes, a livre manifestação do pensamento, a livre comunicação, o sigilo nas comunicações, o acesso à informação e a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. Passados mais de vinte e cinco anos da promulgação da Constituição Federal, o Marco Civil da Internet (MCI), aprovado pela Lei nº 12.965/14, transportou para o mundo virtual

todas essas garantias constitucionais basilares que definem, em sua essência, os ideais democráticos brasileiros.

Em que pese a necessidade e o acerto das disposições contidas no MCI, os depoimentos de diversas autoridades de investigação, que compareceram em reiteradas Audiências Públicas realizadas pela CPI dos Crimes Cibernéticos, atentaram para duas questões que merecem reparos.

O primeiro ponto diz respeito à dificuldade em se manter fora da rede mundial de computadores conteúdos considerados como infringentes por ordens judiciais. Essa questão é extremamente importante, pois, no mundo da internet, conteúdos difamatórios, ofensas e outros tipos de ataques pessoais, especialmente pelas redes sociais, são extremamente deletérios. A amplificação do dano advém da característica das mídias digitais que permitem a replicação e a continuidade das postagens de forma impessoal e com pouco ou nenhum esforço. Some-se às facilidades tecnológicas a possibilidade de viralização dos conteúdos e a honra de uma pessoa pode ser destruída em poucos dias. Mais do que a honra, os ataques podem resultar, nos casos mais extremos, em linchamentos e até mortes. Em suma, a replicação continuada de conteúdos pode custar vidas e resultar em prejuízos incalculáveis.

Outra consequência a ser ressaltada desta replicação continuada é que, no mundo digital, deve-se considerar a impossibilidade prática do direito ao esquecimento. Bastam alguns cliques para que postagens sejam revividas e o pesadelo das vítimas seja reiniciado.

Por esses motivos, é imperativo que sejam envidados esforços substanciais para que conteúdos tidos como infringentes pela justiça, permaneçam fora do ar. O novo parágrafo ao artigo 19 que propomos ao MCI determina aos provedores de aplicação tomar as providências técnicas necessárias para que conteúdos infringentes continuem indisponíveis em caso de cópia, dispensada a necessidade de nova ordem judicial para a retirada desses novos materiais.

Entendemos que pela prática atual, em que os provedores de conteúdos exigem nova decisão judicial para a remoção de réplicas do mesmo conteúdo originalmente bloqueado, as vítimas são penalizadas de sobremaneira. As principais aplicações dispõem de todas as condições técnicas e os recursos

financeiros necessários para bloquear essas replicações. As vítimas, em contrapartida, precisam acionar de maneira contínua a justiça, depreendendo tempo e recursos, muitas vezes escassos. O país possui desigualdades sociais que não podem ser desconsideradas, o acesso à justiça não se dá de maneira equânime por parte de todos os segmentos da sociedade. Esta é uma forma de facilitar a proteção desses segmentos.

No estudo da matéria pela CPI dos Crimes Cibernéticos foram sugeridas diversas propostas para regulamentar o assunto. Após profícuo debate com Parlamentares, instituições e membros da sociedade organizada, entendemos que o CGI.br apresentou contribuição que mais se aproxima do entendimento por parte dos membros desta Comissão sendo acatada em sua quase totalidade nesta proposta. A sugestão determina que conteúdos idênticos devem ser retirados após notificação por parte do usuário. No entanto, a sólida instituição técnica indica que essa retirada também deva se dar em casos de conteúdos “que contenham parte majoritária e que reproduza a infração decorrente do conteúdo removido por ordem judicial”. As discussões no colegiado salientaram o fato de que a introdução de elementos de subjetividade poderia levar ao uso extremado de retiradas como medida de precaução por parte dos provedores de aplicação e seria, consequentemente, danoso para o desenvolvimento saudável da internet. Portanto, não consideramos a melhor solução essa extensão. Por outro lado, o CGI.br não estabelece prazos para a retirada, o que entendemos ser deletério para a manutenção da proteção dos usuários. Neste particular determinamos que a retirada deva se dar em 48 horas após a notificação.

Salientamos que variantes desta abordagem, similar ao que se convencionou chamar NOTICE AND STAY DOWN, é objeto de estudos e de decisões judiciais em diversos países, tais como Estados Unidos e Alemanha. Sendo que a principal argumentação que justifica sua implementação é que os grandes provedores de aplicação, deveriam fazer mais para a proteção dos cidadãos e dos pequenos criadores.

O segundo ponto tratado pelo projeto, correlato ao anterior, diz respeito ao atendimento das notificações pelas empresas estrangeiras. Também 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 estas alterações ao Marco Civil da Internet, as dificuldades pelas quais estão passando as autoridades de investigação, o Poder Judiciário e, principalmente, as vítimas de crimes contra a honra 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

1.6 – PROJETO DE LEI QUE POSSIBILITA O BLOQUEIO DE APLICAÇÕES DE INTERNET POR ORDEM JUDICIAL, NOS CASOS EM QUE ESPECIFICA.

(Decorrente da Constatação item 2.1.4 e 2.2.3)

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)

Possibilita o bloqueio a aplicações de internet por ordem judicial, nos casos em que especifica.

O Congresso Nacional decreta:

Art. 1º Esta lei altera a Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet, para possibilitar o bloqueio a aplicações de internet por ordem judicial, nos casos em que especifica.

Art. 2º A Lei nº 12.965, de 23 de abril de 2014, passa a vigorar com a seguinte redação:

"Seção V

Do Bloqueio a Aplicações de Internet em Atendimento a Ordem Judicial

Art. 23-A O Juiz somente poderá determinar que o provedor de conexão bloqueie o acesso a aplicação de internet hospedada no exterior ou que não possua representação no Brasil e que seja precipuamente dedicada à prática de crimes puníveis com pena mínima igual ou superior a dois anos de reclusão, excetuando-se os crimes contra a honra.

§ 1º Para o bloqueio de que trata este artigo deverão ser considerados o interesse público, a proporcionalidade, o alcance da medida e a celeridade necessária para promover a efetiva cessação da conduta criminosa.

§ 2º Considera-se representada no Brasil a aplicação de internet que possua responsável legalmente constituído no País ou que pelo menos um integrante do mesmo grupo

econômico possua filial, sucursal, escritório ou estabelecimento no País.

§ 3º As aplicações de mensagens instantâneas, de uso público geral, ficam excluídas do bloqueio de que dispõe este artigo.” (NR)

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

JUSTIFICAÇÃO

A internet, como se sabe, desde o seu surgimento trouxe enormes benefícios à sociedade, em termos de conhecimento, relações sociais, dentre outros. Mas, infelizmente, da mesma forma que a internet pode ser utilizada – e de fato o é – para a realização de coisas boas, ela também vem sendo palco para a realização de diversos crimes, conforme amplamente demonstrado na CPI dos Crimes Cibernéticos.

Inclusive, não é novidade a existência se sites voltados quase que exclusivamente à disponibilização e distribuição de conteúdos ilícitos.

Dessa forma, mostra-se importante inserir no Marco Civil da Internet a possibilidade de o judiciário brasileiro determinar aos provedores de conexão medidas técnicas de bloqueio de tráfego, quando esses conteúdos estejam fora do alcance de medidas judiciais céleres de proteção das pessoas.

Isso se faz necessário porque a indisponibilização de serviços ilegais prestados a partir de provedores de hospedagem localizados em território brasileiro pode ser bastante simples, uma vez que basta ao juiz determinar ao provedor de hospedagem brasileiro a retirada de conteúdos que violam direitos de qualquer gênero. Ademais, a ação pode se dar no emprego direto da força policial para desbaratar operações ilegais. O mesmo não se verifica para serviços ilegais hospedados para fora da jurisdição do Estado Brasileiro.

Como exemplo, um website que disponibiliza ilegalmente materiais protegidos por direitos autorais ou fotos de pornografia infantil e que se encontre hospedado em um servidor no exterior, não cumprirá ordem do poder judiciário brasileiro, salvo por meio de carta rogatória, o que evidentemente não representa uma solução adequada do ponto de vista do tempo necessário à sua implementação. Em casos como o mencionado, a solução possível é se determinar aos provedores brasileiros de conexão, que obedecem à jurisdição brasileira, que neguem tráfego ao destino que tenha sido considerado ilegal.

Desta forma, ainda que o hospedeiro estrangeiro não possa ser obrigado a apagar o conteúdo ilegal de seus servidores, o acesso a esses será prejudicado pela medida técnica implementada por provedores brasileiros de conexão.

É com esse intuito que apresentamos o presente projeto de lei.

O Projeto determina a possibilidade de bloqueio ao acesso apenas a aplicações hospedadas no exterior ou que não possuam representação no País e que se dediquem precipuamente à prática de crimes puníveis com pena maior ou igual a dois anos de reclusão. Nesse rol encontram-se aqueles relacionados à exploração sexual de crianças e adolescentes, ao tráfico de drogas, ao tráfico internacional de armas de fogo e à violação de direito autoral com fim de lucro. A proposta prevê que sejam considerados o interesse público, a proporcionalidade o alcance da medida e a celeridade necessária de acordo com cada caso. Propomos excluir expressamente da aplicação deste artigo aqueles conteúdos relacionados a crimes contra a honra.

Por fim, devido à polêmica relacionada com o bloqueio ao aplicativo de mensagens instantâneas, Whatsapp, em que decisão de juiz determinou sua suspensão em todo o território nacional, optamos por expressar claramente que o bloqueio não poderá se dar para esses tipos de aplicativos.

Estamos certos de que com a redação proposta as autoridades judiciais terão um instrumento legal que lhes permitirá agir com proporcionalidade.

Aponte-se que a proteção ora pretendida já encontra previsão em outras democracias ocidentais, a exemplo de países da União

Europeia, Estados Unidos e Chile. A lei chilena, por exemplo, que trata a neutralidade da rede de forma extremamente ampla, veda o bloqueio e garante o acesso apenas a serviços ou a aplicações legais (Ley 20.453, art. 24H). A Regulação 2120, de 2015, do Conselho e do Parlamento da Europa, em seu art. 3º, garante aos usuários o acesso a conteúdos e serviços, desde que estes sejam legais, permitindo o seu bloqueio para o cumprimento de leis ou ordens judiciais. Da mesma forma, nos Estados Unidos a lei não isenta os provedores de tomarem medidas necessárias para coibir atividades ilegais. A Constituição daquele País e em particular a Primeira Emenda garantem a liberdade de expressão como um pilar basilar dos direitos do cidadão, o que abrange, segundo o entendimento da Suprema Corte daquele país, até mesmo o direito ao anonimato (o que não encontra respaldo na Constituição brasileira). No intuito de assegurar essa elástica garantia constitucional, o órgão regulador das telecomunicações daquele país publicou a Resolução de Proteção e Promoção da Internet Aberta, de 13/04/2015, assegurando ao usuário o direito a acessar destinos legais na internet e que provedores não podem bloquear conteúdos legais. Assim, o Código de Regulações Federais (CFR, Título 47, Capítulo I, Subcapítulo A, Parte VIII, Seção 8.5), determina que os provedores de internet não podem bloquear conteúdos legais. No entanto, na Seção 8.9 do Código, é determinado que não são proibidos esforços razoáveis por provedores de acesso com o intuito de resolver infrações a direito autoral ou a outras atividades ilegais. Como não poderia deixar de ser, essa exceção, focada na manutenção da legalidade, guarda total consonância com os preceitos constitucionais daquele país.

Ressaltamos que conforme amplamente divulgado por diversas entidades de proteção aos direitos autorais, tais como Associação Brasileira de Direito Autoral, Associação Brasileira de Propriedade Intelectual, Associação Brasileira de Produtores Independentes de Televisão e Fórum Nacional Contra a Pirataria e a Ilegalidade, esse tipo de bloqueio existe em países com democracias solidamente estabelecidas, entre elas Reino Unido, Austrália, Espanha, França, Coreia do Sul, Bélgica, Dinamarca, Alemanha, Suécia, Holanda e Itália.

Por esses motivos, conclamamos os nobres pares à aprovação da matéria.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

2 – PROPOSTA DE FISCALIZAÇÃO E CONTROLE

2.1 – 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.

(Decorrente da Constatação item 2.4.5)

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.

6. Examinar se a Anatel possui levantamento do quantitativo de uso de celulares pré-pagos para o acometimento de crimes, discriminados por tipos, e o registro de linhas desativadas ou denunciadas devido ao seu uso para a prática de delitos.

7. Estudar a viabilidade de inclusão no termos do regulamento do Serviço Móvel Pessoal a aplicação de multa às operadoras, nos casos de fraudes contra clientes do Sistema Financeiro Nacional em que houver falha na correta identificação do proprietário da linha ou uso de dados falsos ou inverídicos.

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

2.2 – 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 BILHETAGEM DOS SERVIÇOS DE DADOS POR PARTE DAS PRESTADORAS DO SERVIÇO MÓVEL PESSOAL.

(Decorrente da Constatação item 2.5.1)

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 bilhetagem dos serviços de dados por parte das prestadoras do Serviço Móvel Pessoal.

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 às ações de acompanhamento e controle daquela Agência acerca da correta bilhetagem dos serviços de dados por parte das prestadoras do Serviço Móvel Pessoal, para elucidar as seguintes questões:

1. Verificar quais foram os procedimentos de fiscalização realizados pela Agência com o intuito de averiguar a coleta e a consolidação das informações de tráfego de dados dos usuários por parte das prestadoras do Serviço Móvel Pessoal, bem como a cobrança pela prestação do serviço, e quais os resultados dessas fiscalizações;

2. Verificar quais foram os procedimentos de fiscalização realizados pela Agência com o intuito de verificar o cumprimento do disposto na Resolução n.º 632, de 2014, que *"Aprova o Regulamento Geral*

de Direitos do Consumidor de Serviços de Telecomunicações – RGC", especialmente quanto ao art. 62, incisos VII, VIII e X, no que tange aos serviços de conexão à internet oferecidos por prestadoras do Serviço Móvel Pessoal, e quais os resultados dessas fiscalizações;

3. Verificar quantas e quais foram as multas aplicadas pela Anatel por descumprimento do citado regulamento, em consonância com o disposto na Resolução n.º 589, de 7 de maio de 2012, que "*Aprova o Regulamento de Aplicação de Sanções Administrativas*";

JUSTIFICAÇÃO

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.

Durante os trabalhos da CPI seus integrantes receberam diversas indicações de descontentamento por parte dos usuários com os serviços prestados pelas operadoras de telecomunicações, em especial no que diz respeito ao consumo de dados nos planos de banda larga da telefonia móvel.

Na análise da importância da matéria é necessário o entendimento de que a internet trouxe consigo uma revolução em diversas dimensões da sociedade brasileira, modificando definitivamente o modo como as pessoas se relacionam e acessam informações. Tal é a importância dessa tecnologia na vida do cidadão contemporâneo que sequer consegue-se imaginar

como seria o mundo de hoje sem a rede mundial de computadores.

A ubiquidade da internet tira grande parte de sua força na evolução sofrida pelos aparelhos celulares que, se há duas décadas serviam apenas para realizar ligações telefônicas, hoje se tornaram computadores portáteis capazes de fazer uma infinidade de tarefas. De fato, a evolução da internet e dos *smartphones* se confunde, ao ponto destes se tornarem completamente reféns da existência daquela para funcionarem em sua plenitude.

Dados do setor apontam que, em 2013, havia cerca de 52 milhões de usuários de internet móvel no Brasil[36]. Esse número saltou para mais de 82 milhões de pessoas ao final e 2014[37], uma evolução de 57% em apenas um ano. Atualmente, a internet móvel já é utilizada por metade da população brasileira, e certamente essa penetração continuará crescendo.

É certo que o crescimento meteórico no número de usuários de internet móvel veio acompanhado de um aumento não menos expressivo no volume de dados trafegados pelas redes das operadoras do Serviço Móvel Pessoal (SMP). Infelizmente, e como não poderia deixar de ser, essa bonança veio acompanhada também da explosão na insatisfação e no número de reclamações dos consumidores relativamente a esse serviço.

Possivelmente motivados por todo esse crescimento, e incapazes de expandir suas próprias redes a um ritmo tão acelerado, as prestadoras SMP resolveram, de forma mais ou menos coordenada, acabar com a possibilidade do usuário continuar desfrutando da internet móvel, mesmo que com velocidade reduzida, após superada a franquia de dados contratada. Essa decisão das prestadoras evidenciou ainda mais uma dúvida que já era um dos grandes motivos de reclamação dos assinantes, qual seja, como saber se a prestadora está medindo o consumo de dados corretamente.

A preocupação da sociedade com o assunto é tão evidente que, atualmente, já tramitam nessa casa os PL 418/2015 e PL 4470/2015, ambos no sentido de proibir as prestadoras de SMP de interromper o acesso a internet para o usuário que exceder a franquia de dados contratada no SMP.

[36] http://cetic.br/tics/usuarios/2013/total-brasil/J5/
[37] http://cetic.br/tics/usuarios/2014/total-brasil/J5/

Importante ressaltar que a Anatel já regulamentou a questão por meio da Resolução n.º 632, de 7 de março de 2014, que dispõe, no art. 62, que as prestadoras deverão disponibilizar aos assinantes, entre outras, as seguintes informações: *"VII – o volume diário de dados trafegados; VIII - os limites estabelecidos por franquias e os excedidos; ...; X - o valor da chamada, da conexão de dados ou da mensagem enviada, explicitando os casos de variação horária;"*. Entretanto, esta CPI não tem conhecimento de nenhuma atividade de controle ou fiscalização por parte do órgão regulador com intuito de verificar o cumprimento desses dispositivos.

Este é, certamente, um campo em que o Poder Público precisa se debruçar. Nesse sentido e até para chancelar as boas práticas das operadoras de telefonia, é mister avaliar as práticas de bilhetagem, especificamente na questão do consumo de dados. Por estas razões, a CPI dos Crimes Cibernéticos apresenta esta Proposta de Fiscalização e Controle para que, com o apoio do Tribunal de Contas da União, possamos verificar como o órgão público a quem compete a fiscalização das telecomunicações, ou seja, a Anatel, tem realizado o acompanhamento e o controle das prestadoras do SMP no que tange a cobrança e a medição do consumo dos pacotes de dados móveis.

Ademais, deve ser levado em consideração que o corte após o uso da franquia de dados contratada pode levar os usuários a deixarem de atualizar aplicativos e diretivas de segurança como forma de economizar seu pacote de dados. Assim, a segurança dos dispositivos fica comprometida. Neste particular, entendemos que a mudança dos planos permitindo a desconexão de usuários quando atingem a franquia contratada é potencialmente nociva para a segurança cibernética. Neste particular entendemos que a legalidade dessa medida, em face de seus impactos na qualidade das redes, deve igualmente ser analisada nesta fiscalização.

Dessa forma, considerando a importância de garantirmos o cumprimento da regulamentação vigente para o setor, bem como a transparência das ações de fiscalização e controle exercidas pelo órgão regulador, insto os nobres Pares para a aprovação desta Proposta de Fiscalização e Controle.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

3 – INDICAÇÕES

3.1 – 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.

(Decorrente da Constatação item 2.4.7)

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 Presidente:

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) adote guia de boas práticas em segurança da informação;

ii) implemente processo de gestão de riscos de segurança da informação;

iii) avalie a possibilidade da adoção de tecnologias, padrões e formatos abertos e livres no estabelecimento de controles de segurança da informação;

iv) realize auditoria em sua infraestrutura pública de TI;

v) celebre instrumentos de cooperação técnica entre autoridades públicas de segurança cibernética e entidades privadas;

vi) direcione esforços para a consecução dos objetivos propostos na Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF, em especial instituir modelo de governança sistêmica de SIC e de SegCiber.

vii) Elabore proposta de “Política Nacional de Segurança da Informação e Comunicações e de Segurança Cibernética”, conforme previsto na Estratégia de

Segurança da Informação e Comunicações e de Segurança Cibernética da Secretaria Executiva do Conselho de Defesa Nacional e que contemple, dentre outras ações, a segurança das comunicações de dados no país, a segurança dos sistemas e da infraestrutura, o monitoramento e a operação contínua da segurança da infraestrutura, e, estabelecimento de regras, padrões e procedimentos para processos e governança das tecnologias de informação e comunicação;

viii) retome Grupo de Trabalho para o estudo da temática da Segurança da Informação em Grande Volume de Dados e sua possível regulamentação, no âmbito do Poder Executivo;

ix) inclua o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Casa Militar nas articulações com as demais instituições públicas que tratam de incidentes e crimes cibernéticos;

x) realize 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;

xi) celebre 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

3.2 – INDICAÇÃO AO BANCO CENTRAL, POR INTERMÉDIO DO MINISTÉRIO DA FAZENDA, SUGERINDO A ADOÇÃO DE MEDIDAS DE COMBATE AOS CRIMES CIBERNÉTICOS.

(Decorrente da Constatação item 2.1.3)

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 Banco Central, por intermédio do Ministério da Fazenda, sugerindo a adoção de medidas de combate aos 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 Banco Central do Brasil a Indicação em anexo, sugerindo a adoção de medidas de combate aos 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 a adoção de medidas de combate aos crimes cibernéticos.

Excelentíssimo Senhor Ministro da Fazenda:

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 Instituições Financeiras e Comércio Virtual, a cargo do Sub-Relator Deputado Sandro Alex. Em sua análise, essa Sub-Relatoria considerou que o combate aos crimes cibernéticos praticados contra a ordem financeira e, em especial, contra as instituições bancárias deve ser realizado com melhor atenção às informações prestadas pelas instituições reguladas e com

maior integração entre as partes envolvidas como a temática.

Por esses motivos, a CPI vem oferecer esta Indicação para a instituição das seguintes medidas:

i) **Promover as medidas necessárias para a promoção de maior integração da instituição com a Polícia Federal, a Febraban e e com órgão responsável pelo tratamento de incidentes de segurança de redes de computadores ligado à Presidência da República para a comunicação de incidentes e o compartilhamento das informações com o objetivo de mitigar os crimes digitais;**

ii) **Propor instrumento regulatório que permita a correta aferição dos crimes cibernéticos no sistema financeiro, em separado, sem desconsiderar o caráter sensível das informações;**

iii) **Elaboração de um sistema de classificação de risco das instituições financeiras que permita aos cidadãos escolher seus prestadores de serviços financeiros e bancários com base em informações que avaliem a incidência de crimes cibernéticos nas instituições, sem desconsiderar o caráter sensível das informações.**

Certos de contar com a compreensão e o comprometimento do Senhor Ministro para a adoção das medidas. Acreditamos que as conclusões emanadas por esse colegiado servirão de sobremaneira para a diminuição de crimes cibernéticos contra o sistema financeiro.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

3.3 – INDICAÇÃO AO MINISTRO DA JUSTIÇA SUGERINDO A ADOÇÃO DE MEDIDAS DE COMBATE AOS CRIMES CIBERNÉTICOS.

(Decorrente da Constatação item 2.1.3)

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 a adoção de medidas de combate aos 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 Indicação ao Ministério da Justiça sugerindo a adoção de medidas de combate aos 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 ao Ministério da Justiça a adoção de medidas de combate aos crimes cibernéticos.

Excelentíssimo Senhor Ministro 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 Instituições Financeiras e Comércio Virtual, a cargo do Sub-Relator Deputado Sandro Alex. Em sua análise, essa Sub-Relatoria considerou que o combate aos crimes cibernéticos praticados contra a ordem financeira e, em especial, contra as instituições bancárias deve ser realizado com

melhor atenção às informações prestadas pelas instituições reguladas e com maior integração entre as partes envolvidas como a temática.

Por esses motivos, a CPI vem oferecer esta Indicação para a criação de Grupo de Trabalho no âmbito dessa instituição com o seguinte escopo:

i) **Promover as medidas necessárias para a promoção de maior integração da Polícia Federal com o Banco Central e com órgão responsável pelo tratamento de incidentes de segurança de redes de computadores ligado à Presidência da República para a comunicação de incidentes e o compartilhamento das informações com o objetivo de mitigar os crimes digitais e, em especial, estabelecer entendimentos para o compartilhamento das informações e a manutenção de um Banco (de Dados) Nacional de Fraudes Bancárias;**

ii) **Regulamentar o inciso VI, do art. 1º da Lei no 10.446/02, Lei das Infrações Federais, obrigando a entrega pelos bancos de notícia crime em casos de crimes cibernéticos.**

iii) **Sugere-se o estabelecimento de convênios entre as polícias federal e civis dos Estados para eventual aplicação de receitas do Fistel, transferidas para o Tesouro Nacional, no financiamento das estruturas de combate a crimes cibernéticos**

Certos de contar com a compreensão e o comprometimento do Senhor Ministro para a implementação das medidas indicadas. Acreditamos que as conclusões emanadas por esse colegiado servirão de sobremaneira para a diminuição de crimes cibernéticos contra o sistema financeiro.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

3.4 – INDICAÇÃO AO CNJ SUGERINDO A CRIAÇÃO DE VARAS JUDICIAIS ESPECIALIZADAS EM CRIMES ELETRÔNICOS.

(Decorrente da Constatação item 2.1.3)

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 Judiciário, sugerindo a criação de Varas Especializadas em Crimes Cibernéticos nos Tribunais brasileiros.

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 Judiciário a Indicação em anexo, sugerindo a criação de Varas Especializadas em 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 a criação de Varas Especializadas em Crimes Cibernéticos nos Tribunais brasileiros.

Excelentíssimo Senhor Presidente do Conselho Nacional de 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 Instituições Financeiras e Comercio Virtual, a cargo do Sub-Relator Deputado Sandro Alex. Em sua análise, essa Sub-Relatoria identificou a necessidade de se avaliar a criação, na estrutura do Poder Judiciário, de Varas Judiciais Especializadas em Crimes Eletrônicos. Com tal medida, seria possível dar maior uniformidade e celeridade ao tratamento desses crimes, e seria possível a criação e a especialização de equipes também no âmbito da Justiça.

Dessa forma, a CPI vem oferecer esta Indicação, sugerindo que o Conselho Nacional de Justiça recomente a criação dessas Varas Especializadas nos Tribunais pátrios.

Certos de contar com a compreensão e o engajamento de Vossa Excelência na consecução da medida sugerida, reiteramos nossos votos de elevada estima e consideração.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

3.5 – INDICAÇÃO AO MINISTÉRIO DA EDUCAÇÃO SUGERINDO A OFERTA DE NOÇÕES DE EDUCAÇÃO DIGITAL NAS ESCOLAS

(Decorrente da Constatação item 2.2.1)

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 da Educação sugerindo a oferta obrigatória de noções de educação digital nas escolas públicas e privadas de ensino fundamental e médio.

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 da Educação Indicação sugerindo a oferta obrigatória de noções de educação digital nas escolas públicas e privadas de ensino fundamental e médio.

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 ao Ministério da Educação a oferta obrigatória de noções de educação digital nas escolas públicas e privadas de ensino fundamental e médio.

Excelentíssimo Senhor Ministro da Educação:

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 Crimes Contra a Criança e o Adolescente, a cargo do Sub-Relator Deputado Rafael Motta. Em sua análise, essa Sub-Relatoria considerou que a educação nos diversos aspectos do uso das tecnologias digitais é de fundamental importância no combate aos crimes cibernéticos, especialmente

àqueles praticados contra essa parcela vulnerável da população.

As tecnologias digitais são de fundamental importância para a vida em sociedade na atualidade. Inúmeros serviços públicos e privados são oferecidos pela internet e muitos destes são apenas oferecidos pela grande rede. Ademais da oferta de produtos e serviços se dar de forma crescente pelos meios digitais de comunicação, as possibilidades de geração de emprego e renda também são cada vez mais importantes na economia real.

Nesse contexto de transformação, em que muitos países estão conseguindo migrar para a economia do mundo digital, o uso que se dá à navegação na internet no Brasil não é necessariamente produtiva. Inúmeras pesquisas apontam que, no País, o uso primário da internet é a conexão às redes sociais, restando as demais atividades a um segundo plano. Também, as investigações da CPI se depararam com inúmeros depoimentos em que foi constatado o desconhecimento dos jovens internautas no uso de práticas de navegação segura na rede mundial. Crianças e adolescentes estão despreparados e desassistidos para o enfrentamento dos desafios inerentes às tecnologias digitais.

Por isso, é absolutamente necessário promover uma mudança radical no uso das tecnologias digitais no país e essa transformação deve ser dada pela educação das pessoas, iniciando pelos jovens internautas.

O Plano Nacional de Educação (PNE), aprovado pela Lei nº 13.005/2014, prevê entre suas diretrizes, constantes do 2º, a “formação para o trabalho e para a cidadania” e a promoção tecnológica do país. Assim, entendemos que para o atingimento dos objetivos do PNE faz-se necessária a capacitação da população estudantil brasileira nas novas tecnologias digitais.

Entretanto, somos cientes de que a criação de disciplinas, áreas de estudo e conteúdos, em qualquer nível ou modalidade de ensino, não é competência do Poder Legislativo, mas sim - como o art. 9º, § 1º, alínea “c”, da Lei nº 9.131, de 1995, determina - do MEC, Conselhos de Educação, unidades escolares e suas comunidades.

Por isso, sugerimos ao Ministério da Educação adotar as medidas necessárias para incluir a oferta obrigatória de noções de educação digital nas escolas públicas e privadas de ensino fundamental e médio.

Registramos a oportunidade da medida em tempos de discussão da criação de uma Base Nacional Comum Curricular, tal como exigida pelo Plano Nacional de Educação. Tendo em vista que o Ministério da Educação apresentou uma primeira versão para debate público, que recebeu contribuições até 15 de março de 2016, a presente Indicação reveste-se da tempestividade necessária. Por isso consideramos que esta sugestão representa importante aporte do Poder Legislativo no processo de atualização da educação fundamental e média brasileira.

Certos de contar com o apoio dos nobres pares, conclamamos pela aprovação deste projeto.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

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

(Decorrente da Constatação item 2.4.2)

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 ou tecnologia similar 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 ou de tecnologia similar 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 ou de tecnologia similar 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 ou de tecnologia similar 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

3.7 – INDICAÇÃO AO TRIBUNAL SUPERIOR ELEITORAL PARA FORMAÇÃO DE FORÇA TAREFA PARA APURAÇÃO CÉLERE DE CRIMES ELEITORAIS PELA INTERNET.

(Decorrente da Constatação item 2.4.2)

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. Presidente do Tribunal Superior Eleitoral sugerindo a formação de força tarefa para apuração célere de crimes eleitorais praticados pela internet.

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 Sr. Presidente do Tribunal Superior Eleitoral, Indicação sugerindo a formação de força tarefa para apuração célere de crimes eleitorais praticados pela internet no próximo pleito eleitoral.

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 formação de força tarefa para apuração célere de crimes eleitorais praticados pela internet.

Excelentíssimo Senhor Presidente do Tribunal Superior Eleitoral:

A internet tem se tornado importante veículo de comunicação social e também de participação popular. A facilidade e a gratuidade do uso das redes sociais, assim como a possibilidade de replicação infinita de conteúdos fazem com que as informações que circulam pela grande rede alcancem vastos contingentes populacionais.

Se no dia a dia dos cidadãos a grande rede é ferramenta de participação social, durante os pleitos eleitorais ela se transforma em verdadeiro espaço de debate e caixa de ressonância dos principais anseios da população. Os fórums formais ou informais, mas principalmente funcionalmente desorganizados e sem nenhum ordenamento preestabelecido, são locais onde a população se reúne para discutir propostas de candidatos ou sugerir e criticar propostas de ações parlamentares.

Apesar desse ambiente colaborativo e que convida à participação e reflexão dos eleitores ser majoritariamente utilizado para o bem, muitos se aproveitam do anonimato e da falta da fronteira física para agredir e

perpetuar as mais variadas formas de ataques pela internet.

Se considerarmos que os pleitos eleitorais são relativamente curtos, um ataque organizado que vise um determinado candidato pode ter efeitos devastadores não só sobre aquela pessoa em particular, mas pode macular todo o processo eleitoral e decidir o futuro de uma região.

Neste contexto e considerando o próximo pleito eleitoral que se avizinha, consideramos de fundamental importância que o egrégio Tribunal tome as devidas providências para mobilizar força tarefa com servidores do Departamento da Polícia Federal, Ministério Publico Eleitoral e Tribunal Regional Eleitoral em cada estado da federação. Somente com a constituição da força tarefa se poderá coibir, de maneira célere crimes eleitorais, oriundos do mau uso da internet, em especial aqueles tratados na Lei Eleitoral (9.504/97), nos artigos 57-A a 57-I.

Certos de contar com a compreensão e o engajamento do Senhor Presidente para a implementação das medidas, temos a convicção de que a criação dessa força tarefa será mais uma garantia da lisura e justeza do processo eleitoral.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

4 – OUTROS

4.1 – OFÍCIOS AOS PODERES EXECUTIVOS DO ESTADO E DO MUNICÍPIO DE SÃO PAULO, ASSIM COMO AO MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO, COM A RECOMENDAÇÃO DE QUE INVESTIGUEM EVENTUAL IRREGULARIDADE NA FALTA DO RECOLHIMENTO DE TRIBUTOS, BEM COMO PRÁTICA, EM TESE, DE CRIME CONTRA A ORDEM TRIBUTÁRIA (LEI Nº 8.137, DE 27 DE DEZEMBRO DE 1990).

(Decorrente da Constatação item 2.1.2)

Ofício nº Brasília, em de de 2016.

À Sua Excelência o Senhor

Fernando Haddad

Prefeito do Município de São Paulo

Assunto: Fiscalização Tributária

Excelentíssimo Senhor Prefeito,

Por ocasião da realização dos trabalhos da Comissão Parlamentar de Inquérito (CPI) destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país, as empresas Facebook Serviços Online do Brasil Ltda., Twitter Brasil Rede de Informação Ltda. e Yahoo! do Brasil Internet Ltda. informaram a esta CPI que não recolhem o Imposto Sobre Serviços de Qualquer Natureza (ISS) em virtude do veto ao subitem 17.07 da lista prevista na Lei Complementar nº 116, de 31 de julho de 2013.

Constatou-se, todavia, que a Prefeitura Municipal informou à empresa Facebook Serviços Online do Brasil Ltda. por meio da Solução de Consulta nº 42/2013 que a mesma está sujeita ao recolhimento do tributo com base em receitas de intermediação de serviços, situação essa que também pode ocorrer em relação às outras duas empresas.

Esta Solução de Consulta não foi mencionada pela empresa a esta CPI, o que pode ter ocorrido com o intuito de ocultar irregularidade na falta do recolhimento do tributo, situação que, em tese, pode caracterizar a prática de crime contra a ordem tributária (Lei nº 8.137, de 27 de dezembro de 1990).

Pelo exposto, esta Comissão Parlamentar de Inquérito aprovou o envio do presente Ofício a fim de que os fatos sejam comunicados a

esta Prefeitura com vistas a que sejam adotadas as providências cabíveis para a realização de procedimento de fiscalização e apuração dos fatos.

No ensejo, informamos que a comunicação dos fatos ora narrados também foi oficiada ao Ministério Público do Estado de São Paulo, o que recomendaria atuação conjunta dos órgãos.

Atenciosamente,

Ofício nº Brasília, em de de 2016.

À Sua Excelência o Senhor

Geraldo Alckmin

Governador do Estado de São Paulo

Assunto: Fiscalização Tributária

Excelentíssimo Senhor Governador,

Por ocasião da realização dos trabalhos da Comissão Parlamentar de Inquérito (CPI) destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país, as empresas Facebook Serviços Online do Brasil Ltda., Twitter Brasil Rede de Informação Ltda. e Yahoo! do Brasil Internet Ltda. informaram a esta CPI que não recolhem o Imposto sobre Circulação de Mercadorias e sobre Serviços de Transporte Interestadual, Intermunicipal e de Comunicações (ICMS).

Em reunião desta CPI realizada em 17 de novembro de 2015 servidor da Administração Tributária do Estado convocado para tanto informou que as atividades das referidas empresas podem se caracterizar como prestação de serviços de comunicação no país, serviços esses que se encontram no campo de incidência do ICMS.

Pelo exposto, esta Comissão Parlamentar de Inquérito aprovou o envio do presente Ofício a fim de que os fatos sejam comunicados ao Governo do Estado de São Paulo com vistas a que sejam adotadas as providências cabíveis para a realização de procedimento de fiscalização e apuração de, em tese, irregularidade na falta do recolhimento do tributo, bem como para a apuração de, em tese, prática de crime contra a ordem tributária (Lei nº 8.137, de 27 de dezembro de 1990).

No ensejo, informamos que a comunicação dos fatos ora narrados também foi oficiada ao Ministério Público do Estado de São Paulo, o que recomendaria atuação conjunta dos órgãos.

Atenciosamente,

Ofício nº Brasília, em de de 2016.

À Sua Excelência o Senhor

Márcio Fernando Elias Rosa

Procurador-Geral do Ministério Público do Estado de São Paulo

Assunto: Investigação

Excelentíssimo Senhor Procurador-Geral,

Por ocasião da realização dos trabalhos da Comissão Parlamentar de Inquérito (CPI) destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país, as empresas Facebook Serviços Online do Brasil Ltda., Twitter Brasil Rede de Informação Ltda. e Yahoo! do Brasil Internet Ltda. informaram a esta CPI que não recolhem o Imposto Sobre Serviços de Qualquer Natureza (ISS) em virtude do veto ao subitem 17.07 da lista prevista na Lei Complementar nº 116, de 31 de julho de 2013 e nem o Imposto sobre Circulação de Mercadorias e sobre Serviços de Transporte Interestadual, Intermunicipal e de Comunicações (ICMS).

Constatou-se, todavia, que a Prefeitura Municipal informou à empresa Facebook Serviços Online do Brasil Ltda. por meio da Solução de Consulta nº 42/2013 que a mesma está sujeita ao recolhimento do tributo com base em receitas de intermediação de serviços, situação essa que também pode ocorrer em relação às outras duas empresas.

Esta Solução de Consulta não foi mencionada pela empresa a esta CPI, o que pode ter ocorrido com o intuito de ocultar irregularidade na falta do recolhimento do tributo, situação que, em tese, pode caracterizar a prática de crime contra a ordem tributária (Lei nº 8.137, de 27 de dezembro de 1990).

Do mesmo modo, em reunião desta CPI realizada em 17 de novembro de 2015 servidor da Administração Tributária do Estado de São Paulo convocado para tanto informou que as atividades das referidas empresas podem se caracterizar como prestação de serviços de comunicação no país, serviços esses que se encontram no campo de incidência do ICMS.

Pelo exposto, esta Comissão Parlamentar de Inquérito aprovou o envio do presente Ofício a fim de que os fatos sejam comunicados ao Ministério Público do Estado de São Paulo com vistas a que sejam adotadas as providências cabíveis para a realização de investigação a fim de apurar se, em tese, houve irregularidade na falta do recolhimento dos citados tributos, bem como prática, em tese, de crime contra a ordem tributária (Lei nº 8.137, de 27 de dezembro de 1990).

No ensejo, informamos que a comunicação dos fatos ora narrados também foi oficiada à Prefeitura do Município de São Paulo e ao Governo do Estado de São Paulo, o que recomendaria atuação conjunta dos órgãos.

Atenciosamente,

4.2 – REQUERIMENTO DE INFORMAÇÕES À SECRETARIA DE COMUNICAÇÃO SOCIAL DA PRESIDÊNCIA DA REPÚBLICA.

(Decorrente da Constatação item 2.1.1)

REQUERIMENTO DE INFORMAÇÕES 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)

Solicita ao Sr. Ministro-Chefe da Secretaria de Comunicação Social da Presidência da República o envio de informações relativos aos gastos com publicidade digital pelo Poder Executivo.

Senhor Presidente:

Requeiro a V. Exa., com base no art. 50, §2º da Constituição Federal, e nos arts. 115 e 116 do Regimento Interno que, ouvida a Mesa, sejam solicitadas ao Sr. Ministro-Chefe da Secretaria de Comunicação Social da Presidência da República o envio de informações relativas aos gastos com publicidade digital pelo Poder Executivo, detalhado por veículo de comunicação.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

JUSTIFICAÇÃO

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 Publicidade, Instituições Financeiras e Comércio Virtual, a cargo do Sub-Relator Deputado Sandro Alex.

De maneira concomitante ao andamento das investigações conduzidas pelo Sub-Relator afeito à área de publicidade, Deputado Sandro Alex, a Polícia Federal deflagrou a operação Barba Negra que resultou no fechamento de sítio de internet que oferecia ilegalmente filmes e outros conteúdos audiovisuais. A denúncia apresentada nesta CPI pelo Deputado Sandro Alex, desencadeou, também, mudanças nos procedimentos de alocação de publicidade governamental na internet. Conforme se evidenciou na audiência pública realizada, no dia 08/10/2015, com o Ministro Edinho Silva, da Secretaria de Comunicação Social da Presidência da República, propagandas de empresas tradicionais e até do governo estavam sendo veiculadas em sítios utilizados para a prática de crimes cibernéticos, tais como o *streaming* ilegal de filmes e de séries de televisão. Na ocasião o Ministro declarou que encaminharia à Comissão “todo o ranqueamento [isto é, investimento em publicidade], assim como o ranqueamento das redes sociais para que a Comissão tenha todas as informações necessárias sobre o que é investido em publicidade, por meio da SECOM”. Ressaltamos que essas informações não foram encaminhadas até o encerramento dos trabalhos da CPI.

Em face ao exposto, solicitamos a aprovação do Requerimento.

Sala das Sessões, em de de 2016.

CPI – Crimes Cibernéticos

5 – RECOMENDAÇÕES E ENCAMINHAMENTOS DA COMISSÃO

Tendo em vista os fatos apurados nesta Comissão Parlamentar de Inquérito, decide-se pela realização dos seguintes encaminhamentos e recomendações:

a) Encaminhe-se à mesa da Câmara dos Deputados, para adotar as providências de alçada desta ou do Plenário, para implementar matéria legislativa referente aos projetos de lei apresentados por esta Comissão;

b) Encaminhe-se ofício aos Relatores e aos Presidentes das Comissões em que tramitam os Projetos de Lei nº 1776/2015 (de autoria do Deputado Paulo Freire), 3237/2015 (de autoria do Deputado Vinícius Carvalho), 5555/2013 (de autoria do Deputado João Arruda), 3686/2015 (de autoria do Deputado Ronaldo Carletto), 7544/2014 (de autoria do Deputado Ricardo Izar), 1755/2015 (de autoria do Deputado Raul Jungmann), 6726/2010 (de autoria do Deputado Arnaldo Faria de Sá), 2315/15 (de autoria do Dep. Enio Verri), 2801/2015 (de autoria do Dep. JHC) e PL 5074/2016 (de autoria do Senador Otto Alencar), indicando que esta CPI reconheceu a importância em se debater as matérias neles tratadas;

c) Encaminhe-se ao Poder Executivo e ao Poder Judiciário, para análise das Indicações e Requerimento anexados;

d) Encaminhe-se aos Poderes Executivos do Estado e do Município de São Paulo, assim como ao Ministério Público do Estado de São Paulo, com a recomendação de que investiguem eventual irregularidade na falta do recolhimento de tributos, bem como prática, em tese, de crime contra a ordem tributária, nos termos dos ofícios anexados;

e) Encaminhe-se ao Ministério Público Federal, com a

recomendação de que avalie a pertinência de: I) realizar-se um Termo de Cooperação com o Poder Executivo, operadoras de telefonia e principais provedores de acesso à internet e de aplicações de computador e de internet, no sentido de promover ações educativas continuadas, nas escolas, para o uso seguro da internet por crianças e adolescentes, reforçando e ampliando o programa de educação já em desenvolvimento a que se refere a Portaria nº 735/15, daquele órgão; II) realizar-se um Termo Cooperação com o Poder Executivo, operadoras de telefonia, principais provedores de acesso à internet e de aplicações de computador e de internet, no sentido de promover ações educativas continuadas para o uso seguro da internet por adultos; III) realizar-se um Termo de Ajustamento de Conduta com as entidades envolvidas com a publicidade no meio digital, para evitar a comercialização de espaço para anúncios publicitários em plataformas digitais que disponibilizem conteúdos ilícitos, pratiquem condutas ilegais e/ou fomentem a prática de tais condutas pelos seus usuários;

f) Encaminhe-se à Comissão de Educação da Câmara dos Deputados, com a sugestão de que crie uma Subcomissão Especial para tratar do tema relativo à inclusão de noções de educação digital nas escolas;

g) Encaminhe-se à Comissão de Segurança Pública e Combate ao Crime Organizado da Câmara dos Deputados, com a sugestão de que crie uma Subcomissão Especial para tratar do tema relativo à segurança nas Olimpíadas de 2016;

h) Encaminhe-se à Comissão de Meio Ambiente e Desenvolvimento Sustentável, com a sugestão de que crie uma Subcomissão Especial para tratar do tema relativo à introdução de códigos maliciosos pelas montadoras de veículos para burlar a legislação ambiental;

i) Encaminhe-se à Comissão de Ciência, Tecnologia,

Comunicações e Informática, com a sugestão de que crie Subcomissão para tratar do tema dos crimes cibernéticos;

j) Encaminhe-se ao Cedes - Centro de Estudos e Debates Estratégicos – Ofício ao Centro de Estudos e Debates Estratégicos para que desenvolva estudo sobre o impacto e a necessidade de regulação na questão do *bigdata*.

Sala da Comissão, em 04 de maio de 2016.

Deputado ESPERIDIÃO AMIN
Relator

Deputada MARIANA CARVALHO
Presidente

CÂMARA DOS DEPUTADOS

CPI – CRIMES CIBERNÉTICOS

COMISSÃO PARLAMENTAR DE INQUÉRITO DESTINADA A INVESTIGAR A PRÁTICA DE CRIMES CIBERNÉTICOS E SEUS EFEITOS DELETÉRIOS PERANTE A ECONOMIA E A SOCIEDADE NESTE PAÍS.

REFORMULAÇÃO DO RELATÓRIO FINAL

(ITEM 1.2, PARTE III)

Presidente: Deputada Mariana Carvalho

Relator: Deputado Esperidião Amin

Sub-Relatores: Deputados Sandro Alex, Rafael Motta,

Daniel Coelho e Rodrigo Martins

Brasília, _____ de _____

REFORMULAÇÃO DO RELATÓRIO FINAL
(ITEM 1.2, PARTE III)

Durante a votação do Relatório Final no dia 04/05/2016, foi apresentado Destaque Supressivo nº 14 pelo Deputado Nelson Marchezan Júnior, requerendo a supressão da expressão “expondo os dados informatizados a risco de divulgação ou de utilização indevidas”, do Projeto de Lei constante do item 1.2 da Parte III do Relatório Final. Após discussão e votação o Destaque foi aprovado.

Portanto, reformulamos a redação apresentada ao referido Projeto constante do Relatório Final, com a alteração resultante da aprovação do Destaque pelo Plenário desta Comissão, conforme anexo.

Sala da Comissão, em 04 de maio de 2016.

Deputado ESPERIDIÃO AMIN
Relator

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 três meses a um ano, 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 - obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, arquivos, senhas, informações ou outros documentos ou dados privados;

III - controle remoto não autorizado do dispositivo acessado:

Pena – detenção, de seis meses a dois 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 um a quatro anos, e multa.

§ 4º 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 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.

Ressalte-se que a conduta continua a ser punida apenas em sua forma dolosa, ou seja, quando há a intenção de acessar sistema informatizado contra a vontade de quem de direito. A modalidade culposa apenas pode ser punida quando há expressa previsão legal (art. 18, inciso II, parágrafo único, do Código Penal), o que não é o caso do tipo penal em questão.

O que se propõe é, apenas, que não se exija um dolo específico para a configuração do delito (ou seja, a finalidade específica de "obter, adulterar ou destruir dados ou informações" ou de "obter vantagem ilícita", como consta da atual redação). Isso porque o acesso indevido, independentemente da finalidade, já viola os direitos relacionados à intimidade e à privacidade da vítima. Ademais, conforme aponta a doutrina, "*com essa previsão de elemento subjetivo específico, percebe-se que o tipo penal fez uma restrição temerária ao horizonte de abrangência da norma. É possível que nessas invasões despretensiosas (em que a satisfação da conduta restringe-se a conseguir violar a segurança de determinado sistema computacional, mesmo sem a intenção de obter, adulterar ou destruir dados), o primeiro autor deixe aberta as portas para que um segundo criminoso, sem qualquer ajuste entre os dois, agora com a intenção de obter informações, por exemplo, atue livremente, chegando ao extremo de nem mesmo responder pelo crime, já que ele não violou indevidamente a segurança, pois esta já estava violada*"[38].

Com este Projeto, busca-se suprimir do tipo, também, a necessidade de que haja a violação de mecanismo de segurança. Afinal, repita-se, o acesso indevido, por si só, já viola os direitos relacionados à intimidade e à privacidade da vítima. Faz-se um paralelo com o crime de invasão de domicílio,

[38] BRITO, Auriney. Direito penal informático. São Paulo: Saraiva, 2013, p. 71.

que não exige, para a sua configuração, que a porta da residência esteja trancada.

Aponte-se por fim, que não se está alterando a ação penal relacionada ao tipo, que continua sendo condicionada à representação, a não ser em casos específicos como contra a Administração. Dessa forma, invasões em que a vítima não vislumbrar a necessidade de dar início a investigação criminal, isso não ocorrerá.

Sala das Sessões, em 04 de maio de 2016.

CPI – Crimes Cibernéticos

Relator