CPI DA ESPIONAGEM

RELATÓRIO FINAL

Comissão Parlamentar de Inquérito destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar emails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal

Parte I – CPI DA ESPIONAGEM

I. 1. Apresentação

O Poder Legislativo exerce funções legislativas, fiscalizadoras, administrativas e jurisdicionais. Há preponderância, porém, pelas atividades legiferante e de fiscalização. Essa circunstância é explicável à vista da clássica divisão dos poderes estatais.

Uma comissão parlamentar de inquérito insere-se no âmbito da atribuição fiscalizadora. Nesse campo, o Poder Legislativo tem importante papel tanto de investigação quanto de controle dos atos do poder público. Para isso, importa recordar que "são pelo menos quatro os meios constitucionais de que dispõe o Parlamento para exercer as atribuições de fiscalização: interpelação parlamentar; pedido de informações; inspeções e auditorias realizadas por meio do Tribunal de Contas da União (TCU); e o inquérito parlamentar".[1]

O inquérito legislativo tem em vista assunto específico, como exige o texto constitucional: "apuração de fato determinado" [art. 58, § 3°, da Constituição Federal (CF)]. Para além disso, os temas a serem investigados devem estar, de tal ou qual modo, inseridos no âmbito de atribuições do poder público doméstico.

---

[1] SANTI, Marcos Evandro Cardoso. *Criação de comissões parlamentares de inquérito*: tensão entre o direito constitucional de minorias e os interesses políticos da maioria. Porto Alegre: Sergio Antonio Fabris Ed., 2007. p. 29

Nesse sentido, a competência fiscalizadora do Congresso Nacional é extensa e abrangente, alcançando todos os limites da sua competência legislativa. Vale dizer: o Congresso Nacional tem poder de fiscalizar todos os assuntos e temas a respeito dos quais está capacitado, pela Constituição, para legislar.

As comissões parlamentares de inquérito (CPIs) constituem, assim, um dos mais importantes instrumentos de que o Congresso Nacional dispõe para exercer sua competência constitucional. Não por acaso, é perceptível que o funcionamento de uma CPI (ao lado do manejo do instituto da medida provisória e do controle de constitucionalidade das leis) traduz uma das pedras de toque do modelo brasileiro de repartição funcional dos Poderes entre o Executivo, o Legislativo e o Judiciário.

A presente comissão parlamentar de inquérito, que versa sobre esquema de espionagem empreendido por órgãos de governo estrangeiro, expressa movimento político na história recente do Brasil, e resulta de entendimento entre lideranças políticas do Senado no sentido de investigar com isenção fatos que, inequivocamente, atingiram a soberania do Brasil.

I. 2. Papel fiscalizador do Congresso Nacional

Antes de passarmos à análise dos fatos investigados ao longo dos últimos meses, convém apreciar, para mais exata compreensão do leitor, a natureza do meio utilizado para a realização das investigações, bem como de sua importância.

O Congresso, como instituição, não pode se separar de sua vocação histórica para se configurar em espécie de caixa de ressonância da

sociedade na qual está inserido. Os fundadores das formas modernas do Estado, ao divisarem a separação de poderes, tiveram consciência das características de cada um desses poderes. Notadamente ao Poder Legislativo, além da capacidade de produção de leis, foi reconhecida sua importância para a fiscalização dos atos dos governantes, bem como para a preservação dos direitos das minorias.

Na origem do parlamento moderno, já se reconhece a preocupação com o abuso do direito dos monarcas, de um lado, e, de outro, com o risco apresentado pela tirania da maioria. Os excessos apresentados durante o período que antecedeu a revolução gloriosa foram essenciais para a configuração do moderno sistema parlamentar.

Também, a radicalização dos ímpetos revolucionários ocorridos na França nos anos que se seguiram a 1789, que culminaram na supressão física de toda uma geração de homens públicos e na ascensão de uma nova autocracia, serviu para iluminar as gerações futuras dos perigos da excessiva valorização do Executivo em detrimento das minorias representadas no parlamento.

O imenso custo, em vidas humanas, recursos e energia que a história da democracia vem apresentando não deve servir de argumento para aqueles que, em todos os momentos, buscam substituir a democracia por outro regime. Esses buscam destruir o regime democrático, atacando suas instituições, por meio de argumentos que, sob a capa da moralidade, não escondem a nostalgia do cesarismo, o desejo de substituir a vontade popular pela vontade de um indivíduo ou grupo de indivíduos.

Essa forma de proceder não deixa de conhecer seu sucesso, para eventuais despreparados ou ansiosos, a lentidão do processo

democrático pode ser facilmente confundida com vacilação; o entrechoque de opiniões pode se assemelhar a indecisão; o reconhecimento da existência de nuances, com fraqueza das convicções.

Na sociedade democrática, a existência e o fortalecimento das instituições depende, muitas vezes, do exercício das possibilidades oferecidas pelos acontecimentos históricos, por mais negativos que possam parecer. Esse é o traço principal e qualidade mais destacada da democracia, seu permanente aperfeiçoamento.

A atividade parlamentar é caracterizada pela representatividade (em princípio, todos os extratos da sociedade se refletem no parlamento), pela colegialidade (existência de um órgão coletivo que, contém, em si, setores de situação e oposição) e pela continuidade (permanência dos órgãos legislativos ao longo do tempo). Tais características tornam o Congresso organismo adequado para a operação de uma das múltiplas instâncias de fiscalização que, em uma democracia, ajudam a compor o sistema de freios e contrapesos destinado a evitar a tirania e o desvirtuamento das instituições.

Notavelmente, ao longo do século XX, a função de controle por meio do Parlamento adquiriu cada vez maior relevo, assumindo, em alguns momentos, primazia em relação à produção normativa.

A demanda social por ordenamento jurídico estável, somada à proliferação de fontes do direito – decorrente da criação de novas instâncias técnicas dotadas de relativa capacidade de produzir normas, tais como as agências reguladoras – produziram uma redução relativa da capacidade legiferante dos Parlamentos em todo o mundo. Efetivamente, da totalidade das normas em vigência nas sociedades modernas, apenas uma fração

seguiu os trâmites parlamentares tradicionais.

Mesmo que mantenham o monopólio da produção de normas hierarquicamente superiores, os parlamentos de todo o mundo não são responsáveis pela maioria das normas que afetam a sociedade. Principalmente em matérias tidas como de natureza técnica, o grosso da produção normativa está concentrada em órgãos do Executivo, sendo apenas indiretamente derivados de atos parlamentares.

Em decorrência, a fiscalização dos atos administrativos assume importância fundamental para a manutenção da ordem jurídica e das liberdades públicas. Em universo normativo em constante expansão, os atos do Executivo devem ser cuidadosamente analisados, sob pena de florescerem abuso e arbítrio.

A atividade de controle parlamentar não é, propriamente, uma inovação dos dias de hoje. Montesquieu já admitia que aos parlamentos caberia fiscalizar o cumprimento das normas por eles criadas. A execução orçamentária, por exemplo, sempre foi tema cuja fiscalização parlamentar era admitida.

Houve, no entanto, alteração substancial quanto à natureza do poder de investigação dos parlamentos, a passagem de um poder implícito de investigação, baseado na capacidade do Legislativo de buscar a implementação dos atos dele provenientes para uma faculdade explicitamente reconhecida de perquirição acerca de atos cuja competência originária não seria, em princípio, do Congresso, tais como os atos de administração, quer do Executivo, quer do Judiciário.

As alterações no padrão tradicional de divisão dos poderes,

com maior ingerência do Executivo, tornam imperativa, portanto, maior participação do Legislativo no controle dos atos dos governantes e de seus órgãos auxiliares. Representantes do conjunto da sociedade e guardiões das aspirações últimas dos povos, os parlamentos devem se adaptar a essa nova realidade e desenvolver métodos para desempenhar essa função.

I. 3. Natureza e objetivos da comissão parlamentar de inquérito

É preciso deixar claro, de início, aquilo que a sociedade brasileira pode esperar de uma comissão parlamentar de inquérito. Isso porque, como ocorre com qualquer instituição do Estado, no regime democrático, os poderes das CPI não são ilimitados.

Percebe-se inclinação dos formadores de opinião por medir o êxito de uma CPI pela quantidade de autoridades, agentes políticos e cidadãos que, em função dela, venham a ser punidos. Isso, não obstante, parece-nos equivocado. Portanto, para evitar especulações, os objetivos de uma CPI devem ser definidos de maneira precisa, até para que não se estimulem ilusões, e não se pretenda alcançar objetivos que não lhe dizem respeito.

Em tese, pode-se esperar de uma CPI:

a) que contribua para a transparência da administração pública, na medida em que revela, para a população, fatos e circunstâncias que, de outra forma, não seriam do conhecimento público;

b) que, na qualidade de órgão do Poder Legislativo, possibilite

o exame crítico da legislação aplicável ao caso sob investigação, para, a partir desse exame, eventualmente sugerir medidas saneadoras e proposições visando ao seu aprimoramento.

c) que proponha à respectiva Casa do Congresso Nacional, sempre que cabível, a abertura de processo contra parlamentar quando seu nome estiver vinculado a fatos ou atos que possam implicar prejuízo à imagem do parlamento e sempre que se possa identificar possível quebra do decoro parlamentar;

d) que, ao fim, aponte ao Ministério Público, caso identifique, fatos que possam caracterizar delitos ou prejuízo à administração pública, para que aquele órgão promova a responsabilidade civil e penal correspondente.

A CPI da Espionagem, pela sua natureza singular, terá como principal objetivo identificar falhas nos sistemas de inteligência e contrainteligência e de proteção de dados que trafegam pela internet, e eventualmente fazer proposições para o seu aprimoramento.

Como se verá no decorrer da leitura deste relatório, não foi possível confirmar a materialidade de crime, de modo que as investigações, sob essa ótica, restaram inconclusas. Não obstante, a CPI foi de fundamental importância para fazer uma primeira avaliação dos sistemas brasileiros de inteligência e de segurança das comunicações. A partir do diagnóstico feito, os atores envolvidos poderão oferecer sugestões para o aprimoramento desses sistemas.

I. 4. Histórico dos fatos

A série de denúncias que motivou a criação desta CPI começou em maio de 2013, quando foram publicados os primeiros documentos secretos vazados pelo especialista em computação Edward Snowden, que trabalhou para empresas ligadas à Agência de Segurança Nacional dos Estados Unidos, [*National Security Agency* (NSA)] e à Central de Inteligência Americana [*Central Intelligence Agency* (CIA)].

Snowden teve acesso às informações divulgadas quando prestava serviços terceirizados para a Agência de Segurança Nacional no Havaí. Ao procurar a imprensa e entregar parte dos dados que possuía, Snowden deixou o estado do Havaí e foi, de início, para Hong Kong, em 20 de maio, antes de as primeiras reportagens virem a público. Em junho, os Estados Unidos da America (EUA) pressionaram as autoridades chinesas responsáveis para responder ao pedido de extradição do referido senhor, que foi formulado com base em tratado para esse fim em vigor desde 1998.

Em 23 de junho, Snowden deixou Hong Kong e partiu rumo a Moscou, na Rússia. A viagem foi feita com apoio do WikiLeaks, de Julian Assange, que enviou militante para ajudar o ex-técnico da CIA. O americano ficou na área de trânsito do aeroporto de Sheremetyevo por quarenta dias, em verdadeiro "limbo" jurídico, já que não tinha documentos para entrar em território russo – seu passaporte havia sido cancelado pelos Estados Unidos da América.

Snowden enviou pedido de asilo para 21 países, entre eles Brasil, Cuba, Venezuela, Bolívia, Nicarágua, China, Rússia, Alemanha e França, segundo o WikiLeaks. Três desses países se dispuseram a abrigá-lo – Venezuela, Bolívia e Nicarágua.

No dia 16 de julho, Snowden pediu oficialmente asilo temporário à Rússia. Em 1º de agosto, ele recebeu os documentos necessários e deixou a área de trânsito do aeroporto rumo a "local seguro" em território russo.

Contrariada, a Casa Branca desmarcou encontro de cúpula entre os presidentes Obama e Putin previsto para setembro.

I. 5. Notícias que deram ensejo à instauração da CPI

Documentos repassados por Snowden ao advogado e colunista Glenn Greenwald, do jornal britânico *The Guardian,* revelaram que os EUA vinham há tempos espionando seus próprios cidadãos e que o esquema de vigilância cibernética também se estendia à Europa e à China.

Em julho do ano passado, novos documentos apontaram o Brasil como um dos alvos preferenciais do serviço de inteligência norte-americano. Brasília teria inclusive sediado, pelo menos até 2002, uma das 16 bases de espionagem da NSA ao redor do mundo. A embaixada do Brasil em Washington e a missão do Brasil na Organização das Nações Unidas (ONU) estariam entre os espionados.

Novas denúncias, também em julho de 2013, indicaram que o esquema de vigilância dos EUA havia se espalhado pela América Latina. Logo em seguida, revelações sobre o alcance dos programas Prism e XKeyscore, usados para a espionagem, jogaram por terra a justificativa oficial de que a vigilância seria restrita aos chamados metadados, colhidos apenas nos pontos de troca do tráfego de informação, ou seja, nas conexões de redes de dados nacionais com as denominadas supervias da internet. O

serviço secreto norte-americano teria, na verdade, amplo acesso aos conteúdos das comunicações telefônicas e digitais, dentro e fora do território americano.

Novas revelações, cada vez mais graves, foram feitas aos poucos. Os Estados Unidos teriam espionado ao menos oito países – entre eles o Brasil – para aprovar sanções contra o Irã, no Conselho de Segurança da ONU, em 2010. Também teriam espionado os planos de participantes da 5ª Cúpula das Américas, em 2009, e pago 100 milhões de libras ao centro de escutas britânico [*Government Communications Headquarters* (GCHQ)] nos últimos três anos, para trabalho conjunto de espionagem digital. Parceria semelhante teria sido firmada com a agência de inteligência alemã [*Bundesnachrichtendienst* (BND)].

Três semanas após a divulgação dos primeiros dados, a revista alemã *Der Spiegel* publicou reportagem afirmando que a União Europeia era um dos "objetivos" da Agência Nacional de Segurança (NSA). A publicação sustentou as acusações com documentos confidenciais a que teve acesso graças às revelações do ex-funcionário americano.

Em um dos documentos, de setembro de 2010 e considerado "estritamente confidencial", a NSA descreve como espionou a representação diplomática da UE em Washington, usando microfones instalados no edifício e entrando na rede de informática, o que permitia a leitura de e-mails e de documentos internos.

A Agência chegou a ampliar suas operações até Bruxelas. "Há mais de cinco anos", afirma a *Der Spiegel*, os especialistas em segurança da UE descobriram um sistema de escuta na rede telefônica e de internet do

edifício Justus-Lipsius, sede principal do Conselho da UE, que alcançava até o quartel-general da Organização do Tratado do Atlântico Norte (OTAN), na região da capital belga.

Ao longo do mês de outubro, novas revelações sobre espionagens feitas pelos EUA (e também pelo Reino Unido) contra chefes de Estado europeus vieram à tona. Alemanha, Itália, e França tiveram seus presidentes e chanceleres espionados, segundo documentos revelados pelas imprensas locais. Os países pediram satisfações aos EUA e convocaram os embaixadores americanos em seus territórios para maiores esclarecimentos.

Líderes da União Europeia divulgaram comunicado no dia 25 de outubro de 2013 dizendo que a desconfiança sobre o esquema de espionagem dos Estados Unidos poderia prejudicar os esforços mundiais no combate ao terrorismo. A declaração foi dada após o jornal *The Guardian* revelar que 35 líderes mundiais tiveram conversas telefônicas monitoradas, inclusive a chanceler alemã, Angela Merkel, e o presidente francês, François Hollande.

No dia 28 de outubro de 2013, o jornal espanhol *El Mundo* revelou que mais de 60 milhões de ligações na Espanha foram monitoradas em um período de trinta dias. O governo espanhol convocou o embaixador dos EUA no país para dar explicações.

No dia 30, uma publicação italiana revelou que o Vaticano e o Papa Francisco também teriam sido monitorados, inclusive durante o conclave que elegeu o Papa. Os EUA negaram as acusações.

Até a China passou a cobrar explicações do governo estadunidense, após a imprensa australiana revelar que os EUA usavam

suas representações diplomáticas em território chinês para coletar dados sobre o país. A Indonésia também teria sido espionada por meio de embaixadas australianas.

I. 6. Brasil como alvo da espionagem

Reportagens do jornal *O Globo* publicadas a partir de 6 de julho de 2013, com dados coletados por Snowden, mostraram que milhões de e-mails e ligações de brasileiros e estrangeiros em trânsito no país foram monitorados. Ainda segundo os documentos, uma estação de espionagem da NSA funcionou em Brasília pelo menos até 2002. Os dados apontam ainda que a embaixada do Brasil em Washington e a representação do país junto à ONU, em Nova York, também podem ter sido monitoradas.

A revista *Época* também publicou reportagem sobre documento secreto que revela como os Estados Unidos espionaram ao menos oito países – entre eles o Brasil – para aprovar sanções contra o Irã.

Reportagem do programa *Fantástico*, da *TV Globo*, veiculada no dia 1° de setembro de 2013, mostrou que o esquema de espionagem norte-americano não teria poupado nem mesmo a presidente Dilma Rousseff. Ligações telefônicas e mensagens eletrônicas entre a presidente e seus assessores diretos teriam sido monitoradas. Conversas entre esses assessores e entre eles e terceiros também teriam estado na mira do serviço secreto dos Estados Unidos.

Notícias veiculadas nas semanas subsequentes demonstram que Petrobras e Ministério das Minas e Energia também foram alvo de espionagem.

Segundo revelou o programa *Fantástico*, a NSA, em um plano de treinamento de agentes, fez uma apresentação que recebeu a classificação "ultrassecreta" e que foi elaborada em maio de 2012, para instruir procedimentos de espionagem de redes privadas de computador – redes internas de empresas, governos e instituições financeiras e que existem, justamente, para proteger informações. O nome da Petrobras, a maior empresa do Brasil, aparece logo no início do documento mostrado pelo *Fantástico*, com o título "Muitos alvos usam redes privadas".

No caso do Ministério das Minas e Energia, a espionagem teria sido feita pela Agência Canadense de Segurança em Comunicação [*Communications Security Establishment Canada* (CSEC)], De acordo com apresentação obtida com exclusividade pelo programa *Fantástico*, o Ministério teria sido alvo de espionagem, cujo objetivo seria a rede de comunicações da pasta – telefonemas, e-mails e uso da internet.

Segundo a matéria, a apresentação canadense foi exibida em junho de 2012 em conferência que reuniu analistas ligados a agências de espionagem de cinco países, do grupo conhecido como *Five Eyes* (Cinco Olhos, em português): Estados Unidos, Inglaterra, Canadá, Austrália e Nova Zelândia.

Não há indicação de que o conteúdo das comunicações tenha sido acessado. Aparentemente, foram captados os metadados, que indicam quem falou com quem, quando, onde e como. A mesma apresentação, no entanto, sugere ao fim que seja realizada também uma espionagem conhecida como *man on the side* ("homem ao lado"), em que toda informação pode ser copiada nos momentos em que entra e sai da rede (não em trânsito).

I. 7. Apresentação do requerimento para instauração da CPI

Após a revelação de que o Brasil é um dos principais alvos da rede de espionagem global montada pelo serviço de inteligência norte-americano e de que milhões de brasileiros e estrangeiros residentes ou em trânsito no País, além de instituições e empresas sediadas no Brasil tiveram sua privacidade digital violada, fez-se imprescindível investigar não apenas o alcance das denúncias, mas também as fragilidades do sistema de telecomunicações brasileiro e do nosso sistema de inteligência e defesa cibernética.

Diante desse quadro, foi apresentado e aprovado o Requerimento nº 811, de julho de 2013-SF, de autoria da Senadora Vanessa Grazziotin (PCdoB/AM) e outros Senadores, para criação da presente comissão parlamentar de inquérito (CPI), para, no prazo de cento e oitenta dias, investigar "a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal".

I. 8. Instalação da CPI

Em 3 de setembro de 2013, foi realizada a 1ª reunião (instalação) da Comissão, oportunidade em que foram eleitos Presidente, Senadora Vanessa Grazziotin, e Vice-Presidente, Senador Pedro Taques, e designado o Relator, Senador Ricardo Ferraço.

I. 9. Composição

A Comissão Parlamentar de Inquérito foi composta por onze titulares e sete suplentes, devidamente indicados pelas respectivas lideranças partidárias. O quadro abaixo indica a atual composição da CPI, sendo, logo a seguir, detalhadas as mudanças ocorridas durante o período de sua existência.

Cargo	Senador
Presidente	**Vanessa Grazziotin**
Vice-Presidente	**Pedro Taques**
Relator	**Ricardo Ferraço**
Membros Titulares	Roberto Requião (PMDB-PR)
	Ricardo Ferraço (PMDB-ES)
	Benedito de Lira (PP-AL)
	Sérgio Petecão (PSD-AC)
	Vanessa Grazziotin (PC do B-AM)
	Walter Pinheiro (PT-BA)
	Anibal Diniz (PT-AC)

	Pedro Taques (PDT - MT)
	Eduardo Amorim (PSC-SE)
Membros Suplentes	Eunício Oliveira (PMDB-CE)
	Eduardo Suplicy (PT - SP)
	Lídice da Mata (PSB - BA)
	Antonio Carlos Rodrigues (PR - SP)

I. 10. Atividades realizadas

A CPI da Espionagem apreciou e aprovou 72 dos 74 requerimentos apresentados pelos seus membros. Entre os aprovados estão requerimentos de convite ou convocação e requerimentos de pedido de informações. Os requerimentos de informações dirigidos a órgãos governamentais e também a órgãos não governamentais foram atendidos, sendo que quase todos os documentos foram digitalizados pela Secretaria da CPI e disponibilizados para o conjunto das assessorias dos membros da CPI.

De um total de doze reuniões ocorridas na CPI, oito foram destinadas à realização de audiências públicas para colher o depoimento de especialistas, de servidores públicos e de jornalistas. Outras quatro reuniões foram administrativas.

Parte II – ESPIONAGEM E DIREITO INTERNACIONAL

II. 1. Considerações iniciais

Verifica-se, nos dias de hoje, crescente internacionalização dos interesses nacionais. A superlativa interdependência entre os povos é, nos tempos de agora, um fato. Ignorar o que se passa no planeta é, portanto, opção arriscada. A matéria é, por certo, um dos desdobramentos da crescente interdependência dos países em época de avanço tecnológico sem precedentes na história da humanidade, bem como em momento de incrível velocidade nas trocas de comunicações em escala global. A essas circunstâncias alguns autores apuseram a etiqueta "globalização". Cuida-se, com efeito, de nova dimensão no relacionamento interestatal.

Nessa ordem de ideias, é apropriado partir de estudo contextualizado da palavra "globalização" para compreensão mais exata dos fatos que motivaram esta CPI. Isso se dá tendo em vista que o termo adquiriu ares de unanimidade, não necessariamente quanto ao seu exato conteúdo, mas no tocante à sua utilização para explicar fenômenos que transcendem o espaço territorial de um Estado. Esses episódios têm impacto direto nas transformações à medida que aceleram a velocidade das mudanças verificadas no direito internacional das últimas décadas.

A "ideia" de globalização permeia a vida contemporânea em todos os domínios à vista, sobretudo, de sua natureza plurívoca. Como destacado em relatório do Banco Mundial, a "Globalização (...) é um

processo que afeta muitos aspectos das nossas vidas. Os ataques terroristas aos Estados Unidos em 11 de setembro de 2001 foram um aspecto da globalização. O rápido crescimento e a redução da pobreza na China, na Índia e em outros países que eram pobres 20 anos atrás é outro. O desenvolvimento da Internet, a comunicação e o transporte mais fáceis em todo o mundo são um terceiro aspecto. A disseminação da AIDS é parte da globalização, da mesma forma que o acelerado desenvolvimento de tecnologias que aumentam a expectativa de vida das pessoas"[2].

O rol indicado pelo Banco, embora passível de críticas, exemplifica a dimensão do fenômeno, que atinge de maneira contundente formas de atuação dos Estados nacionais no campo da espionagem.

De início, o termo buscava caracterizar nova fase da economia mundial. Com o tempo, invadiu outros domínios — político, social, ambiental, cultural. Cuida-se do vocábulo da moda. Parece, pois, acertada a observação de Bauman no sentido de que "todas as palavras da moda tendem a um mesmo destino: quanto mais experiências pretendem explicar, mais opacas se tornam"[3]. Reside, provavelmente, nessa opacidade o caráter perene que o vocábulo adquiriu em vários contextos.

Uma primeira definição do fenômeno indica que ele compreende o conjunto de trocas econômicas entre diferentes partes do globo. O espaço mundial torna-se, assim, o lugar das transações entre os diferentes povos. Desse modo, parece certo dizer que o processo verificado

---

[2] GLOBALIZAÇÃO, crescimento e pobreza: a visão do Banco Mundial sobre os efeitos da globalização. São Paulo: Futura, 2003. p. 9

[3] BAUMAN, Zygmunt. Globalização: as consequências humanas. Rio de Janeiro: Jorge Zahar, 1999. p. 7.

na atualidade sucede outras globalizações: as grandes descobertas ibéricas, a colonização europeia, a revolução industrial britânica. O assunto está, portanto, ligado ao estado das técnicas e ao seu impacto sobre a acessibilidade ao espaço físico. A revolução nos meios de comunicação e a velocidade no fluxo de informações incorporaram ao termo novas perspectivas[4]. Vale acrescentar, ainda, que as percepções vinculadas aos limites físicos da Terra são alteradas.

Já se definiu o fenômeno na linha da ampliação do relacionamento social em dimensão planetária de modo que eventos ocorridos a muitos quilômetros de distância têm impacto sobre acontecimentos locais e vice-versa. Verifica-se, assim, a "morte" da localização geográfica.

Pode-se considerar, em síntese, que isso acontece no plano econômico, graças, sobretudo, aos seguintes fatores: 1) terceira revolução tecnológica (vinculada a busca, processamento, difusão e transmissão de informações; inteligência artificial; engenharia genética); 2) formação de áreas de livre comércio (União Européia, Mercado Comum do Sul, Área de Livre Comércio da América do Norte); e 3) interligação e interdependência dos mercados físicos e financeiros em escala planetária.

---

[4] GIDDENS, por exemplo, recorda que "Nos Estados Unidos, o rádio levou quarenta anos para atingir os cinquenta milhões de ouvintes. O mesmo número de pessoas usava o computador pessoal, apenas quinze anos depois de a máquina ter sido inventada. Só foram precisos uns meros quatro anos, para haver cinqüenta milhões de americanos que usam a Internet com regularidade" (GIDDENS, Anthony. O mundo na era da globalização. Lisboa: Presença, 2000. p. 23).

Importante destacar que, na esfera política, a derrocada do único grande sistema que concorria com o capitalismo liberal em âmbito mundial contribuiu, por igual, para a aceleração do processo. O desaparecimento da bipolaridade levou Fukuyama a propor o "fim da história", com a consagração do modelo neoliberal[5]. Para ele não haveria mais alternativas ao capitalismo e à democracia liberal.

Lafer, por sua vez, ao comentar os acontecimentos do romper dos anos 1990, pondera que "a vida internacional deixou de ter como elemento estruturador as polaridades definidas das relações Leste/Oeste; Norte/Sul. Passou a caracterizar-se por polaridades indefinidas, sujeitas às "forças profundas" de duas lógicas que operam numa dialética contraditória de mútua complementaridade: a lógica da globalização (das finanças, da economia, da informação, dos valores etc.) e a lógica da fragmentação (das identidades, da secessão dos Estados, dos fundamentalismos, da exclusão social etc.)"[6]. As "forças profundas" produzem globalização desigual, permeada de promessas não cumpridas de vantagens iguais para todos[7].

Nessa ordem de ideias, Ricupero convida nossa atenção para alguns mitos que se criaram em torno do conceito[8]. O primeiro deles aponta para o sonho de modelo único: democracia representativa e economia de

---

[5] FUKUYAMA, Francis. *The end of history and the last man*. New York: Avon Books, 1998.

[6] LAFER, Celso. A identidade internacional do Brasil e a política externa brasileira: passado, presente e futuro. São Paulo: Perspectiva, 2001, p. 109.

[7] STIGLITZ, Joseph. A globalização e seus malefícios: a promessa não cumprida de benefícios globais. São Paulo: Futura, 2002. Ver, ainda, SANTOS, Milton. Por uma outra globalização: do pensamento único à consciência universal. 5. ed. São Paulo: Record, 2004.

[8] RICUPERO, Rubens. O Brasil e o dilema da globalização. São Paulo: Serviço Nacional de Aprendizagem Comercial, 2001. pp. 27-88.

mercado. Outra quimera indicada pelo embaixador relaciona-se à ideia da agonia do conceito de soberania do Estado. Em relação a esse, ele oferece exemplo que deixa, no mínimo, grande interrogação. O professor argumenta que

> "(....) se fosse verdade que a globalização inelutavelmente acarreta o encolhimento das soberanias e a superação do Estado-nação, em nenhum lugar essas tendências deveriam ser tão evidentes como nos EUA, inventor e centro da globalização e Estado mais globalizado do planeta. Ora, é o inverso que ocorre. Nunca a soberania americana dispôs de tantos instrumentos de poder e nunca os utilizou com tamanha desenvoltura, para afirmar-se como faz hoje"[9].

Essa perspectiva parece confirmada pelos novos métodos utilizados pelo governo estadunidense para espionar não só pessoas físicas e jurídicas, mas também governos estrangeiros.

Do exposto, parece razoável supor que a globalização tem, por igual, desdobramento no plano jurídico. Esse desdobramento ocorre tanto na esfera interna quanto na externa. Em sua dimensão exterior, a globalização jurídica representa o braço de segurança necessário à consolidação do que até aqui se alcançou, sobretudo, no plano econômico: transnacionalização dos mercados de insumos, produção, capitais, finanças e consumo. Cuida-se, portanto, de apreciar o impacto da globalização no direito internacional. Esse estudo é importante para o exato enquadramento tanto da espionagem quanto de suas exatas consequências. Em derradeira análise, como controlar, pela via do direito, o abuso no desrespeito tanto à

---

[9] RICUPERO, op. cit., p. 46.

dignidade da pessoa humana quanto da privacidade que a espionagem oficial desmedida encerra.

Trata-se, pois, de evitar análise pela ótica tanto da imposição por "extensão universal de um sistema legal" quanto da "criação de sistemas regulatórios não-estatais"[10]. Nesse passo, é relevante destacar a observação de Brigitte Stern no sentido de que "a única maneira de regulamentar a economia global e o mundo globalizado é desenvolver a eficiência da lei internacional, tanto no seu conteúdo quanto na sua estrutura legal. Em outras palavras, não há salvação fora da 'criação de um verdadeiro sistema internacional legislativo de regulamentação universal'"[11]. Essa perspectiva é tanto mais verdadeira quanto mais se tem em atenção os efeitos da tecnologia na vida das pessoas.

Com isso, e em consonância como pensamento de Matias, é razoável sustentar que a globalização do direito

> "pode ser desdobrada em dois aspectos principais: aumento no número de regras internacionais e proliferação das organizações internacionais. Ambos os aspectos possuem caráter jurídico e político e contribuem para a construção da sociedade global. O primeiro, de caráter mais geral, é abordado como globalização jurídica. O segundo pode ser visto sob dois ângulos principais: a cooperação internacional e a integração regional".[12]

---

[10] Para maiores aprofundamentos, ver STERN, Brigitte. "How to regulate globalization?". In: BYERS, Michael (Ed.) The role of law in international politics: essays in international relations and international law. Oxford: Oxford University Press, 2001. pp. 246-268.

[11] STERN, Brigitte. O contencioso dos investimentos internacionais. Barueri: Manole, 2003. p. 8.

[12] MATIAS, Eduardo. Humanidade e suas fronteiras: do Estado soberano à sociedade global. Rio de Janeiro: Paz e Terra, 2005. p. 197.

Parece, de início, que esse modo de agir poderia dar o tom do tratamento a ser ministrado para os abusos cometidos por agências do governo dos Estados Unidos da América (EUA) no tocante à invasão indiscriminada de correspondências eletrônicas e de comunicações de inúmeras pessoas em plano global. Os desafios, no entanto, são imensos. É conhecida a virtual ausência de normas a vincular os Estados nesse domínio. E mais, no campo do direito das gentes, seguimos em terreno fortemente marcado pelo voluntarismo estatal. Isso é tanto mais verdadeiro quanto mais se considera determinados modos de proceder na arena internacional de potências como os EUA.

Dessa forma, a implementação de marco legislativo no âmbito do direito internacional de modo a regulamentar os espaços de atuação excepcional dos Estados na intromissão no direito à privacidade em um mundo globalizado, bem como os mecanismos multilaterais de controle dessa eventual intromissão, ainda está por ser feito.

Tendo em conta o que foi dito, esse capítulo do relatório objetiva dar notícia do papel, ainda que rarefeito, do direito internacional público no atual combate a sistemas de espionagem como o implementado pela Agência de Segurança Nacional dos EUA. Essa parcela do relatório trará, ainda, notícia sumária dos trabalhos da comissão instalada no âmbito do Parlamento Europeu para cuidar do assunto.

II. 2. Direito internacional público

No campo do direito internacional público, o aspecto mais diretamente vinculado com os fatos investigados pela CIP da Espionagem relaciona-se com a dimensão de proteção aos direitos humanos. E, nesse domínio, com a necessidade de se respeitar a vida privada das pessoas.

O direito à privacidade sobressai como mecanismo de proteção contra a arbitrariedade praticada por agências de governo estadunidenses no vasculhar indiscriminada e indistintamente a vida de súditos de diferentes países, bem como seus respectivos governos. Os episódios que levaram à instalação desta CPI representaram, a juízo de muitos, verdadeira ofensa a esse direito, consagrado em vários instrumentos internacionais.

Dessa forma, a interceptação irrestrita de comunicações, bem como a gravação injustificada de dados pelos serviços de inteligência dos EUA denota implacável violação à privacidade do ser humano. Essa forma de agir significa — sobretudo em democracias consolidadas como as envolvidas no episódio — ofensa gravíssima a esse direito.

Nessa ordem de ideias, convém recordar o que estabelecem alguns instrumentos internacionais em relação ao assunto. De início, a Declaração Universal dos Direitos Humanos [DUDH (1948)], que assim dispõe:

> Artigo XII. Ninguém será sujeito a interferência arbitrária na sua privacidade, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques.

É, por igual, oportuno consignar o estipulado em relação ao tema no Pacto Internacional sobre Direitos Civis e Políticos [PIDCP (1966)][13]:

> Artigo 17.
>
> 1. Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação.
>
> 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.

No ponto, a Convenção Americana de Direitos Humanos [CADH, Pacto de San José da Costa Rica (1969)][14] estipula:

> Artigo 11. Proteção da Honra e da Dignidade
>
> 1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.
>
> 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação.
>
> 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

A Convenção Europeia dos Direitos Humanos [CEDH (1950)] prescreve, por igual, que:

> Artigo 8°. Direito ao respeito pela vida privada e familiar.
>
> 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

---

[13] Incorporado ao ordenamento jurídico brasileiro por meio do Decreto n° 592, de 1992.
[14] Incorporado ao ordenamento jurídico brasileiro por meio do Decreto n° 678, de 1992

> 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção de infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

A Carta dos Direitos Fundamentais da União Europeia (2010)[15] contempla, sobre a matéria, o seguinte dispositivo:

> Artigo 7°. Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Dos textos transcritos, é apropriado destacar que: **a)** inexiste, para fins do direito que se almeja proteger, distinção de substância entre "privacidade" (DUDH) e "vida privada" (CEDH); cuida-se, em derradeira análise, tão só da tentativa de assegurar a concordância entre os textos inglês e francês; **b)** o Artigo 17 do PIDCP, cópia do Artigo XII da DUDH, é, no entanto, mais enfático na proibição. Com efeito, ele visa a proibir "interferência arbitrária *ou ilegal*", ou seja, nenhuma interferência pode ocorrer, exceto nos casos previstos em lei; **c)** a CEDH, por seu turno, prevê (Art. 8°, 2) limitações que podem ser fixadas ao direito proclamado (Art. 8°, 1).

Com exceção do "bem estar econômico do país", as demais limitações previstas na CEDH são compreensíveis. Contudo, mesmo em relação a esses limites é necessário juízo de ponderação, de razoabilidade e de clara percepção no sentido de que, na dúvida sobre se determinada

---

[15] O texto retoma, com adaptações, a Carta proclamada em 7 de dezembro de 2000, e a substitui a partir da entrada em vigor do Tratado de Lisboa.

forma de ação do Estado afronta essa proteção, deve-se garantir o direito à privacidade da potencial vítima.

Tão exato quanto o que foi acima dito é a circunstância de que as normas de direito internacional que, de tal ou qual forma, cuidam da matéria não definem o que se entende por "privacidade" ou "vida privada". O conceito, de resto, é ambíguo também no plano jurídico interno dos Estados. Cuida-se provavelmente do direito mais difícil de definir no amplo catálogo internacional de direitos humanos. As definições variam enormemente à vista do contexto e do ambiente que se tem em consideração. A depender do interessado/intérprete, ele pode adquirir distintas acepções. Assim, por exemplo, contemplar proteção:

> 1. Da inviolabilidade física e mental do indivíduo e da liberdade intelectual e moral da pessoa;
>
> 2. Contra ataques à honra ou reputação do indivíduo e ofensas similares;
>
> 3. Do nome, identidade ou imagem do indivíduo contra uso não autorizado;
>
> 4. Contra a divulgação de informação abrangida pelo dever de segredo profissional; e
>
> 5. Contra ser espionado, vigiado ou molestado[16].

---

[16] Para maiores desdobramentos, v., entre outros, LOUCAIDES, L. "Personality and privacy under the European Convention on Human Rights". British Year Book of International Law, vol. 61, pp. 175-197, 1990.

Entendimento mediano registra que a vida privada seria o direito de viver, de acordo com sua vontade, protegido da publicidade. Ocorre, todavia, que as pessoas vivem em sociedade. Com isso, a proteção à privacidade pode sofrer temperamentos. De toda forma, as autoridades públicas competentes somente podem exigir informação relacionada à vida privada de uma pessoa na hipótese de essa informação ser essencial para os interesses da sociedade em questão. E aqui vale uma advertência: mesmo em relação às ingerências permitidas no direito das gentes, a legislação estatal relevante deve especificar, de maneira detalhada, as circunstâncias precisas em que essas intromissões são permitidas.

Dessa forma, a coleta e o armazenamento de informações pessoais em computadores, banco de dados e outros dispositivos, seja por autoridades públicas ou pessoas físicas ou jurídicas, devem ser regulados por lei. Para além disso, medidas eficazes devem ser tomadas pelo Estado para assegurar que informações a respeito da vida privada de uma pessoa não estejam ao alcance de outras pessoas não autorizadas por lei para receber, processar ou usar tais informações. É, pois, obrigação dos Estados a adoção de medidas legislativas e outras necessárias para dar efeito à proibição de interferências e ataques. Em síntese, a plena fruição do direito à privacidade demanda ação e vigilância constante do Estado.

Os tratados transcritos representam avanço no plano internacional da proteção do direito à privacidade, mas vinculam, tão só, os Estados que formalmente se comprometeram por meio da ratificação/adesão. Essa circunstância não vale para a DUDH, é certo; não menos certo, entretanto, é que esse instrumento não é autoaplicável. A

Declaração, em síntese, não dispõe de mecanismos asseguradores do cumprimento de suas disposições.

Já o PIDCP possui meios de implementação e monitoramento, que envolve a sistemática de relatórios encaminhados pelos Estados-partes, bem como o mecanismo opcional de comunicações interestatais. A esse sistema, o Protocolo Facultativo ao Pacto adiciona a possibilidade de petições individuais a serem apreciadas pelo Comitê de Direitos Humanos. O direito de petição individual mencionado colabora com a institucionalização da capacidade processual internacional dos indivíduos e constitui forma de proteção. Há, assim, algum modo de *international accountability*.

Ocorre, entretanto, que os Estados Unidos da América não estão vinculados a esses meios de proteção. Eis aí um grande paradoxo: o Estado que pretende ser o guardião dos direitos e garantias fundamentais não endossa os documentos internacionais relacionados com a matéria. Em relação aos seus nacionais, o governo americano adota um procedimento; já no tocante aos estrangeiro, a conduta é outra. "Faça o que eu digo, mas não faça o que eu faço". Tratando-se de país com sólida tradição democrática, esse exemplo é, a vários títulos, lamentável.

No âmbito da ONU, convém recordar, desde logo, que o tratado constitutivo da Organização estabelece entre seus propósitos "promover e estimular o respeito aos direitos humanos e às liberdades fundamentais para todos" (Art. 1°, 3, da Carta da ONU). Com o tempo, essa finalidade foi alargada — tanto no que tange aos instrumentos quanto no tocante às instituições — e adquiriu maior consistência. Nos dias de

hoje, o Alto Comissário das Nações Unidas para os Direitos Humanos trabalha para oferecer conhecimento e apoio aos diferentes mecanismos de monitoramento dos direitos humanos no sistema onusiano. Ele é, de algum modo, o coração do sistema.

Dentro do espírito de ampliar o debate em torno das graves violações perpetradas pelo governo dos Estados Unidos e de modo a levá-lo para o campo do multilateralismo, o governo brasileiro estimou adequado acionar os canais disponíveis nas Nações Unidas. Nesse sentido, o Brasil, em conjunto com a Alemanha, ofereceu proposta de resolução à Terceira Comissão da Assembleia-Geral (AG) da Organização. Ambos os países apresentaram, no dia 1° de novembro de 2013, projeto de resolução sobre o direito à privacidade na era digital[17]. O assunto foi endereçado, como referido, à Terceira Comissão da AG, responsável por temas relacionados com aspectos sociais, humanitários e culturais[18].

A proposta bilateral em comento tem sua gênese vinculada, como já destacado no âmbito deste relatório, às revelações feitas pelo Sr. Edward Snowden. Em conformidade com o que foi divulgado, os serviços de espionagem dos EUA devassaram a privacidade de súditos (pessoas físicas e jurídicas) de diversos países, com destaque para as comunicações

---

[17] V. íntegra da proposta tanto na versão autêntica (em inglês) quanto na oficial (em português) em: http: //www.itamaraty.gov.br/sala-de-imprensa/notas-a-imprensa/brasil-e-alemanha-apresentam-a-assembleia-geral-da-onu-projeto-de-resolucao-sobre-o-direito-a-privacidade-na-era-digital. Acesso em: 4 de nov. de 2013.

[18] A Assembleia-Geral desempenha suas funções por meio do trabalho de seis Comissões principais, nas quais todos os membros têm direito a representação. São elas: Primeira Comissão (política e segurança); Segunda Comissão (econômica e financeira); Terceira Comissão (social, humanitária e cultural); Quarta Comissão (tutela); Quinta Comissão (administrativa e orçamentária); e Sexta Comissão (jurídica).

telefônicas e eletrônicas de distintos chefes de Estado. O tema motivou oportuno discurso da Presidente Dilma Rousseff na abertura do Debate Geral da 68ª Assembleia-Geral da ONU, em 24 de setembro de 2013[19]. O governo brasileiro dava, assim, início ao lançamento de ação, no âmbito das Nações Unidas, com vistas a coibir ou diminuir semelhante conduta.

Desde então, a matéria tem avançado com certa dificuldade. Diferentes países, destacadamente europeus, hesitam em assumir atuação mais bem definida no plano diplomático. O cenário começa a se alterar com revelações de que os Estados Unidos também espionaram alemães, franceses, espanhóis e, até mesmo, o Papa. Nesse sentido, a Chanceler Federal alemã, Angela Merkel, ficou particularmente agastada com a apresentação de indícios veementes de que seu aparelho celular havia sido "grampeado" por agentes norte-americanos.

Em face disso, o Brasil conseguiu, como referido, apoio da Alemanha na tentativa de avançar na ONU proposta de resolução, a ser encaminhada à consideração da Assembleia-Geral (AG), com o objetivo de ampliar o direito à privacidade previsto no Pacto Internacional de Direitos Civis e Políticos. A proposta foi aprovada no dia 26 de novembro de 2013 na referida Comissão, tendo sido encaminhada à apreciação da AG no final do ano. Nessa ordem de ideias, o projeto em comento é o primeiro passo no sentido de conter, ainda que minimamente, a intrusão de determinados

---

[19] V. íntegra do discurso em: http://www.itamaraty.gov.br/sala-de-imprensa/discursos-artigos-entrevistas-e-outras-comunicacoes/presidente-da-republica-federativa-do-brasil/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-york-eua-24-09-2013. Acesso em: 5 de nov. de 2013.

órgãos de governo de diferentes países nas comunicações, sobretudo *online*, de estrangeiros.

A proposta representa o prelúdio do projeto de resolução a ser encaminhada à consideração da AG das Nações Unidas. Assim, convém ter notícia, ainda que breve, dos efeitos de uma resolução aprovada pelo órgão plenário máximo da Organização.

As resoluções da Assembleia-Geral das Nações Unidas não têm, em princípio, o condão de produzir norma vinculante de direito internacional[20]. Elas, de resto, obedecem à dinâmica própria no campo internacional. Sua gênese se dá no contexto de uma organização internacional e o ato final de aprovação não prevê, em regra, audiência preliminar dos respectivos parlamentos dos Estados membros da organização.

Dessas características — ausência de força vinculante e gênese organizacional —, a primeira tem, aos olhos de muitos, sofrido abrandamentos. Assim, as resoluções aprovadas com maioria qualificada, as que interpretam dispositivos do tratado constitutivo da ONU e as vocacionadas a codificar normas consuetudinárias na esfera internacional têm adquirido, para alguns, estatura de norma vinculante. Há, por igual, percepção de que, em determinados casos, as resoluções da Assembleia constituem evidência de direito consuetudinário internacional.

---

[20] Registramos que o termo "resolução" não se encontra no Tratado Constitutivo da Organização das Nações Unidas (ONU). A Carta da ONU faz menção à palavra "recomendação" (arts. 10, 11, 12, 13 e 14). Os usos e costumes, no entanto, fizeram com que as recomendações oriundas da Assembleia-Geral fossem comumente referidas como resoluções.

Essa constatação, no entanto, não cria, por si só, nova regra de direito consuetudinário. Representa, contudo, importante ponto de partida para o estabelecimento de norma costumeira. Nesse sentido, é digna de nota manifestação da Corte Internacional de Justiça (CIJ) sobre a matéria externada em opinião consultiva de meados dos anos 90.

Da decisão do principal órgão judiciário das Nações Unidas, recolhemos a seguinte passagem [ênfase acrescida (tradução livre)]:

> "A Corte observa que as resoluções da Assembleia-Geral mesmo que não sejam vinculantes, podem eventualmente ter valor normativo. Elas podem, em determinadas circunstâncias, proporcionar importante evidência para o estabelecimento da existência de norma ou do surgimento de *opinio juris*. Para fixar quando isso ocorre, é necessário apreciar seu conteúdo, bem assim as condições de sua adoção"[21].

Esse o quadro, passamos a tecer considerações sobre o conteúdo da proposta germano-brasileira. De início, é oportuno registrar, uma vez mais, que o assunto foi encaminhado à Terceira Comissão à vista da circunstância de que para lá são endereçados os temas que tenham desdobramento social, humanitário e cultural. Parte importante do trabalho dessa Comissão está direcionada ao exame de questões pertinentes aos direitos humanos.

---

[21] Texto original: "The Court notes that General Assembly resolutions, even if they are not binding, may sometimes have normative value. They can, in certain circumstances, provide evidence important for establishing the existence of a rule or of emergence of an opinio juris. To establish whether this is true of a given General Assembly resolution, it is necessary to look at its content and the conditions of its adoption". UNITED NATIONS. International Court of Justice. Legality of the Theater or Use of Nuclear Weapons (Opinião Consultiva), ICJ Reports, 8 de julho de 1996, § 70, pp. 254-255. Disponível em: <http://www.icj-cij.org/docket/files/93/7407.pdf>. Acesso em: 4 nov. 2013.

Dessa maneira, a Comissão acompanha os desenvolvimentos produzidos na esfera dos direitos humanos no âmbito onusiano. Na 67ª Sessão da AG, por exemplo, a Terceira Comissão apreciou 59 minutas de resoluções sobre essa temática, das quais mais da metade foi submetida ao órgão colegiado máximo da Organização[22].

Nessa ordem de ideias, ambos os países estimaram por bem apresentar o projeto de resolução em análise. O texto produzido foi o primeiro esboço. Ele recebeu sugestões e resultou aprovado no âmbito da Terceira Comissão. Com efeito, no dia 26 de novembro de 2013 essa Comissão aprovou, como mencionado, o texto. A redação final sofreu, no entanto, alguma alteração. De forma a angariar o apoio dos EUA, da Grã-Bretanha, da Austrália, do Canadá e da Nova Zelândia, o projeto foi amenizado em seu tom inicial. A principal modificação foi no sentido de afastar eventual relação direta entre espionagem e direitos humanos.

A proposta dá o tom do que se deseja: ampliar e reafirmar na era digital o direito à privacidade, contemplado em distintos instrumentos internacionais[23]. O documento segue o linguajar diplomático de estilo. Ele começa em forma de considerandos. Dentre estes, vale destacar os seguintes:

> PP4. Observando que o ritmo acelerado do desenvolvimento tecnológico permite aos indivíduos em todas as regiões utilizarem novas tecnologias de informação e comunicação e, ao mesmo

---

[22] Dados extraídos do endereço eletrônico da Comissão (http://www.un.org/en/ga/third/. Acesso em: 5 de nov. de 2013).

23 V., por exemplo, Art. 12 da Declaração Universal dos Direitos Humanos; Art. 17 do Pacto Internacional de Direitos Civis e Políticos, e Art. 7° da Carta dos Direitos Fundamentais da União Europeia (UE).

> tempo, aumenta a capacidade de governos, empresas e indivíduos de vigiar, interceptar e coletar dados, o que pode violar os direitos humanos, em particular o direito à privacidade, tal como consagrado no artigo 12 da Declaração Universal dos Direitos Humanos e no artigo 17 do Pacto Internacional de Direitos Civis e Políticos e constitui, portanto, tema de preocupação crescente
>
> (...)
>
> PP8. Enfatizando que a vigilância ilegal das comunicações, sua interceptação, bem como a coleta ilegal de dados pessoais constituem atos altamente intrusivos que violam o direito à privacidade e à liberdade de expressão e que podem ameaçar os fundamentos de uma sociedade democrática.
>
> PP10. Profundamente preocupada com violações e abusos dos direitos humanos que podem resultar de qualquer vigilância, inclusive extraterritorial, das comunicações, sua interceptação, bem como coleta de dados pessoais, em particular da vigilância, interceptação e coleta de dados em massa.

Na sequência, o projeto prescreve que os mesmos direitos que as pessoas possuem fora da rede (*offline*) devem ser protegidos em rede (*online)*. O texto termina conclamando os Estados a respeitar os direitos humanos, de modo especial, o direito à privacidade; a adotarem medidas com vistas a cessar eventuais violações; a revisarem suas práticas, procedimentos e legislação no que tange ao tema; e a estabelecerem mecanismos nacionais independentes de supervisão de modo a assegurar transparência e responsabilização por possíveis transgressões. O projeto solicita, por fim, à Alta Comissária das Nações Unidas para os Direitos Humanos, Senhora Navanathen (Navi) Pillay, que apresente à AG relatório preliminar sobre a proteção do direito à privacidade no contexto da vigilância nacional e extraterritorial das comunicações, sua interceptação e coleta de dados pessoais em massa.

O teor do documento aprovado na Terceira Comissão e na AG não oferece elementos caracterizadores da *opinio juris*. Sendo assim, ele não tem, mesmo que em estado latente, o jeito de costume. Ou seja, o projeto como redigido não tem efeito jurídico gerador de obrigações internacionais. Em resumo, trata-se, ao menos no primeiro momento, de instrumento mais político do que jurídico. E mesmo sob essa ótica, ambos os governos não pretendem apontar os EUA como grandes vilões. Eles buscam, de um lado, dar recado político de suas insatisfações; de outro, caminhar no sentido de se ampliar a proteção para as comunicações *online* do direito à privacidade. Essa extensão, ao sentir de muitos, é necessária, visto que o Pacto Internacional de Direitos Civis e Políticos foi adotado pela XXI Sessão da Assembleia-Geral das Nações Unidas, em 16 de dezembro de 1966. Naquela altura, os meios de comunicação e de troca de informações eram muito mais rudimentares.

Historicamente, as resoluções da Assembleia-Geral representam mais a necessidade de manter o tema objeto do instrumento na agenda internacional e na direção de algo vinculante no futuro do que fonte cogente do direito internacional. Os exemplos podem ser contados à exaustão. Ocorre, no entanto, que, passados quase 69 anos do nascimento das Nações Unidas, tanto a doutrina quanto a jurisprudência internacionais começam a indicar que determinados documentos têm, pelo menos, o requisito da *opinio juris* que todo costume encerra.

Isso não é, ao que parece, o que se apresenta no caso presente. Cuida-se de iniciativa que poderá, de modo eventual, tornar-se o embrião de algo mais consistente no sentido de se proteger o direito à privacidade na era digital. Essa perspectiva, havendo vontade política no campo

internacional, já dispõe de instrumentos para sua implementação. Outro aspecto a considerar é o fato de que possível resolução no sentido do que se deseja carrega forte conteúdo moral.

De todo o exposto, vê-se que, no campo do direito internacional, as perspectivas de ação contra os Estados Unidos da América pelos fatos objeto desta CPI são praticamente inexistentes. De toda maneira, esse ramo da ciência jurídica pode dar o tom de tratamento mais abrangente do assunto, tendo em conta o que descrito no romper desse capítulo, ou seja, o inexorável processo de globalização em que o mundo está inserido.

Assim, também em relação ao trato dessa matéria, o Estado individualmente considerado tornou-se pequeno demais para enfrentar a questão de maneira isolada. Há necessidade de atuação conjunta, de modo a erigir alguma forma de governança global no tocante à matéria.

Em resumo, os mecanismos atualmente existentes para tanto são pequenos, para não dizer inexistentes, mas as possibilidades são grandes. De todo modo, parece cada vez mais necessário o estabelecimento de marco multilateral para a governança internacional do setor de comunicações, sobretudo da internet, de forma a assegurar a efetiva proteção de dados, bem assim a privacidade das pessoas e das empresas, para não mencionar as informações dos governos.

A necessidade de manter sob controle os excessos do Estado na vigilância secreta é manifesta. O tema, no entanto, demandará muito consumo de energia nos anos que estão por vir. De toda maneira, é

fundamental manter os olhos no alvo certo, que não é, de modo necessário, a questão da espionagem mútua entre os Estados, mas a profunda erosão do direito à privacidade.

Outro aspecto relacionado ao direito das gentes é o que se vincula à Convenção de Viena sobre Relações Diplomáticas de 1961. Esse instrumento convencional codificou normas consuetudinárias que têm atrás de si longa história. O documento invoca em seus considerandos os propósitos e princípios da Carta das Nações Unidas relativos à igualdade soberana dos Estados, à manutenção da paz e da segurança internacional e ao desenvolvimento das relações de amizade entre as nações. Vários dispositivos estão, dessa ou daquela maneira, vinculados ao tema objeto de nossas preocupações (p. ex.: arts. 24, 27 e 40).

O artigo 41 da Convenção, entretanto, merece destaque. Em seu inciso terceiro, ele prescreve que os locais da Missão não devem ser utilizados de maneira incompatível com as funções da Missão. Entre essas funções está a de inteirar-se por todos os **meios lícitos** das condições existentes e da evolução dos acontecimentos no Estado acreditado e informar a respeito o Governo do Estado acreditante [art. 3, d (ênfase acrescida)].

As notícias divulgadas demonstram, em larga medida, que princípios caros aos membros da ONU, transcritos em seu tratado constitutivo, foram afrontados. Elas revelam, ainda, que os EUA, também mediante sua Missão em Brasília, utilizaram-se de meios ilícitos para se *inteirar* de "acontecimentos" em nosso país envolvendo não só amplo

leque de nacionais (pessoas físicas e jurídicas), mas também escalões mais elevados da administração federal.

O contexto antes descrito de afronta à Convenção de Viena é tanto mais grave quanto mais temos em atenção a circunstância de que ambos os países possuem Acordo de Assistência Judiciária em Matéria Penal[24]. Esse tratado visa justamente facilitar a execução das tarefas das autoridades responsáveis pelo cumprimento da lei de ambos os países, na investigação, inquérito, ação penal e prevenção do crime por meio de cooperação e assistência judiciária mútua em matéria penal. O governo estadunidense poderia ter utilizado essa via em sua luta no combate ao terrorismo, por exemplo. De outra maneira, pode-se destacar a existência de mecanismo idôneo para se alcançar o fim almejado em estrita observância aos direitos e garantias fundamentais. O regime democrático impõe sacrifícios. O absoluto respeito à ordem jurídica é, por vezes, um deles.

II. 3. Direito comunitário

O chamado direito comunitário representa desdobramento do direito da integração, que se desenvolveu a partir da consolidação de blocos econômicos regionais. Esses blocos têm como objeto a integração entre países para a proteção e a consolidação de objetivos comuns. Diferenças institucionais, relacionadas com realidades históricas, econômicas e

---

[24] Incorporado ao ordenamento jurídico brasileiro por meio do Decreto nº 3.810, de 2001.

políticas, caracterizam os diferentes modelos de integração econômica. Nesse sentido, o Mercado Comum do Sul (Mercosul) e a União Europeia (UE) são bons exemplos dessas distintas formas de integração.

O Mercosul representa forma de integração em fase de desenvolvimento. Ele tem como principal instituto a intergovernabilidade. Não há, portanto, delegação de soberania dos Estados. Há, assim, necessidade de que as normas provenientes do processo de integração sejam aceitas por todos os membros do bloco. Em que pese o avanço verificado desde sua criação, esse Mercado ainda se mostra imaturo em relação aos seus objetivos. Cuida-se de modelo integracionista que tem por base o direito internacional público. Nesse sentido, pode-se dizer que o Mercosul é uma organização internacional de corte clássico.

Já a UE simboliza integração mais consistente. Ela logrou adotar, por exemplo, um mercado comum e uma moeda única. Seus fundamentos se encontram no direito comunitário, que tem por base a subsidiariedade, a aplicabilidade imediata das normas provenientes do bloco e a supranacionalidade.

Outro aspecto a levar em conta é o que diz com a institucionalização do bloco. No caso europeu, ela é muito mais sólida. Assim, por exemplo, a existência de ordenamento judiciário, que tem por vértice o Tribunal de Justiça da UE. Esse órgão atuou e atua de modo decisivo por meio de decisões que corroboram a autonomia desse direito. Ele, em última análise, proporciona uniformidade na interpretação jurisprudencial e na aplicação das normas comunitárias.

Tendo em conta a maior solidez — no âmbito do direito da integração — do direito comunitário, bem assim as iniciativas da UE no tocante tanto à proteção dos direitos humanos, sobretudo de seus cidadãos, quanto ao combate da espionagem indiscriminada mediante novas tecnologias, esta parte do relatório levará em conta os trabalhos que nesse domínio vêm sendo produzidos na Europa integrada, de modo destacado no âmbito do Parlamento Europeu (PE). Essa análise revela-se importante no sentido de verificar outras práticas, bem como de constatar que a indignação do parlamento brasileiro com a espionagem realizada pela NSA não é ato isolado.

Na amplo espectro de instituições da UE, merece destaque para as finalidades desta parte do relatório os trabalhos no PE. Trata-se, como o nome indica, da instituição parlamentar da UE. Nesse Parlamento, que tem sede em Estrasburgo, estão representadas as grandes tendências políticas encontráveis nos países membros. Ele tem três competências principais:

> 1) adoção de atos legislativos europeus, que tem sua forma mais usual no processo de "co-decisão" entre esse órgão e o Conselho da UE, detentor do monopólio legislativo em alguns domínios (agricultura, política econômica e de imigração, por exemplo). Ainda nesse campo, a adesão de novos países à UE demanda a aprovação do Parlamento;
>
> 2) controle democrático das demais instituições europeias. Assim, por exemplo, a aprovação dos membros da Comissão indicados pelos Estados membros e a possibilidade de estabelecimento de uma "moção de censura", que implica a demissão de toda a Comissão; a análise periódica de relatórios enviados pela Comissão, de petições apresentados por cidadãos e instituição de comissões de inquérito; e
>
> 3) aprovação e controle da execução do orçamento anual da UE, decidido em conjunto como Conselho. O Parlamento exerce,

ainda, controle sobre a gestão de créditos e avalia os efeitos dos financiamentos realizados com base no orçamento.

É, portanto, na competência que trata do controle democrático que reside o papel do PE para também avaliar os episódios trazidos a público e fartamente noticiados pelo *The Guardian*. O PE tem experiência acumulada no tocante à criação de comissões de inquérito (*committee of inquiry*). Para o assunto que nos interessa, suficiente recordar a comissão sobre a existência de sistema global para a interceptação de comunicações privadas e comerciais (*ECHELON interception system*). Essa comissão apresentou seu relatório final em julho de 2001[25]. De tal ou qual maneira, ela cuidou de aspectos assemelhados aos que constituem objeto da nossa CPI.

Passados doze anos, o PE viu-se, uma vez mais, diante da perspectiva de investigar novos fatos reveladores de ampla e indiscriminada espionagem levadas a efeito por governo de país considerado, a vários títulos, aliado e amigo dos países membros da UE. Dessa maneira, foi instituída, no âmbito da Comissão de Liberdades Civis, Justiça e Assuntos Internos [*Civil Liberties, Justice and Home Affairs* (*LIBE*)] do Parlamento, a Comissão de Inquérito sobre Espionagem Eletrônica em Massa de Cidadãos da União Europeia (*LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens*). Por meio de resolução de 4 de julho de 2013, o PE estabeleceu o mandato da Comissão

---

[25] Relatório final disponível em: http://www2.europarl.eu.int/omk/OM-Europarl?PROG=REPORT&L=EN&PUBREF=-//EP//TEXT+REPORT+A5-2001-0264+0+NOT+SGML+V0//EN. Acesso em: 25 de nov. de 2013.

e seu programa de trabalho[26]. A experiência pretérita (Sistema ECHELON) e o resultado das inúmeras audiências realizadas no âmbito da Comissão darão suporte para o relatório final, votado no primeiro semestre de 2014.

Os desafios da Comissão de Inquérito da LIBE são, também, imensos. Eles dizem respeito, por exemplo, à exata separação entre competências domésticas e comunitárias na proteção os respectivos sistemas de dados. Para além disso, é importante registrar que os trabalhos dessa comissão estão incluídos em marco legal distinto daquele em que se insere o Senado Federal. De qualquer forma, as atribuições e competências de um parlamento doméstico são distintas daquelas outorgadas a um parlamento comunitário.

Para além dessa circunstância, convém sublinhar que os *europarlamentares* têm suas origens em países com sistema de governo parlamentarista. Esse fato repercute, de algum modo, na análise da situação, sobretudo no tocante às eventuais medidas a serem adotadas em relação ao objeto da investigação. É que no sistema presidencialista, ao qual estamos inseridos, a condução das relações exteriores é competência privativa do Presidente da República (art. 84, VII, da Constituição Federal). É virtualmente inexistente nesse contexto ação ativa por parte do Congresso Nacional. Nesse domínio, o parlamento pode, tão só, exercer sua função fiscalizadora [p.ex.: realização de audiência pública, convocação de Ministro de Estado, (des)aprovação do orçamento, (des)aprovação da escolha de chefes de missão diplomática de caráter

---

26 Encontrável em: http://www.europarl.europa.eu/document/activities/cont/201309/20130904ATT70774/20130904ATT70774EN.pdf. Acesso em: 25 de nov. de 2013.

permanente, (des)autorização de operações externas de natureza financeira de interesse da União].

O quadro antes descrito ficou evidenciado quando da videoconferência realizada entre o PE e membros desta CPI no dia 18 de dezembro de 2013. O encontro, para além do seu pioneirismo, representou importante aproximação do Senado com a instituição parlamentar da União Europeia. A percepção que restou é a de que, definidos os exatos limites das respectivas competências (doméstica e comunitária), o PE pode ter atuação um pouco mais destacada em relação ao assunto, sem que ela, no entanto, seja exuberante.

Nesse sentido, o relatório final da Comissão da LIBE, a que esta Comissão teve acesso em 21 de fevereiro de 2014, faz invocação de inúmeras decisões nas esferas internacionais, comunitárias, domésticas e estrangeiras relacionadas, de alguma maneira, ao assunto da espionagem em massa. Reconhece que muitos dos problemas de agora são similares àqueles apontados no relatório do Sistema ECHELON. Indica que a ausência de marco legislativo consistente para acompanhar as recomendações da Comissão de Inquérito ECHELON representa importante lição para a situação presente. Nesse sentido, o relator da Comissão, Senhor Claude Moraes, sugere a implementação de 8 ações no marco do que denomina "*Habeas Corpus* Digital Europeu – protegendo direitos fundamentais na era digital" (*A European Digital Habeas Corpus – protecting fundamental rights in a digital age*). Propõe, ao final, minuta de resolução para apreciação plenária do respectivo parlamento.

O *Relatório LIBE* oferece, ainda, em sua "justificação" (*explanatory statement*) observação relevante a vários títulos. Cuida-se do fato de que as reações aos graves fatos divulgados terem tido pouco repercussão nos parlamentos dos Estados membros da UE. Com exceção da Alemanha, o tema não mereceu considerações mais severas nem mesmo nos países cuja imprensa foi mais contundente: Reino Unido (*The Guardian*) e France (*Le Monde*). Nesse sentido, o relatório registra a contribuição de órgãos dos parlamentos belga, neerlandês, dinamarquês e norueguês. Os parlamentos britânico e francês declinaram participação. O fato é, de alguma forma, eloquente das percepções em relação à matéria e chama a atenção para a relevância desta Comissão, que apesar de alguma resistência não deixou o tema passar em branco por "decurso de prazo".

Assim, as conclusões a que chegaremos neste relatório estão mais relacionadas com nosso marco jurídico. Em derradeira análise, as avaliações aqui feitas dizem mais respeito às imperfeições dos nossos serviços de inteligência e contrainteligência; às debilidades dos nossos sistemas de comunicação e, como tal, merecem resposta e tratamento no âmbito interno, ao menos no primeiro momento. É nele que o Parlamento brasileiro pode exercer suas atribuições de fiscalização de modo mais consistente. De toda maneira, é fundamental perceber com atenção o exercício do PE por intermédio da Comissão de Inquérito da LIBE de forma a oferecer perspectiva comparada nas medidas que hão de ser aplicadas nos anos que estão por vir.

II. 4. Conclusões

O direito das gentes atual trata de temas os mais variados. Isso se dá considerando, entre outras coisas, a globalização, a proliferação de normas, o aumento no número de atores com poder negocial, o fim do mundo bipolar e a emergência da democracia em seus domínios, ainda que relativamente mitigada. Ele, em síntese, penetra áreas que se relacionam ao econômico, social, cultural, técnico. Esse aumento nas faixas de atuação é, de tal ou qual modo, consequência da crescente necessidade de os atores internacionais enfrentarem novas questões no seu relacionamento mútuo sem as amarras de muitos dos acontecimentos referidos.

Os problemas, novos ou sob novas roupagens, transcendem a noção de território estatal. Assim, por exemplo, direitos humanos, meio ambiente, saúde, comunicações, crime organizado, terrorismo, domínio público (regiões polares, mar, bacias hidrográficas, espaço extra-atmosférico e sideral), patrimônio comum da humanidade, comércio, finanças e propriedade intelectual.

Recentes ou antigos, os atuais desafios perpassam diferentes domínios, que faz com que o direito internacional continue em constante evolução. Para compreender esse processo parece mais apropriado ter os pés no chão. Nesse sentido, as observações de Alan Pellet são pertinentes. Segundo o teórico francês, "o direito reflete o estado das relações de força. Esta conclusão pode parecer pessimista. Mas o direito não é um trabalho dos poetas; e me parece o contrário, como a dura escola do realismo. Ele fotografa a sociedade tal como ela é, *compreendo que esta imagem pode ser — deveria ser, sem dúvida — um encorajamento para tentar modificar*

as relações de força que a atravessam. Mas não esqueçamos, o direito, e nele compreendido o Direito Internacional, pode e deve se adaptar às mudanças sociais, porém ele é mais a consequência destas mudanças do que sua causa" (ênfase acrescida).[27]

Entre arroubos otimistas e notas pessimistas, parece-nos que a linha mediana deve prevalecer na compreensão das fases de desenvolvimento do direito internacional, mas, sobretudo, na projeção de seus desdobramentos futuros. Tendo em conta essa maneira de perceber, o tema objeto de consideração desta CPI apresenta desdobramento no campo do direito das gentes. Ele, no entanto, tem suas limitações, na linha do que proposto pelo Prof. Pellet.

A leitura do assunto pela ótica do direito internacional pode vir a ter alargamentos futuros, que, no entanto, dependem mais da ação do Poder Executivo. Assim o é pelo mandamento constitucional que entrega ao Presidente da República a condução da vida externa da Nação. Ao parlamento compete chancelar, ou não, as negociações presidenciais e controlar essa ação por meio, por exemplo, de convocação do Ministro de Estado das Relações Exteriores. Outra possibilidade se coloca no momento de aprovação do orçamento.

Nesse sentido, é importante estimular toda iniciativa no sentido de levar o assunto para foros multilaterais. Para tanto, as organizações internacionais [p. ex. ONU, Organização para a Cooperação e

---

[27] PELLET, Alain. "As novas tendências do direito internacional: aspectos 'macrojurídicos'". In: BRANT, Leonardo (Coord.). O Brasil e os novos desafios do direito internacional. Rio de Janeiro: Forenses, 2004, pp. 3-25, p. 25.

o Desenvolvimento Econômico (OCDE), União Internacional de Telecomunicações (UIT)] representam espaço mais adequado para a ampliação dos debates em torno dos temas abordados nesta CPI. É certo também que as organizações têm suas vicissitudes; não menos certo é que, apesar dos seus enormes desafios, os debates realizados em seus domínios têm o condão de deixar o assunto em evidência. Isso, por si, representa algo bastante relevante. Na linha da proposição do escritor Saramago: não devemos ter pressa, mas não podemos perder tempo.

Outra possibilidade é caminhar no sentido da positivação, por meio de tratados, de aspectos do assunto, em relação aos quais a comunidade internacional possui mais consistência e consenso em seus desígnios. A via convencional pode consolidar, por exemplo, a iniciativa brasílico-germânica apresentada à consideração da ONU. Ela pode, ainda, partir para a elaboração de arcabouço jurídico internacional de forma a dar os contornos mínimos dos assuntos aqui analisados. Partir para uma governança global e mais democrática da Internet, por exemplo. Esse caminho é mais longo, mas é também aquele em que se podem vislumbrar maiores possibilidades de êxito futuro no sentido de se combater episódios como os denunciados pelo Sr. Edward Snowden.

Parte III – ATIVIDADE DE INTELIGÊNCIA

III. 1. Segunda profissão mais antiga do mundo

Costuma-se dizer que a atividade de inteligência é tão antiga quanto a existência humana. Desde que começa a viver em comunidade e a se relacionar com outros povos, o homem precisa de informações para decidir. Nesse sentido, a inteligência tem ocupado papel de destaque entre líderes que precisem acessar conhecimentos protegidos e, ao mesmo tempo, proteger-se contra investidas de adversários.

Muitas são as definições de inteligência, que variam conforme a percepção histórica, político-institucional ou jurídica daqueles que as concebam. Nesse sentido, para os fins deste Relatório, convém destacar a chamada "percepção trina da inteligência", primeiramente formulada por Sherman Kent, ao final da década de 1940 e publicada em sua obra *Strategic Intelligence for American World Policy*.[28] De acordo com Kent, inteligência pode ser definida como **produto** (o conhecimento produzido), **organização** (os serviços secretos, estruturas funcionais que têm como missão primordial a obtenção de informações e produção de conhecimento de inteligência) e, ainda, **processo** (a atividade de reunião desses dados, seu processamento conforme metodologia específica, e disponibilização ao tomador de decisões para assessorá-lo).

---

[28] KENT, Sherman. *Strategic intelligence for American world policy*. Princeton: Princeton University Press, 1949.

Já a lei brasileira (art. 1º, § 2º, da Lei nº 9.883, de 7 de dezembro de 1999) define inteligência como:

> "a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado".

A contrainteligência, por sua vez, é compreendida como "a atividade que objetiva neutralizar a inteligência adversa" (art. 1º, § 2º, da Lei nº 9.883, de 1999).

Importante destacar que inteligência se divide, para fins didáticos e algumas vezes operacionais, em três funções, missões ou ramos: **inteligência** (relacionada à reunião e análise de informações para produção de conhecimento); **contrainteligência** (que objetiva proteger seu próprio conhecimento e neutralizar a inteligência adversa); e **operações de inteligência** (compreendidas como as ações, inclusive com recurso a meios e técnicas sigilosos, para a obtenção dos dados protegidos). As três funções são exercidas pelos serviços secretos, sendo difícil dissociá-las.[29]

Também é importante diferenciar a inteligência produzida a partir de dados obtidos de fontes humanas (chamada pelos anglo-saxões de *humint*) daquela cujos dados que compuseram seu conhecimento foram reunidos por intermédio de meios técnicos, como a interceptação telefônica, a captação de sinais eletromagnéticos e a reunião de imagens. A

---

[29] Para maiores informações sobre conceitos, escopo e categorias, funções e outros aspectos teóricos e doutrinários da atividade de inteligência, vide GONÇALVES, *Atividade de Inteligência e Legislação Correlata.* 3. ed. Niterói: Impetus, 2013.

essa segunda categoria pode-se atribuir a denominação genérica de inteligência técnica (chamada, pelos anglo-saxões, de *techint*).

Observe-se, também, que o termo "espionagem", apesar de mais presente no imaginário popular, é muito menos abrangente que inteligência. Afinal, espionagem envolve um conjunto de medidas voltadas à obtenção do dado negado, enquanto a inteligência diz respeito, repita-se, a todo um processo de obtenção desses dados e informações (inclusive com o recurso à espionagem), processamento e análise desses dados e informações, e produção de um conhecimento para assessorar o processo decisório.

Dos diversos conceitos de inteligência, é possível extrair os aspectos essenciais que diferenciam esta de quaisquer outras voltadas à produção de conhecimento. São eles:

> 1) o objetivo da inteligência, qual seja, a produção de conhecimento com o fim precípuo de assessorar o processo decisório em diferentes instâncias;
>
> 2) o caráter sigiloso do conhecimento produzido, pois este tem uma componente do chamado "dado negado", obtido por meios e métodos operacionais; e
>
> 3) o uso de metodologia própria e específica para a obtenção do dado e a produção do conhecimento de inteligência.

Onde houver processo decisório e também conhecimento a ser protegido, a inteligência deve estar presente. E isso se aplica em diferentes

níveis, no âmbito governamental e também na esfera privada. Destaque-se, ademais, que a atividade de inteligência é usada como recurso por todos os governos, tanto em regimes democráticos quanto em sistemas autoritários.

III. 2. Panorama das comunidades de inteligência pelo mundo

Para estabelecer um panorama dos diversos serviços de inteligência pelo globo, o presente Relatório teria de dedicar centenas de páginas, sem, entretanto, esgotar o assunto. Dos quase duzentos países que compõem a sociedade internacional, a maioria absoluta possui serviços de inteligência e, mais precisamente, sistemas de inteligência compondo o que se determinou chamar de comunidades de inteligência.

Portanto, sejam Estados democráticos, sejam regimes autoritários, pequenas, médias e grandes potências, todas as nações civilizadas dispõem de aparato organizacional voltado à obtenção de dados negados para a produção de conhecimentos que assessorarão o processo decisório, bem como instituições encarregadas de proteger conhecimento sensível. Parte significativa desse caleidoscópio de instituições se estrutura com base em normas e protocolos de caráter sigiloso, o que dificulta a reunião de informações a seu respeito.

É possível, entretanto estabelecer alguns padrões e certa taxonomia da estrutura de serviços secretos pelo globo. Um primeiro recorte diz respeito à distribuição do aparato de inteligência entre órgãos de inteligência interna e serviços de inteligência externa. Muitos países optam

por duas agências distintas. Exemplo disso são: Alemanha, EUA, França, Israel, Reino Unido e Rússia (vide tabela 1.1).

1.1. SERVIÇOS DE INTELIGÊNCIA PELO MUNDO		
País	**Inteligência Externa**	**Inteligência Interna/Doméstica**
Alemanha	*Bundesnachrichtendienst* - BND (Serviço Federal de Informações)]	*Bundesamt für Verfassungsschut* (BfV) (Serviço Federal para a Proteção à Constituição)
EUA	*Central Intelligence Agency* (CIA)	*Federal Bureau of Investigation* (FBI)
França	*Direction générale de la sécurité extérieure* (DGSE) (Diretoria Geral de Segurança Exterior)	*Direction centrale du renseignement intérieur* (DCRI) (Diretoria Geral de Inteligência Interna)
Israel	*Mossad – Ha-Mossad le-Modiin ule-Tafkidim Meyuhadim* (Instituto para Inteligência e Operações Especiais)	Shin Bet – *Sherut ha-Bitachon ha-Klali* (Serviço de Segurança Geral)

Reino Unido	*Secret Intelligence Service – Military Intelligence: Section Six* ou *MI6* (Serviço Secreto de Inteligência)	*Security Service – Military Intelligence: Section Five* ou *MI5* (Serviço de Segurança)
Rússia	Serviço de Inteligência Externa (SRV) (*Служба Внешней Разведки*)	Serviço Federal de Segurança (FSB) (*Федеральная служба безопасности Российской Федерации*)

Outras nações, como Argentina, Brasil e Canadá, preferem concentrar as atividades de inteligência externa e doméstica em uma única agência (vide tabela 1.2). A esse respeito, a opção está relacionada a escolhas políticas, orçamentárias e, ainda, à maneira como o país percebe suas ameaças, seu papel e sua atuação no cenário internacional.

1.2. SERVIÇOS DE INTELIGÊNCIA PELO MUNDO	
País	**Agência para Inteligência Externa e Inteligência Interna**
Argentina	*Secretaría de Inteligencia* – SI
Brasil	Agência Brasileira de Inteligência - ABIN

Canadá	*Canadian Security Intelligence Service* – CSIS (Serviço Canadense de Segurança e Inteligência)

Além dessa divisão entre campo interno e externo, as comunidades de inteligência dos países também costumam dispor de agências distribuídas de acordo com o escopo da atividade. Daí haver agências de inteligência militar e de defesa (vinculadas às Forças Armadas, por exemplo), agências de inteligência policial e de segurança pública (aquelas voltadas à inteligência financeira e à inteligência fiscal).

Assim, para as distintas atividades estatais, podem existir órgãos ou setores de inteligência na estrutura governamental voltados ao assessoramento do processo decisório nos diferentes níveis e sobre distintos assuntos. Mais recentemente, com a era da informação e o desenvolvimento tecnológico em larga escala no campo da informática, tem aumentado a preocupação dos governos com a inteligência de sinais e a atuação dos serviços secretos no ambiente virtual.

III. 3. Inteligência tecnológica (*techint*)

Inteligência técnica ou tecnológica (*techint*, no jargão estadunidense) diz respeito ao grupo de técnicas que usam mais tecnologia que fontes humanas para a reunião de dados ou informações. A inteligência técnica envolve uma série de subcategorias, com destaque para a inteligência de sinais [*signals intelligence (sigint)*], a inteligência fotográfica ou [*photographic intelligence (photint)*] de imagens [*imagery intelligence (imint)*], inteligência de comunicações [*communication*

intelligence (comint)], inteligência eletrônica [*electronics intelligence (elint)*], telemétrica [*telemetry intelligence (telint)*] e aquela relacionada à interpretação de ondas e sinais eletromagnéticos ou assinaturas físicas [*measurements and signatures intelligence (masint)*].

A inteligência de sinais (*sigint*) tornou-se o meio de reunião de dados mais prolífico do século XX[30]. Mark Lowenthal a descreve como um importante fenômeno daquele século para a inteligência[31]. Trata-se do termo genérico dado ao processo de interceptação de ondas eletromagnéticas, geralmente referidas como sinais, para uso da inteligência. Inteligência de sinais corresponde, portanto, à interpretação, processamento, análise e difusão de informações procedente de comunicações e outros sinais eletro-eletrônicos.[32]

Nesse sentido, a inteligência de sinais compreende:

- inteligência de comunicações (*comint*), a qual corresponde à interceptação – e consequente inteligência dela proveniente – de sinais de comunicações (por exemplo, mensagens de rádio) para análise e produção de conhecimento de inteligência. No século XXI, a importância da *comint* pode ser evidenciada no contexto de combate a organizações criminosas, por exemplo,

---

[30] HERMAN, Michael. *Intelligence Services in the Information Age*. London: Frank Cass Publishers, 2001.
[31] LOWENTHAL, Mark. *Intelligence: From Secrets to Policy*. Washington, D.C.: CQ Press, 2003.
[32] A importância da inteligência de sinais pode ser percebida pelo fato de que, por décadas, o maior orçamento estadunidense de Inteligência foi destinado exatamente à agência encarregada de inteligência de sinais naquele país, a *National Security Agency* (NSA).

em termos de interceptação das comunicações entre narcotraficantes na Amazônia.

- inteligência telemétrica (*telint*), relacionada à interpretação, processamento e análise de telemetria (processo ou técnica de obtenção, processamento e transmissão de dados a longa distância), ou seja de sinais de rádio que fornecem, por exemplo, informações de sensores de bordo de veículos relativos às características de um voo ou do desempenho da aeronave. *Telint* assume relevância ao permitir a obtenção de informações relacionadas às capacidades de equipamentos militares, como mísseis ou veículos de controle remoto.

- inteligência eletrônica (*elint*), que corresponde à informação técnica ou de inteligência procedente de coleta ou interceptação e processamento de radiações eletromagnéticas (exceto de comunicações) originárias de fontes como o radar. A inteligência eletrônica é útil tanto para um país rastrear elementos importantes das forças armadas de outros países – como sistemas de radares de defesa aérea, centros de comando e controle –, provendo o que se conhece como ordem de batalha eletrônica, quanto para detectar a presença de um emissor de sinais[33]. De fato, a inteligência eletrônica tem sido de grande importância na guerra moderna, cunhando-se inclusive o termo *electronic warfare.*

---

[33] SHULSKY, Abraham. *Silent warfare: understanding the world of intelligence*. New York: Brassey's, 1992.

- inteligência relacionada à interpretação de assinaturas eletromagnéticas ou sinais físicos (*masint*), uma vez que, a princípio, qualquer onda eletromagnética, emitida como parte ou como produto do funcionamento de um equipamento eletrônico (como o radar, ou até mesmo o monitor de um computador ou, ainda, os sinais emitidos por uma máquina de escrever eletrônica) está sujeita a interceptação por um receptor devidamente situado, ajustado e sensível[34]. *Masint* pode ser útil, também, na identificação de tipos de gases ou dejetos originários de uma fábrica, o que adquire grande importância, por exemplo, na assinalação de armas químicas. Um último exemplo no uso de *masint* é a identificação de características específicas de sistemas de armas[35].

Mais antiga e tão importante quanto a inteligência de sinais, a inteligência de imagens (*imagery*) ou inteligência fotográfica (*photint*), como o próprio nome esclarece, diz respeito às informações ou inteligência provenientes de fotografia e interpretação de imagens. O uso de imagens para reunir informações de inteligência é anterior mesmo à invenção da fotografia, quando espiões produziam desenhos ou pinturas que descreviam tudo que interessasse à Inteligência.

Em termos mais específicos, *imagery* relaciona-se ao uso de fotografias em larga escala para obtenção de imagens de lugares ou coisas cujo acesso direto é impossível. Inicialmente por meio de reconhecimento

---

[34] Shulsky, *op. cit.*, p. 27.
[35] Lowenthal, *op. cit.*, p. 73.

aéreo, o uso da fotografia a serviço da inteligência alcançou a era espacial, estando presente desde os primeiros satélites lançados. De fato, as necessidades de inteligência foram motivadores de pesquisa e desenvolvimento tecnológico desses equipamentos.

Convém assinalar a importância do emprego da inteligência de imagens em nossos dias, utilizada, por exemplo, na identificação de campos de treinamento e bases de terroristas ou na vigilância aérea. Nesse sentido, vale lembrar que a obtenção de imagens via satélite é complementada pelo tradicional reconhecimento aéreo – tanto por meio de aviões convencionais quanto de aeronaves não-tripuladas, as quais se desenvolveram bastante nas últimas décadas e têm sido empregadas em teatros operacionais como o Afeganistão e o Iraque[36] e, ainda, no patrulhamento de áreas sensíveis do território brasileiro, como a região de fronteira.

No que concerne à espionagem no espaço cibernético, com o desenvolvimento tecnológico das ultimas décadas, o recurso a essas práticas por governos, organizações e empresas passou a ser cada vez mais comum e, em muitos casos, com custos baixos para aqueles que as conduzem e muito altos para os que delas são alvo.

Além de governos, empresas e organizações também têm recorrido a iniciativas no espaço cibernético, o que inclui espionagem comercial e crimes cibernéticos. Há, ainda, o temor de que grupos terroristas passem a recorrer ao ambiente virtual para causar danos:

---

[36] Lowenthal, *op. cit.*, p. 70.

> "Até o momento, grupos terroristas não têm demonstrado capacidade de realizar ataques cibernéticos em pequena ou larga escala. Isso mudará no futuro. Até então, o ciberespaço tem funcionado para os terroristas majoritariamente como meio de comunicação e treinamento. Grupos de hackers (de cunho nacionalista ou não) são uma ameaça cibernética maior que grupos terroristas (que ainda não possuem capacidade de criar armas cibernéticas independentemente de Estados), mas os hackers, quando atuam com interesse político, frequentemente agem com apoio de algum governo ou grupo político organizado".[37]

Nesse sentido, constata-se também aumento na vulnerabilidade frente às chamadas "novas ameaças" (por exemplo, terrorismo e crime organizado) quando seus agentes recorrem ao ambiente virtual. Isso, associado à prática tradicional de países no jogo de poder global, faz com que os Estados devam criar mecanismos de resposta e neutralização dessas agressões.

III. 4. Estabelecimento de agências de inteligência de sinais

Diante desse novo cenário em que o ambiente virtual adquire grande relevância, diversos países decidiram estabelecer estruturas robustas no campo cibernético, entre as quais se encontram as agências de inteligência de sinais. A esse respeito, Moura e Tavares esclarecem, em Nota Técnica à Comissão de Relações Exteriores do Senado Federal, produzida em 20 de outubro de 2013, pela Tech Polis Consultoria, que:

---

[37] MOURA, Philipe; TAVARES, Ricardo. "Defesa da Democracia Brasileira no Contexto da Guerra Cibernética". Nota Técnica à Comissão de Relações Exteriores do Senado Federal, produzida em 20 de outubro de 2013, pela *Tech Polis* Consultoria.

> "No caso alemão, foi criado em 2011 o Centro Nacional de Resposta Cibernética, com o principal objetivo de coordenar as várias agências do governo da Alemanha. Este centro está subordinado ao Escritório Federal de Segurança da Informação, em relação muito próxima com o Escritório Federal de Proteção da Constituição e com o Escritório Federal de Proteção Civil e Assistência a Desastres. No caso americano, está em operação desde 2010 o Comando Cibernético dos EUA (USCYBERCOM), uma unidade vital do Comando Estratégico das Forças Armadas dos EUA. O USCYBERCOM coordena tanto o ataque quanto a defesa cibernética dos EUA, e sob ele atuam o comando cibernético do Exército, da Aeronáutica e da Marinha".[38]

Enquanto em certos países essa atividade se associa à guerra eletrônica, sendo absorvida em estruturas de defesa cibernética, normalmente no âmbito militar, em outros a inteligência de sinais se dá com uma agência civil própria. Há casos, ainda, em que órgãos civis e militares de inteligência e defesa cibernética convivem em uma mesma comunidade e se mesclam em certas missões. Essas organizações geralmente estão entre as mais secretas da comunidade de inteligência, de modo que não é possível dispor de muita informação a seu respeito.

De toda maneira, para efeitos deste Relatório, buscar-se-á apresentar algumas dessas agências de inteligência de sinais pelo mundo. Um aspecto interessante que merece destaque é o fato de que todas, indistintamente, exercem inteligência (portanto, reunião de dados, inclusive protegidos, para produção de conhecimento) e contrainteligência (proteção contra a inteligência adversa). Na tabela 1.3 estão dispostas algumas das agências de inteligência de sinais pelo globo.

---

[38] MOURA, Philipe; TAVARES, Ricardo. "Defesa da Democracia Brasileira no Contexto da Guerra Cibernética". Nota Técnica à Comissão de Relações Exteriores do Senado Federal, produzida em 20 de outubro de 2013, pela *Tech Polis* Consultoria.

1.3. SERVIÇOS DE INTELIGÊNCIA PELO MUNDO AGÊNCIAS DE INTELIGÊNCIAS DE SINAIS	
País	**Agência de Inteligência**
Austrália	*Defense Signals Directorate (DAS)*
Canadá	*Communications Security Establishment (CSE)*
EUA	*National Security Agency* (NSA)
Nova Zelândia	*Government Communications Security Bureau* (GCSB)
Reino Unido	*Government Communications Headquarters* (GCHQ)

Código de campo alterado

Criada em 1947, a *Defense Signals Directorate* (DAS) é a agência australiana que tem atribuições de realizar inteligência de sinais segurança da informação e tem como lema "Revelar o segredo deles, proteger o nosso" (*reveal their secrets, protect our own*). Dessa forma, suas duas funções principais são: 1) reunir dados de inteligência externa, analisá-los e produzir inteligência de sinais; e 2) prover o Governo australiano e suas Forças Armadas com produtos e serviços de tecnologia e segurança da informação. Atua em conjunto com o *Royal Australian Corps of Signals* em matérias de guerra eletrônica.

A contraparte neozelandesa da DAS australiana é o *Government Communications Security Bureau* (GCSB), criado em 1977, estando diretamente vinculado à pasta de Inteligência do Gabinete,

usualmente atribuída ao Primeiro Ministro. A agência tem como missão garantir a segurança nacional da Nova Zelândia, provendo: 1) segurança da informação e segurança cibernética; 2) inteligência externa para assessoramento ao processo decisório; 3) auxílio na proteção de infraestruturas críticas contra ameaças cibernéticas; 4) cooperação e assistência tecnológica a outras agências governamentais neozelandesas. Atua em inteligência de sinais, inteligência geoespacial e garantia da informação (*information assurance*). Note-se que é a agência de inteligência externa por excelência daquele país.

A agência de inteligência de sinais do Reino Unido é o *Government Communications Headquarters* (GCHQ). Sucedendo, em 1946, à *Government Code and Cypher School*, por sua vez criada em 1919, o GCHQ tem por missão proteger o Reino Unido e seus cidadãos contra pessoas grupos e países que lhes representem ameaça, operando na área de comunicações e inteligência de sinais. É organização tradicionalmente das mais secretas da comunidade de inteligência do país, e opera sob o controle direto do Gabinete, por meio do *Joint Intelligence Committee*.

O GCHQ atua em estreita parceria com outras agências governamentais e, ainda, com empresas e instituições privadas britânicas, como universidades e centros de pesquisa. A agência desenvolve programas na área de proteção ao conhecimento. Em novembro último, o Diretor do GCHQ compareceu a audiência na Comissão de Segurança e

Inteligência do Parlamento britânico, em sessão em que pela primeira vez foi possível a cobertura da imprensa[39].

Nos EUA, a principal agência encarregada de inteligência de sinais é a *National Security Agency* (NSA). Umas das principais organizações de inteligência estadunidense, tanto em orçamento quanto em pessoal, a NSA está na estrutura do Departamento de Defesa [*Department of Defense* (DoD)] e se reporta ao Diretor Nacional de Inteligência [*Director of National Intelligence* (DNI)].

Criada em 1952, a NSA é órgão central de uma série de sistemas que lidam com inteligência de sinais, proteção e garantia da informação, interceptação de comunicações, criptografia e criptoanálise. Devido ao seu alto grau de sigilo, durante muitos anos o Governo dos EUA negou sua existência. A agência tem atuado na reunião de dados e informação em âmbito interno e externo, desde que consideradas de interesse da segurança nacional dos EUA. Exatamente por isso, seu papel passou a ser questionado quando se tornou público seu envolvimento em práticas mais intrusivas para obter informações sobre cidadãos e empresas estadunidenses.

Com as denúncias de Edward Snowden, questionou-se a atuação da NSA em interceptar comunicações em operações de espionagem contra Governos, autoridades públicas, empresas e cidadãos estrangeiros, inclusive os provenientes de nações consideradas "amigas" dos EUA. O

---

[39] Para maiores Informações, vide a página referente à matéria no website da Comissão do Parlamento in http://isc.independent.gov.uk/news-archive/7november2013-1. Acesso em: 30/11/2013.

argumento da Casa Branca é que isso teria sido feito no contexto da luta contra o terrorismo. A prática, porém de espionar autoridades públicas estrangeiras e de, além disso, reunir informações de caráter econômico e comercial sobre Governos e empresas de outros países gerou reação internacional contra a NSA e o Governo dos EUA.

Uma vez que o modelo de serviço secreto brasileiro toma por base a experiência canadense, convém aqui fazer observações mais detalhadas sobre a agência canadense de inteligência de sinais, o *Communications Security Establishment* (CSE).

Considerada a mais secreta organização de inteligência do Canadá, o *Communications Security Establishment* (CSE) é a agência de criptologia canadense. Ligado ao Ministério da Defesa (DND), e regulado pelo *National Defense Act,* de 1985, a CSE é responsável por duas funções básicas no Governo canadense: produzir inteligência de sinais em apoio às políticas externa e de defesa; proteção da informação e do conhecimento eletrônico e das comunicações. Para alcançar esses objetivos, o CSE dispõe de métodos e tecnologias avançados. A título de esclarecimento, a equivalente do CSE nos EUA é a NSA, com a qual atua em estreita parceria[40].

As origens do CSE remontam à II Guerra Mundial. Em 1975, a agência foi transferida para o DND. Entretanto, o Governo do Canadá não reconhecia publicamente a existência da agência até 1983, e só veio a

---

[40] Lembre-se que o Canadá é membro do UKUSA e que, além da NSA, é estreito o relacionamento entre a CSE e GCHQ britânico, a DSD australiana e GCSB neozelandês.

regulamentá-la em 2001. O Chefe do CSE, responsável pelo controle e gerenciamento do órgão, reporta-se diretamente ao Vice-Ministro da Defesa para assuntos financeiros e administrativos, e ao Assessor de Segurança Nacional para questões operacionais e diretrizes políticas.

Diferentemente do serviço secreto canadense, o CSIS, e da Real Polícia Montada do Canadá [*The Royal Canadian Mounted Police* (RCMP)], o CSE não coleta inteligência de fontes humanas. Repita-se, sua tarefa é obter dados para produção de conhecimento de inteligência a partir de sinais – emissões eletrônicas, comunicações por diferentes meios. Assim, de acordo com o *National Defense Act*, compete ao CSE:

- adquirir e utilizar informação proveniente da infraestrutura mundial de informação – por exemplo, de sinais de comunicação –, com o objetivo de fornecer inteligência externa, em conformidade com as prioridades do Governo do Canadá em matéria de inteligência;

- assessorar o Governo fornecendo-lhe conhecimento e outros serviços com o objetivo de proteger a informação eletrônica e as infraestruturas importantes para os interesses canadenses;

- prover assistência técnica e operacional aos órgãos federais encarregados da aplicação da lei (*law enforcement*) e da garantia da segurança, nos termos da lei.

Questão importante nos últimos anos é se o CSE, em meio à política antiterrorista, estaria sendo usado para reunir informações sobre

cidadãos canadenses, o que é proibido por lei. Antes de 2001, a agência era mesmo proibida de interceptar comunicações em que um alvo no exterior enviasse ou recebesse do Canadá.

Com as normas de 2001, tem-se a possibilidade de interceptação de "comunicações privadas", entendidas como toda

> "comunicação oral ou telecomunicação cujo autor ou destinatário se encontre no Canadá, e que esteja em circunstâncias em que seu emissor ou receptor tenha razoável convicção de que não estão sendo interceptadas por um terceiro, aí compreendida a comunicação radiotelefônica tratada eletronicamente ou qualquer outra em que se busque obstaculizar sua recepção clara por terceiro".[41]

O Ministro da Defesa pode autorizar o CSE a interceptar comunicações privadas com o único propósito de obter inteligência externa, desde que a interceptação se direcione a um ente estrangeiro localizado fora do território canadense. Quaisquer outras comunicações interceptadas que não se enquadrem nessa categoria e estejam explícitas na autorização do Ministro devem ser destruídas.

Naturalmente, o CSE deve compartilhar com o CSIS e a RCMP sua inteligência externa de segurança nacional que tenha relação com assuntos domésticos e de inteligência externa. Por exemplo, se a agência interceptar a comunicação de um terrorista no estrangeiro com alguém no Canadá, e isso tenha algum valor para a inteligência, deve

---

[41] Definição estabelecida pelo Código Penal do Canadá (*Criminal Code*), seção 183. Interessante observar que emissões normais de rádio não se encontram nessa categoria – uma vez que podem ser recebidas por terceiros – bem como comunicações por *pagers* (*Arar Commission Report, Dec/2006*, p. 218, n. 57).

reportar ao CSIS. O mesmo ocorre em relação a outras agências e departamentos. Além disso, são produzidos relatórios periódicos e específicos, difundidos a todos ou a alguns membros da comunidade de segurança e inteligência. Há, ainda, documentos ostensivos que são disponibilizados na *home page* da agência[42].

Também compete ao CSE assessorar os órgãos de aplicação da lei, como a RCMP e outras autoridades policiais. Essa assistência é eminentemente técnica. Assim é que o CSE auxilia a RCMP com programas de investigação criminal, equipamentos ou mesmo na decodificação de material criptografado.

No que concerne à proteção ao conhecimento, é atribuição do CSE prover assessoramento estratégico e técnico para a defesa dos sistemas de informações críticas e bancos de dados do Governo. A agência é responsável, em parceria com outros órgãos, pelo assessoramento técnico em criptografia, segurança cibernética, equipamentos e segurança das comunicações.

A atuação do CSE e sua importância na comunidade de segurança e inteligência do Canadá têm crescido significativamente. A partir de 2002, a agência cresceu em termos de recursos e pessoal, fortalecendo a área de contraterrorismo. Nesse sentido, o CSE trabalha em estreita parceria com as Forças Armadas e os órgãos de segurança nacional. O recurso à tecnologia e à interceptação das comunicações é necessidade premente da inteligência, e isso se aplica tanto para as ameaças tradicionais

---

[42] Vide http://www.cse-cst.gc.ca/publications/publications-e.html. Acesso em: 06/11/2013.

quanto para as novas ameaças, aí incluídos o crime organizado e o terrorismo transnacional. No Canadá, o CSE tem papel fundamental nesses processos.

Também medidas de cooperação foram desenvolvidas pelos países ocidentais, com destaque para projetos como o UKUSA e o Echelon. A aliança de países anglófilos desenvolvidos – Austrália, Canadá, EUA, Nova Zelândia e Reino Unido –, conhecida como *UKUSA* ou *Five Eyes*, formou-se a partir da aproximação entre EUA e Grã-Bretanha durante a II Guerra Mundial para o desenvolvimento de um sistema de coleta/busca de dados e produção de informações baseado em inteligência de sinais.

Iniciada nos anos 1940, a UKUSA continua existindo até nossos dias, dela fazendo parte, a *National Security Agency* (NSA – EUA), o *Government Communications Security Bureau* (GCSB – Nova Zelândia), a *Defense Signals Directorate* (DAS – Austrália), a *Communications Security Establishment* (CSE – Canadá), e os *Government Communications Headquarters* (GCHQ – Grã-Bretanha). O acrônimo resulta das siglas, em inglês, dos países líderes do projeto, Reino Unido (UK) e EUA (USA)[43]. O *Echelon*, por sua vez, seria um projeto ultrassecreto de inteligência de sinais desenvolvido pelos EUA em parceria com países europeus[44].

---

[43] Sobre o assunto, vide Jeffrey Richelson & Desmond Ball, *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries*. London: Allen & Unwin, 1985.

[44] Sobre o assunto, vide o estudo de Duncan Campbell para o Parlamento Europeu, "The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband ulti-language leased or common carrier systems, and its applicability to COMINT targetting and selection,

Diante das características de outros serviços de inteligência de sinais pelo mundo, é importante que seja evidenciado que o estabelecimento de uma agência de inteligência de sinais pelo Brasil envolve não somente proteção ao conhecimento e outras medidas de contrainteligência, mas, ainda, a estruturação de um aparato que permita ao País obter dados e informações de interesse nacional por meio desses meios tecnológicos de ponta. Nesse sentido, ter-se-ia mais uma instituição fazendo parte do Sistema Brasileiro de Inteligência, sobre o qual se tratará a seguir.

III. 5. Organização da atividade de inteligência no Brasil

A atividade de inteligência no Brasil tem como marco o ano de 1927, com a instituição, pelo Presidente Washington Luís, do Conselho de Defesa Nacional – que tinha uma secretaria cuja função, entre outras, era assessorar o Chefe de Estado em assuntos de informações e contra-informações. A partir de então, a comunidade de inteligência passou por altos e baixos, cresceu, tornou-se influente e alcançou as mais altas esferas de poder na República, com dois supremos mandatários dela provenientes[45].

---

including speech recognition".Luxemburgo: European Parliament - Directorate General for Research, 1999 - PE 168.184/Vol 2/5.

[45] Os presidentes Emílio Garrastazu Médici (1905-1985) e João Baptista de Oliveira Figueiredo (1918-1999), que governaram o Brasil entre 1969 e 1974, e 1979 e 1985, respectivamente, foram chefes do Serviço Nacional de Informações (SNI), saindo desse cargo para ocupar a Presidência da República, por eleição indireta. Para um breve histórico da atividade de inteligência no Brasil, vide artigo, de Joanisval Gonçalves,

O apogeu da atividade de inteligência no Brasil foi a época do Serviço Nacional de Informações (SNI) e o do Sistema Nacional de Informações (SISNI), quando os serviços secretos tinham grande influência junto às mais altas esferas de governo. Entretanto, com o poder, veio o estigma dos serviços secretos associados ao período militar e das condutas arbitrárias e ilegais de algumas pessoas ligadas à então comunidade de informações. E a sociedade brasileira passou a ver a atividade de inteligência como intimamente associada à repressão.

Com a extinção do SNI e do SISNI em 1990, a atividade de inteligência entraria em um período de obscuridade. A comunidade de informações foi desmantelada, servidores civis foram redistribuídos, aposentados ou demitidos, os militares que trabalhavam nos órgãos de inteligência reconduzidos a suas respectivas Forças. Arquivos foram perdidos ou destruídos e houve uma ruptura na memória organizacional de muitos serviços secretos que dificilmente poderia ser recuperada. Esse cenário começou a mudar a partir de meados da década de 1990, com a proposta, no Governo Fernando Henrique Cardoso, de criação de uma agência de inteligência e de um sistema de inteligência que operassem de forma consentânea com o regime democrático, em defesa do Estado e da sociedade e em estrito cumprimento da lei.

"Visões do Jogo: Percepções das Sociedades Canadense e Brasileira sobre a Atividade de Inteligência" [in: SWENSON, Russel & LEMOZY, Susana (coord.), *Democratización de la función de inteligencia*. Washington, DC: National Defense University College Press, 2009. Vide, também, STEPAN, Alfred. *Os Militares: da Abertura à Nova República*. Rio de Janeiro: Paz e Terra, 1996; e ANTUNES, Priscila C. B., *SNI & Abin: uma leitura da atuação dos serviços secretos brasileiros ao longo do século XX*. Rio de Janeiro: Editora FGV, 2002.

Em 7 de dezembro de 1999, foi promulgada a Lei nº 9.883, que criou a Agência Brasileira de Inteligência (ABIN) e instituiu o Sistema Brasileiro de Inteligência (SISBIN), o qual "integra as ações de planejamento e execução das atividades de inteligência do País, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional" (art. 1º). O Sistema é "responsável pelo processo de obtenção, análise e disseminação da informação necessária ao processo decisório do Poder Executivo, bem como pela salvaguarda da informação contra o acesso de pessoas ou órgãos não autorizados" (art. 2º, § 1º).

A referida lei estatui, em seu art. 1º, § 1º, como fundamentos do Sistema "a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana". Também estabelece que o SISBIN deve "cumprir e preservar os direitos e garantias individuais e demais dispositivos da Constituição Federal, os tratados, convenções, acordos e ajustes internacionais em que a República Federativa do Brasil seja parte ou signatário, e a legislação ordinária".

O art. 2º do diploma normativo mencionado dispõe que "os órgãos e entidades da administração pública federal que, direta ou indiretamente, possam produzir conhecimentos de interesse das atividades de inteligência, em especial aqueles responsáveis pela defesa externa, segurança interna e relações exteriores", constituirão o SISBIN, "na forma de ato do Presidente da República". Esse ato é o Decreto nº 4.376, de 13 de setembro de 2002, que estabelece a seguinte composição do Sistema:

> I – Casa Civil da Presidência da República, por meio de sua Secretaria Executiva;

II – Gabinete de Segurança Institucional da Presidência da República - GSI, órgão de coordenação das atividades de inteligência federal;

III – Agência Brasileira de Inteligência - ABIN, do Gabinete de Segurança Institucional da Presidência da República, como órgão central do Sistema;

IV – Ministério da Justiça, por meio da Secretaria Nacional de Segurança Pública, da Diretoria de Inteligência Policial do Departamento de Polícia Federal, do Departamento de Polícia Rodoviária Federal, do Departamento Penitenciário Nacional e do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, da Secretaria Nacional de Justiça;

V – Ministério da Defesa, por meio da Subchefia de Inteligência Estratégica, da Assessoria de Inteligência Operacional, da Divisão de Inteligência Estratégico-Militar da Subchefia de Estratégia do Estado-Maior da Armada, do Centro de Inteligência da Marinha, do Centro de Inteligência do Exército, do Centro de Inteligência da Aeronáutica, e do Centro Gestor e Operacional do Sistema de Proteção da Amazônia;

VI – Ministério das Relações Exteriores, por meio da Secretaria-Geral de Relações Exteriores e da Coordenação-Geral de Combate aos Ilícitos Transnacionais;

VII – Ministério da Fazenda, por meio da Secretaria-Executiva do Conselho de Controle de Atividades Financeiras, da Secretaria da Receita Federal do Brasil e do Banco Central do Brasil;

VIII – Ministério do Trabalho e Emprego, por meio da Secretaria-Executiva;

IX – Ministério da Saúde, por meio do Gabinete do Ministro de Estado e da Agência Nacional de Vigilância Sanitária – ANVISA;

X – Ministério da Previdência Social, por meio da Secretaria-Executiva;

XI – Ministério da Ciência e Tecnologia, por meio do Gabinete do Ministro de Estado;

XII – Ministério do Meio Ambiente, por meio da Secretaria-Executiva e do Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis – IBAMA;

XIII – Ministério da Integração Nacional, por meio da Secretaria Nacional de Defesa Civil;

XIV – Controladoria-Geral da União, por meio da Secretaria-Executiva.

XV – Ministério da Agricultura, Pecuária e Abastecimento, por meio de sua Secretaria-Executiva;

XVI – Secretaria de Aviação Civil da Presidência da República, por meio de sua Secretaria-Executiva;

XVII – Ministério dos Transportes, por meio de sua Secretaria-Executiva e do Departamento Nacional de Infraestrutura de Transportes – DNIT;

XVIII – Ministério de Minas e Energia, por meio de sua Secretaria-Executiva; e

XIX – Ministério das Comunicações, por meio de sua Secretaria-Executiva.

Os Ministérios dos Transportes, das Minas e Energia e das Comunicações passaram a integrar o SISBIN a partir de 10 de dezembro de 2013, o que revela a preocupação do Estado brasileiro com as vulnerabilidades dessas pastas. Fundamental, assim, que façam parte do Sistema e disponham de setores e mecanismos de contrainteligência para fazer frente às ações externas adversas.

Destaque-se, ainda, que, "mediante ajustes específicos e convênios, ouvido o competente órgão de controle externo da atividade de inteligência, as unidades da Federação poderão compor o Sistema Brasileiro de Inteligência" (art. 2º, § 2º, da Lei nº 9.883, de 1999). Entretanto, desde sua criação, em 1999, nenhum ente federado realizou esses ajustes específicos ou convênios na forma do Decreto nº 4.376, de

2002, integrando-se expressamente à estrutura do SISBIN. Não obstante, na última década foram desenvolvidos subsistemas regionais e estaduais de inteligência de segurança pública, os quais reúnem a comunidade de inteligência local e entes das três esferas (federal, estadual e municipal), da Administração direta, indireta e até de segmentos do setor privado.

Note-se, ainda, que foram estabelecidos, além dos supracitados, um Subsistema de Inteligência de Segurança Pública (SISP), previsto no Decreto nº 3.695, de 21 de dezembro de 2000, e um Sistema de Inteligência de Defesa (SINDE), criado pela Portaria nº 295, de 3 junho de 2002, do Ministério da Defesa.

Integram o SISP os Ministérios da Justiça, da Fazenda, da Defesa e da Integração Nacional e o Gabinete de Segurança Institucional da Presidência da República, dele também podendo fazer parte os órgãos de Inteligência de Segurança Pública dos Estados e do Distrito Federal. O órgão central desse Subsistema é a Secretaria Nacional de Segurança Pública do Ministério da Justiça (SENASP).

Cabe aos integrantes do SISP, "no âmbito de suas competências, identificar, acompanhar e avaliar ameaças reais ou potenciais de segurança pública e produzir conhecimentos e informações que subsidiem ações para neutralizar, coibir e reprimir atos criminosos de qualquer natureza". Assim como acontece com o SISBIN, o Decreto nº 3.695, de 2000, estabeleceu um Conselho Especial do Subsistema, "órgão de deliberação coletiva, com a finalidade de estabelecer normas para as atividades de inteligência de segurança pública, que terá a seguinte composição" (art. 3º):

I – como membros permanentes, com direito a voto:

a) o Secretário Nacional de Segurança Pública, que o presidirá;

b) um representante do órgão de Inteligência do Departamento de Polícia Federal e outro da área operacional da Polícia Rodoviária Federal;

c) dois representantes do Ministério da Fazenda, sendo um do Conselho de Controle de Atividades Financeiras (COAF) e outro da Coordenação Geral de Pesquisa e Investigação (COPEI) da Secretaria da Receita Federal;

d) dois representantes do Ministério da Defesa;

e) um representante do Gabinete de Segurança Institucional da Presidência da República;

f) um representante da Defesa Civil do Ministério da Integração Nacional; e

g) um representante da Agência Brasileira de Inteligência.

II – como membros eventuais, sem direito a voto, um representante de cada um dos órgãos de Inteligência de Segurança Pública dos Estados e do Distrito Federal.

O SISP, assim como os subsistemas regionais e estaduais, têm sido de extrema importância para integrar os órgãos de segurança e inteligência na área de Segurança Pública, particularmente no que concerne ao desenvolvimento de doutrina e metodologia de inteligência para o combate ao crime organizado.

O Sistema de Inteligência de Defesa (SINDE), por sua vez, na forma do art. 1º da Portaria-MD nº 295, e 2002, "integra as ações de planejamento e execução da Atividade de Inteligência de Defesa (AID), com a finalidade de assessorar o processo decisório no âmbito do Ministério da Defesa (MD)". Para esse fim, reúne os "órgãos de inteligência de mais alto nível do MD e das Forças Armadas, especificados nas Normas de Funcionamento do Sistema de Inteligência de Defesa" (NOSINDE) e "fundamenta-se em ligações sistêmicas entre seus elementos, sem vínculos de subordinação".

Como órgão central do SINDE, o art. 5º da Portaria estabelece o Departamento de Inteligência Estratégica (DIE), da Secretaria de Política, Estratégia e Assuntos Internacionais do MD, atual Subchefia de Inteligência Estratégica (SCIE), da Chefia de Assuntos Estratégicos (CAE) do Estado-Maior Conjunto das Forças Armadas (EMCFA). Também dispõe de um Conselho Consultivo (CONSECON), integrado pelos oficiais-generais que chefiam ou dirigem os Órgãos de Inteligência especificados nas NOSINDE. A Portaria prevê, ainda, em seu art. 10, que os órgãos de

inteligência do SINDE ligar-se-ão entre si e com os órgãos do SISBIN, de acordo com as NOSINDE[46].

Essas estruturas são reproduzidas em outros campos da inteligência governamental. Assim, tem-se um conjunto de sistemas e subsistemas que permite integração entre os vários órgãos que realizam inteligência. O maior problema dessa integração diz respeito a sua efetividade, podendo ocorrer que os órgãos se ressintam em compartilhar informação. Daí a importância de mecanismos de controle que permitam o acompanhamento das atividades da comunidade de inteligência.

No Brasil, portanto, há um sistema de inteligência composto por inúmeros órgãos, no qual a Agência Brasileira de Inteligência (ABIN) é o ente central. Esse sistema é também conhecido como comunidade de inteligência. A ABIN, entretanto, não tem qualquer ingerência sobre esses órgãos. Há, ainda, inúmeras empresas que realizam "inteligência privada", sem qualquer controle.

A Lei nº 9.883, de 1999, também dispõe sobre as competências da ABIN, órgão central do Sistema. A Agência tem a seu cargo "planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País, obedecidas à política e às diretrizes superiormente traçadas nos termos desta Lei" (art. 3º). E, ainda, compete à ABIN, na forma do art. 4º da referida Lei:

---

[46] Sobre o SINDE, vide SÁ JUNIOR, G.; MOTA, R. M. Sugestões para a Inteligência de Defesa deste século., Revista das Ciências Militares (Coleção Meira Mattos), vol. 3, nº 27, 3º quadrimestre. Rio de Janeiro, 2012.

I - planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República;

II - planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade;

III - avaliar as ameaças, internas e externas, à ordem constitucional;

IV - promover o desenvolvimento de recursos humanos e da doutrina de inteligência, e realizar estudos e pesquisas para o exercício e aprimoramento da atividade de inteligência.

Outro aspecto importante relacionado à legislação, à estrutura e ao funcionamento da inteligência no Brasil diz respeito à previsão, no art. 5º da Lei nº 9.883, de 1999, de uma Política Nacional de Inteligência (PNI), a ser fixada pelo Presidente da República, que norteará a atuação dos serviços secretos brasileiros. A Lei prevê, ainda, que antes de ser fixada pelo Chefe do Executivo, a PNI deverá ser submetida à apreciação do órgão de controle externo do Congresso Nacional. Em dezembro 2009, projeto de PNI foi encaminhado ao Poder Legislativo,[47] ali apreciado e

[47] Mensagem (CN) nº 198, de 2009 (Mensagem nº 997, de 09/12/2009, na origem), que encaminha ao Congresso Nacional, nos termos do parágrafo único do art. 5º, e do § 1º

devolvido ao Poder Executivo em agosto de 2010. Até a conclusão do presente Relatório, o País ainda não dispunha de uma PNI, uma vez que o Poder Executivo não a havia publicado.

Decorridos quatorze anos da Lei nº 9.883, de 1999, a comunidade de inteligência é ainda recebida com reservas pela sociedade em geral e pelos tomadores de decisão. Os serviços secretos operam com grande dificuldade, tanto devido à falta de respaldo legal quanto pelo escasso orçamento, tendo, ainda, que lidar com a desconfiança da população e de seus clientes, os políticos e os administradores públicos dos altos escalões. O Sistema tem dificuldade de integração e mudanças são necessárias, sobretudo em um contexto em que "novas ameaças" se evidenciam e em um momento em que o Brasil se desenvolve e busca aumentar seu protagonismo em âmbito internacional. Em outras palavras, há muitos problemas, e eles têm que ser resolvidos.

III. 6. Crise da inteligência

Ao analisar a situação da atividade de inteligência no Brasil, Gonçalves destaca os problemas e dificuldades atualmente enfrentados pela comunidade de inteligência no País[48], quais sejam:

---

do art. 6º da Lei nº 9.883, de 7 de dezembro de 1999, o texto da proposta da Política Nacional de Inteligência.

[48] GONÇALVES, Joanisval B. "Brasil, serviços Secretos e Relações Internacionais: conhecendo um pouco mais sobre o Grande Jogo". *In*: SILVA FILHO, Edson Benedito da; MORAES, Rodrigo Fracalossi de (orgs.). *Defesa Nacional para o Século 21*. Rio de Janeiro: IPEA, 2012, pp. 295-316

"1) a falta mandato claro e de apropriada distribuição de competências entre os distintos órgãos do SISBIN;

2) dificuldades de integração e cooperação entre os entes do Sistema;

3) ausência de uma autoridade central que efetivamente coordene os diversos segmentos;

4) falta de legislação que estabeleça mecanismos e protocolos de cooperação;

5) ausência de legislação que dê respaldo à atividade e ao pessoal de inteligência e que proteja o conhecimento sigiloso sob a guarda dos serviços secretos;

6) fragilidade orçamentária; e

7) ausência de mecanismos efetivos de controle, particularmente de controle externo da atividade de inteligência".

Todos esses problemas estão relacionados à ausência de uma cultura de inteligência entre os brasileiros. Pouco se conhece e pouco se discute sobre os serviços secretos e seu trabalho. De fato, quase três décadas após o fim do período militar no Brasil, a atividade de inteligência ainda é vista como algo ilegítimo e relacionado à ditadura[49].

---

[49] Para análise mais detalhada desses problemas, vide, de Joanisval Gonçalves, "O que fazer com nossos espiões? Considerações sobre a atividade de inteligência no Brasil",

Uma consequência da falta de cultura de inteligência no Brasil é o despreparo dos brasileiros (tanto na iniciativa privada quanto no setor público) para fazer frente a ameaças reais como a espionagem (a serviço de outros Estados ou de outras organizações), a atuação de organizações criminosas e mesmo de grupos terroristas. Com isso a vulnerabilidade do Brasil diante desse tipo de ameaça é enorme. Outra consequência é a falta de investimento no setor e a ausência de mecanismos legais e institucionais que viabilizem o trabalho do pessoal de inteligência.

Os acontecimentos que motivaram esta CPI assinalam, portanto, o despreparo do Poder público no Brasil para fazer frente às ações de inteligência de outros Governos e organizações. Afinal, incursões como as que supostamente ocorreram contra autoridades e instituições brasileiras continuarão a ocorrer e passarão despercebidas caso não se desenvolva, com urgência, aparato de contrainteligência e de mecanismos de proteção ao conhecimento para fazer frente a essas ameaças.

No campo da inteligência de sinais e da segurança cibernética[50], por exemplo, os investimentos ainda são ínfimos. Em exposição na 6ª Reunião desta CPI, o Chefe do Centro de Defesa

---

in: MENEGUIN, Fernando (org.), *Agenda Legislativa para o Desenvolvimento Nacional*. Brasília: Senado Federal, Subsecretaria de Edições Técnicas, 2011, pp. 259-280.

[50] De acordo com a Portaria nº 45, de 8 de setembro de 2009 do Grupo Técnico de Segurança Cibernética, entende-se por segurança cibernética "a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infra-estruturas críticas". Sobre o assunto, vide o *Livro Verde da Segurança Cibernética no Brasil*, de Raphael Mandarino Junior e Claudia Canongia (orgs.). Disponível em: http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf . Acesso em: 08/11/2013.

Cibernética do Exército Brasileiro (CDCiber), General-de-Divisão José Carlos dos Santos, assinalou as dificuldades orçamentárias de sua unidade, o principal centro do Governo brasileiro nessa área:

> "Só no Ministério da Defesa, nós já fizemos o levantamento da necessidade imediata: só para fazermos progredir alguns programas que acelerem a implantação da defesa cibernética no âmbito do Ministério, nós teríamos que dobrar o orçamento inicialmente previsto para o setor. O orçamento inicialmente previsto para implantação do setor cibernético dentro do Exército, que é a Força coordenadora e integradora da área, foi de R$400 milhões. Já no primeiro ano orçamentário, de 2012, dos R$81,5 milhões previstos, foram apenas alocados R$61 milhões. No segundo ano orçamentário, que é o ano corrente – estavam previstos, no plano inicial, R$110 milhões –, já tivemos uma redução, por motivos que todos os senhores e senhoras acompanham, para cerca de R$90 milhões."

Esse cenário se evidencia em outros setores do Estado brasileiro que lida com inteligência e segurança. A título de exemplo, a Lei Orçamentária Anual (LOA) de 2012 estabeleceu o orçamento da ABIN em R$ 527,7 milhões, dos quais R$ 467,18 milhões tinham como destinação pessoal e encargos sociais, R$ 55,66 milhões para outras despesas correntes e R$ 4,86 milhões para investimentos (vide quadro com o orçamento da ABIN segundo o Projeto de Lei Orçamentária 2013)[51]. Como comparação, o orçamento oficial da comunidade de inteligência dos EUA (desconsiderando-se despesas de pessoal) para o ano fiscal de 2012/2013 foi de US$ 52,6 bilhões, segundo divulgado por Edward Snowden e

[51] BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Orçamento Federal. *Orçamentos da União exercício financeiro 2013: projeto de lei orçamentária.* Brasília, 2012.

publicado no jornal *The New York Times*[52]. Apenas para a NSA teriam sido destinados US$ 10,8 bilhões, enquanto outros US$ 14,7 bilhões iriam para a CIA e US$ 10,3 bilhões para o *National Reconnaissance Office*[53].

Orçamento da Agência Brasileira de Inteligência - 2013

Órgão: 20000 - Presidência da República
Unidade: 20118 - Agência Brasileira de Inteligência - ABIN

Quadro Síntese

Código / Especificação		Lei+Créditos 2011	Empenhado 2011	PLO 2012	LOA 2012
Total		464.280.626	463.079.997	528.488.863	527.714.658
Programa					
0089	Previdência de Inativos e Pensionistas da União	112.805.229	112.805.185	131.243.845	131.243.8
0541	Inteligência Federal	370.475.397	360.274.812		
0999	Reserva de Contingência	11.000.000			
2101	Programa de Gestão e Manutenção da Presidência da República			397.240.018	396.468.7
Função					
00	Segurança Pública	370.475.397	360.274.812	397.240.018	396.468.7
09	Previdência Social	112.805.229	112.805.185	131.243.845	131.243.8
Subfunção					
122	Administração Geral	324.385.057	319.459.913	370.484.478	369.954.2
126	Formação de Recursos Humanos	3.000.000	999.896	1.100.000	1.100.0
183	Informação e Inteligência	24.290.000	13.262.802	12.870.000	12.839.0
272	Previdência do Regime Estatutário	112.805.229	112.805.185	131.243.845	131.243.8
301	Atenção Básica	3.704.022	3.652.441	3.944.542	3.944.5
306	Alimentação e Nutrição	8.176.934	8.171.379	8.360.000	8.360.0
331	Proteção e Benefícios ao Trabalhador	844.154	618.822	840.000	840.0
365	Educação Infantil	163.230	138.585	158.000	158.0
572	Desenvolvimento Tecnológico e Engenharia	1.800.000	1.800.000	1.475.000	1.475.0
Grupo de Despesa					
1	Pessoal e Encargos Sociais	407.680.286	405.186.312	467.155.321	467.155.3
3	Outras Despesas Correntes	55.190.340	53.812.634	56.435.542	55.664.3
4	Investimentos	19.410.000	4.071.051	4.898.000	4.644.9

Fonte	1-PES	2-JUR	3-ODC	4-INV	5-IFI	6-AMT	9-RES
100	302.504.662		61.000.860	5.053.000			
156	41.783.328						
169	79.337.672						
Total	423.625.662		61.000.860	5.053.000			

Fonte: Brasil. Orçamentos da União – Exercício Financeiro 2013 - Projeto de Lei Orçamentária

---

[52] "*New Leaked Document Outlines U.S. Spending on Intelligence Agencies*", The New York Times, August 29, 2013. Disponível em http://www.nytimes.com/2013/08/30/us/politics/leaked-document-outlines-us-spending-on-intelligence.html?hp&pagewanted=all&_r=0. Acesso em: 10/10/2013.

[53] Sobre o assunto, interessante destacar a cobertura do jornal *The Washington Post*, *Inside the 2013 U.S. intelligence "black budget"*, disponível online em http://apps.washingtonpost.com/g/page/national/inside-the-2013-us-intelligence-black-budget/420/ . Acesso em: 22/11/2013.

III. 7. Aprimoramento da inteligência no Brasil

Assinalados os obstáculos relacionados à atividade de inteligência, cabem algumas considerações sobre como aprimorar essa atividade no Brasil. A esse respeito, um capítulo da obra *Agenda Legislativa para o Desenvolvimento Nacional*, publicada em 2011 pelo Senado Federal trazia importantes recomendações. Primeiramente, destacava-se a necessidade de que o SISBIN fosse reestruturado "para permitir cooperação e integração mais eficazes, eficientes e efetivas entre seus membros". Era um momento em que, em virtude da proposta de PNI apreciada pelo Poder Legislativo, discutia-se "a criação de subsistemas de inteligência voltados para a defesa nacional, a segurança pública, a inteligência econômico-financeira e, naturalmente, a inteligência estratégica (ou de Estado)".

Também se propunha um mandato claro para os mais de vinte órgãos da comunidade de inteligência da Administração Pública federal:

> "O estabelecimento de subsistemas pressupõe maior especialização entre os órgãos do SISBIN. Para que isso ocorra, é fundamental que seja estabelecido mandato claro para cada um dos órgãos e unidades que compõem o Sistema, bem como o âmbito de atuação e seus limites, de modo que um não intervenha na esfera de atuação do outro. Essa especialização só seria possível se a ela estivessem associados mecanismos efetivos, eficientes e eficazes de cooperação e, ainda, regras claras para integração do conhecimento produzido pelos distintos setores. Sem essa delimitação de competências e áreas de atuação um serviço acabará interferindo nos assuntos do outro e poderá haver choque entre eles".[54]

---

[54] GONÇALVES, Joanisval B.. "O que fazer com nossos espiões? Considerações sobre a atividade de inteligência no Brasil", *op. cit.*.

Propunha-se, ademais, a criação de forças-tarefa, o estabelecimento de uma única escola de formação da comunidade ou de estreita cooperação e parcerias entre as escolas existentes[55], e a instituição de "salas de crise" ou "centros de integração" nos principais órgãos.

Outro aspecto relacionado ao aprimoramento da inteligência no Brasil, segundo o texto da *Agenda Legislativa*, "passa também pelo estabelecimento de um arcabouço legislativo que dê respaldo à atividade e garantia aos profissionais que nela atuam em defesa do Estado e da sociedade". Daí necessidade de lei que regulamente, de forma clara, "a atividade, seus limites, o uso de meios e técnicas sigilosos e, ainda, o sigilo nos procedimentos de compras e contratos, na publicação de atos oriundos da comunidade de inteligência".

Também se deu atenção aos profissionais de inteligência. Segundo a publicação de 2011, "estes necessitam de normas claras que lhes deem respaldo para o exercício regular de suas atribuições, que protejam sua identidade e garantam o sigilo profissional de seus atos". Observa-se que, na atualidade, os profissionais dos serviços secretos têm poucas garantias para atuar, "sobretudo aqueles de operações, o que os põe em situação tremendamente delicada de exposição".

Atenção especial deve ser dada, ainda, à legislação sobre salvaguarda de assuntos sigilosos, que precisa de reforma. A atual Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI),

---

[55] Entre as escolas de inteligência que existem atualmente no Brasil, cita-se, por exemplo, a Escola de Inteligência (ESINT), a Escola de Inteligência Militar do Exército (ESIMEX) e a Academia Nacional de Polícia (ANP).

não distingue as informações recebidas, produzidas e custodiadas pelos setores de inteligência daquelas de outros órgãos da Administração. Com isso, vulnerabilidades surgem, sobretudo quando conhecimentos sensíveis passam a ter tratamento semelhante a quaisquer conhecimentos no âmbito da Administração pública. Nesse sentido, recomendava-se na *Agenda Legislativa* que:

> "É importante que os serviços secretos tenham legislação específica referente a suas previsões e alocações orçamentárias. Esse é tema que merece maior discussão no parlamento". [56]

Observe-se, finalmente, que de nada adiantam reformas na estrutura e funcionamento da atividade de inteligência no Brasil sem mudanças em seus mecanismos de controle, em âmbito interno e externo. Para isso, a atuação do Parlamento é imprescindível.

III. 8. Papel do parlamento no fortalecimento do controle da atividade de inteligência

Um aspecto fundamental que diferencia a atividade de inteligência de regimes democráticos daquela exercida sob modelos ditatoriais, repita-se, é exatamente o controle exercido sobre os serviços secretos nas democracias. Nesse contexto, o parlamento assume papel de grande relevância como principal instância de controle externo da atividade de inteligência.

---

[56] GONÇALVES, Joanisval Brito, "O que fazer com nossos espiões? Considerações sobre a atividade de inteligência no Brasil", *op. cit.*.

A Lei nº 9.883, de 1999, estabelece, em seu art. 6º, o controle externo da atividade de inteligência. Com a Lei, foi criada a Comissão Mista de Controle das Atividades de Inteligência do Congresso Nacional (CCAI), instituída em 2000. O Brasil passou, assim, a ser o primeiro país da América Latina a ter um órgão de controle dos serviços secretos funcionando no Poder Legislativo.

A CCAI passou, entretanto, em sua primeira década de existência, por problemas de inoperância e seu controle tem sido pouco efetivo. Essa questão só começa a ser resolvida com a aprovação em 19 de novembro de 2013, do Regimento Interno da CCAI (RICCAI). Referido Regimento traz possibilidades concretas de atuação da Comissão. Os efeitos dessa importante transformação ainda não podem ser mensurados.

Outro mecanismo relevante para tornar mais efetivo o controle é a elevação da atividade de inteligência ao *status* constitucional. Não há qualquer referência na Carta de 1988 à atividade de inteligência ou aos serviços secretos e, muito menos, a seus mecanismos de controle. Isso pode ser feito por Emenda Constitucional que acrescentaria ao Título V da Constituição, referente à "Defesa do Estado e das Instituições Democráticas", um Capítulo IV, sobre "Atividade de Inteligência". A esse respeito, tramita no Congresso Nacional a Proposta de Emenda à Constituição (PEC) nº 67, de 2012, de autoria do Senador Fernando Collor, que a apresentou enquanto presidia a CCAI.

A referida PEC dispõe sobre o conceito de inteligência, a maneira como essa atividade deve ser organizada, e a importância da inteligência para o regime democrático, com respeito às instituições, aos

princípios democráticos, aos direitos e garantias individuais e à ordem constitucional e legal estabelecida. Importante, também, é a ênfase ao papel constitucional da inteligência para a defesa da sociedade e do Estado. Há, ainda, referência à necessidade de estruturação sistêmica da comunidade de inteligência e a salvaguardas ao pessoal e ao conhecimento produzido.

A proposta cuida, por igual, do controle dos serviços secretos, em especial daquele exercido pelo Legislativo. Assim, propõe-se a manutenção da Comissão de Controle das Atividades de Inteligência, mas com *status* constitucional e plenos poderes para fiscalizar o Sistema Brasileiro de Inteligência (SISBIN) como um todo, e, também, com competências autorizativas, isto é, ela deverá ser consultada previamente em determinadas ações.

Ainda sobre controle, a PEC nº 67, de 2012, cria o Conselho de Controle da Atividade de Inteligência. Esse Conselho, composto por não parlamentares, dedicar-se-á em tempo integral à fiscalização e controle de toda a comunidade de inteligência do País e será um órgão auxiliar do Congresso Nacional para a fiscalização e controle finalístico dos serviços secretos brasileiros e de suas atividades.

III. 9. Alteração na legislação infraconstitucional de inteligência

A legislação infraconstitucional de inteligência carece de clareza sobre mandato, direitos e deveres, e limitações à atividade de inteligência no Brasil. Assim, é preciso que seja feito aperfeiçoamento nessas normas.

Os serviços secretos e a ABIN em particular não têm mandato claramente definido por lei. Isso precisa ser mais bem especificado em dispositivo legal, para adequada orientação das atividades desses órgãos. As prescrições gerais adviriam de uma Política Nacional de Inteligência (PNI), enquanto as diretrizes podem ser estabelecidas pela Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (CREDEN).

Finalmente, assinale-se que não há legislação que regulamente a atividade de inteligência privada no Brasil ou seus mecanismos de controle. Sobre o assunto, havia o Projeto de Lei nº 2.542, de 2007, de autoria do Deputado José Genoíno, que tramitava na Câmara dos Deputados e foi arquivado ao final da legislatura. Sobre interceptação telefônica, há a Lei nº 9.296, de 1996. Ressalte-se que, por mandamento constitucional, proposições que tratem de atribuições de órgãos públicos devem ser de iniciativa do Poder Executivo, motivo pelo qual não cabe a esta comissão apresentá-los.

Parte IV – SEGURANÇA DAS COMUNICAÇÕES

IV. 1. Introdução

Após o choque inicial ante as denúncias de Edward Snowden, que apresentou documentos convincentes comprovando as alegações que fazia acerca de espionagem por parte da Agência de Segurança Nacional (NSA), a reação da comunidade internacional de segurança cibernética foi vigorosa. Os maiores expoentes dessa comunidade conclamaram seus pares a reagir e a reconstruir a internet como um território livre e seguro. Nas palavras de Bruce Schneier, especialista em segurança de comunicações, "é impossível construir uma internet onde os mocinhos podem espionar e os bandidos não possam fazê-lo. Temos a opção entre uma internet vulnerável a todos os agressores e uma internet segura contra todos os agressores".

É inegável que as ações da NSA e de suas parceiras integrantes da aliança *Five Eyes* evidenciaram que as aplicações da internet e a forma em que elas são utilizadas facilitam as ações de espionagem, revelando um ambiente pouco seguro para todos os usuários. As vulnerabilidades nas redes, identificadas e aproveitadas pela Agência e por suas aliadas, podem ser exploradas por criminosos de todos os tipos, de terroristas a pedófilos, de traficantes a criminosos de colarinho branco, de predadores sexuais a companhias de seguros desonestas e a chantagistas, enfim, por todo um universo de matizes de criminosos e contraventores. Pode-se mesmo dizer que os fundamentos do direito à privacidade foram solapados.

Os documentos apresentados por Snowden evidenciam que a NSA trabalhou para atacar todos os tipos de comunicação, e dão conta de que o principal meio de espionagem usado pela NSA é a internet. Na maior parte do tempo, são utilizados programas que automaticamente coletam e analisam o tráfico da rede. Valendo-se supostamente de "acordos secretos" com companhias de telecomunicações – americanas e britânicas, além de várias outras parceiras de outros países, segundo as denúncias –, a Agência acessa os cabos de comunicação por onde passa o tráfego da rede. Quando não se estabelec as parcerias, a NSA, segundo consta, age por meio de grampeamento dos cabos submarinos, interceptando comunicações via satélite, atacando dispositivos de rede, tais como *routers*, interruptores (*switches*), *firewalls*, entre outros. A maior parte desses dispositivos, sustenta a denúncia, teria capacidade de vigilância já embutidas de fábrica, sendo necessário apenas ativá-las.

A grande repercussão dessas denúncias deveu-se tanto pela dimensão tecnológica quanto pela abrangência e importância dos alvos escolhidos para obtenção ilegal de informações. Chamou atenção a falta de cuidado de parcelas dos setores público e privado com informações sensíveis e a forma indiscriminada como a espionagem é feita pelas agências de inteligência dos *Five Eyes*.

A questão da dimensão tecnológica é grave diante da constatação de que as atividades humanas (e até não humanas, uma vez que as comunicações entre máquinas representam tendência crescente) tornam-se cada vez mais vinculadas e dependentes das tecnologias de informação e comunicação (TIC).

Nesse cenário, governos, empresas e cidadãos tornam-se agentes ativos e passivos de uma guerra cibernética, em que manobras de ataque e defesa se confundem, e os investimentos em recursos financeiros, tempo e de recursos humanos se avolumam para fazer frente às crescentes ameaças. Um dos maiores desafios da sociedade global hoje é o de se proteger adequadamente sem perder os maiores benefícios das TIC, tais como comunicação global, facilidade de acesso, disseminação da informação sem fronteiras.

As respostas às ameaças cibernéticas – como quebra indiscriminada de privacidade, confiabilidade e sigilo das informações –, em prol de maior segurança, podem vir a criar, em última instância, redes fragmentadas ou isoladas. Na prevalência dessa opção política, "o que começou como uma abrangente rede global se parecerá cada vez mais com o mundo real, cheio de divisões internas e interesses divergentes"[57].

Assim sendo, surge um mercado global de segurança e serviços que deve alcançar 67 bilhões de dólares em 2013, experimentando crescimento para os próximos anos, podendo chegar, em 2016, a 86 bilhões de dólares, de acordo com o *Gartner Group*. Segundo a empresa, as maiores influências sobre os gastos estão agora na crescente complexidade dos ataques, que aumenta o volume de dados necessários para a detecção, o que requer melhores equipamentos, serviços de apoio e ampliação das habilidades dos analistas de segurança[58].

---

[57] SCHMIDT, Eric. A nova era digital. CIDADE: EDITORA, ANO. , p.101.
[58] Revista Tema, Serpro, ano XXXVIII, n 219, 2013.

Antes mesmo das denúncias de Edward Snowden, o Brasil já era apontado como particularmente vulnerável a ataques cibernéticos. Em estudo divulgado pelo centro de pesquisas belga *Security Defense Agenda* (SDA) e pela empresa de antivírus McAfee[59], abrangendo 23 nações, o país figurava como um dos menos preparados para enfrentar possíveis ataques. O estudo levou em consideração a adoção de medidas básicas como *firewalls* (dispositivos que protegem contra *hackers*) adequados e proteção antivírus e outras mais sofisticadas, educação e grau de informação do governo. Importa, portanto, buscar alternativas de atuação do Estado que lhe confiram ferramentas e processos mais adequados diante das ameaças tecnológicas a que está exposto.

Antes, porém, é fundamental compreender detalhadamente como funcionam as redes de telecomunicações e os mecanismos que possibilitam a conectividade global, o que permitirá trazer à luz questões relacionadas à espionagem eletrônica e alternativas concretas de proteção no meio virtual.

No decorrer dos trabalhos desta Comissão, evidenciou-se que, ante a impossibilidade de indiciar possíveis responsáveis pelas ações de espionagem denunciadas, sua principal responsabilidade consistiria em elencar possíveis vulnerabilidades das redes de comunicações do país e levantar opções para eventual alteração legislativa, modificação de processos e atualização tecnológica necessários para a construção de um país apto a enfrentar os crescentes desafios do meio cibernético em que vivemos.

---

[59] http://www.bbc.co.uk/portuguese/noticias/2012/01/120131_ciberdefesa_pai.shtml

Alvo de espionagem estrangeira, a Presidente Dilma Rousseff disse em seu discurso na ONU que "o Brasil sabe proteger-se" de ameaças vindas pela rede. A realidade, contudo, é que o sistema de defesa cibernética do País ainda dá os primeiros passos, e é preciso garantir segurança adequada contra ataques, espionagem e sabotagem. Embora o tema da defesa cibernética já figurasse como prioridade na Estratégia Nacional de Defesa do Brasil, elaborada em 2008, as denúncias ora analisadas oferecem oportunidade para discutir as formas como o Estado, as empresas e as pessoas, devam melhor se equipar para resguardar seus dados.

IV. 2. Ameaças, provocações, guerras e espionagem cibernéticas

As ameaças cibernéticas existem desde os primórdios da internet, e a sua crescente diversidade, sofisticação e abrangência vêm trazendo desafios novos aos governos, corporações e indivíduos.

A dificuldade inicial é a própria definição dos conceitos de segurança, defesa e guerra cibernética. Apesar dessa dificuldade, é unânime o entendimento de que nos encontramos num cenário bastante diverso da guerra cibernética tradicional e de que as novas ferramentas oferecem possibilidades incontestavelmente novas e surpreendentes em caso de conflito interestatal ou não nesse domínio.

O perigo das ameaças cibernéticas reside na capacidade do atacante causar danos consideráveis, físicos e virtuais, a partir de qualquer distância e com o mínimo de recursos. A vigilância onipresente da NSA e

de seus parceiros deve-se em grande parte à redução dos custos de vigilância.

A ameaça assimétrica representada por ataques cibernéticos, pela vigilância desmedida promovida pelas agências de segurança e inteligência dos EUA e seus principais aliados e pelas vulnerabilidades do ciberespaço tornou-se uma significativa preocupação de segurança nacional. Soluções devem ser encontradas por todos, tendo em vista a permeabilidade das TIC no cotidiano de governos, empresas e pessoas e as fragilidades tecnológicas, procedimentais e institucionais que ficaram patentes após as denúncias de Edward Snowden.

Embora as informações divulgadas relacionadas à espionagem contra o Brasil pareçam se restringir à busca de informações privilegiadas de parcelas do governo e da Petrobrás, não se pode descartar a possibilidade de ameaças e ataques, de origem tanto externa quanto interna, contra todas as infraestruturas críticas do País. Desenvolvemos uma dependência crítica de *softwares* e de redes de computadores: o funcionamento de todos os setores críticos do País é controlado por redes de informação: telecomunicações: transportes, energia, saúde, educação, defesa, comércio, mercado financeiro, radiodifusão. Certo é que a utilização do ciberespaço por organizações terroristas, criminosos organizados e atores patrocinados por Estados ou os próprios Estados representa um séria ameaça à segurança global[60].

---

[60] http://www.senado.leg.br/comissoes/cre/ap/AP20120409_Jorge_Fernandes.pdf

A implementação de uma política de segurança e defesa cibernética exige mudanças profundas na tecnologia e nos processos utilizados, bem como no comportamento das pessoas e nas instituições que os utilizam. São mudanças essenciais para fazer frente às ameaças crescentes em número e gravidade.

Nesse sentido, propomos neste relatório sugestões de ações que visam a aumentar a segurança cibernética do País em quatro grandes linhas de atuação: tecnologia, pessoas, processos e instituições.

Para possibilitar a compreensão de como parecem agir os mecanismos de interceptação das comunicações, apresentaremos breve explicação sobre o funcionamento das redes de telecomunicações.

VI. 2.1. Aspectos do funcionamento das redes de comunicações

Com a evolução da eletrônica digital e o desenvolvimento de técnicas de processamento de sinais, as telecomunicações tiveram grande impulso nas últimas décadas do século passado. As redes tornaram-se mais flexíveis, construídas sobre plataformas convergentes, que permitem compartilhar os mesmos recursos físicos e dar suporte a uma grande variedade de serviços. Tal como os computadores, as redes de comunicações são cada vez menos dependentes do *hardware* e cada vez mais baseadas em *software*, tal como já ocorria com suas aplicações e serviços. Em paralelo com as redes, os dispositivos terminais também evoluíram e passaram a ter funções de processamento e armazenamento distribuído de informações.

A internet[61], as redes telefônicas (fixas ou móveis), as de TV por assinatura, as de distribuição de conteúdo (CDN), as corporativas, entre outras, se beneficiaram dessa evolução. Assim, embora possam existir redes isoladas, as redes de comunicação estão, na maioria dos casos, fisicamente interligadas. A separação entre os distintos serviços é cada vez mais lógica do que física. As arquiteturas de rede modernas permitem separar as aplicações (ou serviços) das funções de transporte que lhes dão sustento. Em consequência, a distinção entre os serviços de valor adicionado (SVA) e os serviços de telecomunicações fica difícil de ser feita.

Padrões internacionais abertos adotados garantem alto nível de interoperabilidade entre as redes. Costuma-se associá-los a modelo conceitual, conhecido como interconexão de sistemas abertos (*Open Systems Interconnection* – OSI), que representa as redes de comunicação sob a forma de sete camadas lógicas. Assim, a camada mais alta, que corresponde às aplicações, utiliza os serviços das camadas mais baixas, e assim sucessivamente, até chegar aos meios de transmissão.

Cada uma dessas camadas têm múltiplos padrões, mas merece destaque o uso intensivo na camada 3 das redes de um protocolo conhecido como IP (*internet protocol*, ou, em português, "protocolo interredes"). Esse protocolo, criado nos anos 70, muito utilizado já nos anos 80, ampliou de modo superlativo nos anos 90 com a internet comercial. Ele foi adotado no início do século pelas redes de próxima geração (NGN) e mais

[61] A internet pode ser descrita como uma rede de redes, estruturada em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de endereços IP e outros identificadores únicos.

recentemente pelas redes móveis de 4ª geração (LTE). Essa padronização favorece a crescente interoperabilidade, com os mesmos serviços podendo operar sobre distintas redes.

Essa evolução das redes permitiu o aparecimento de novas empresas e modelos de negócio. Entre os mais exitosos estão as redes móveis, que têm mais de 6 bilhões de assinantes no mundo e a internet, que se aproxima dos 3 bilhões. Atuando na internet estão, atualmente, várias companhias, muitas delas com menos de 20 anos de vida, que disputam as primeiras posições mundiais em termos de valor de mercado.

Se por um lado essa evolução trouxe novas funcionalidades e comodidades, por outro apresentou muitas vulnerabilidades. As redes tradicionais, cabeadas, em poder de grandes empresas monopolistas, possuíam uma estrutura hierárquica mais rígida, com inteligência centralizada. Elas estavam mais protegidas que as redes modernas, até porque as conexões entre elas ocorriam apenas no nível físico, e não havia como aplicações de uma acessar aplicações disponíveis na outra.

Nesse sentido, as revelações de Snowden deram amostra da amplitude e da complexidade do esquema de vigilância cibernética da NSA. Conforme as informações divulgadas, dois métodos principais são utilizados pela Agência para coletar informações:

1) acesso direto às informações fornecidas por um certo número de grandes empresas,[62]

2) programas de interceptação de grandes fluxos de comunicação, por meio da captura de dados nas infraestruturas por onde trafegam ou estão armazenadas.

No primeiro caso, as eventuais ações têm de ser tratadas pelo Executivo em suas relações com outros Estados, visto que é uma forma de interceptação legal feita em outro país.

Já no segundo caso, podemos tomar medidas, embora com limitações. Esse método, divulgado com o nome de *upstream collection*, está baseado em diversos programas (*Blarney, Fairview, Oakstar e Stormbrew*). Há informação divulgada sobre o que fazem, sobre seu volume relativo[63], mas quase nada sobre como realizam tal espionagem.

Para fins de análise dos problemas de espionagem, de forma simplificada as redes de telecomunicações podem ser representadas pelo esquema abaixo:

---

[62] Google, Apple, Microsoft, Facebook, AOL, PalTalk e Yahoo, de acordo com http://www.theguardian.com/world/the-nsa-files

[63] Nove por cento, segundo http://sealedabstract.com/rants/the-part-of-the-fisc-nsa-decision-you-missed/

Um usuário que faz uma chamada telefônica, utiliza um caixa automático de seu banco ou navega na *web*, geralmente utiliza uma ou várias dessas redes. As redes estão interconectadas, normalmente sob a responsabilidade de múltiplos operadores. Pode haver violações devidas a vulnerabilidades que, em princípio, podem estar em quaisquer dessas redes.

Para levantar e qualificar tais vulnerabilidades, a Agência Nacional de Telecomunicações (ANATEL) efetuou pesquisa, envolvendo as principais operadoras licenciadas. A partir dessa coleta de informações, parece claro que as maiores vulnerabilidades estão nos dois extremos das redes, e por razões bem distintas, conforme apontamos a seguir.

As redes locais (redes de usuários), geralmente privadas, apresentam vulnerabilidades que decorrem de omissões de seus administradores e usuários. No caso de redes locais domésticas, nem sempre os usuários têm consciência do problema. No caso de redes locais corporativas, já há maior nível de profissionalismo, mas ainda assim muitas organizações não dão a devida atenção a regras de segurança.

Já em relação às redes globais, valem as leis de outros países. Assim, uma interceptação das comunicações para fins de espionagem, além de extremamente fácil, pode ser absolutamente legal. Estima-se que mais de 70% do tráfego de dados gerado por brasileiros circule fora do Brasil. Isso ocorre porque uma das pontas da comunicação está fora do território nacional. Assim, as medidas de proteção passam por tentar reduzir essa porcentagem, em particular para as informações mais sensíveis. Outras formas de proteção baseadas em criptografia podem ser usadas, mas têm limitações, como escalabilidade e interoperabilidade.

As redes de acesso, por sua vez, pertencem, em geral, às operadoras. Contam, assim, com administração mais profissional. No entanto, são vulneráveis. No Brasil, são mais de 4.000 operadoras, com os mais diversos portes. É grande a variedade em meios de transmissão, métodos de acesso e de tecnologias empregados. Os meios de transmissão abertos, com o uso de radiofrequências, são particularmente frágeis. Sua escuta é fácil. Mesmo quando há uso de criptografia, nem sempre a proteção oferecida é fim a fim. Além disso, há ferramentas disponíveis no mercado para quebrá-las. Os meios de transmissão confinados, metálicos ou óticos, são também vulneráveis devido à capilaridade das redes, acessíveis em postes, em gabinetes de rua e outros espaços públicos. Assim, como nem sempre é possível proteger as redes, recomenda-se realizar a proteção nas camadas mais altas, como forma de proteger os dados independentemente dos meios sobre os quais trafegam.

As redes regionais (ou *backhaul*) são também razoavelmente indefesas. No Brasil, elas utilizam extensivamente enlaces de rádio, um meio de transmissão aberto, de fácil escuta. Mesmo nos casos de redes óticas, que utilizam meios confinados, as vulnerabilidades podem existir. Se houver acesso físico às fibras, não é difícil capturar uma cópia dos dados que nelas trafegam.

Além disso, não há como garantir que estas redes não permitam o vazamento de informação por *backdoors,* que são vulnerabilidades inseridas propositalmente. Essas vulnerabilidades podem ter as mais diversas origens, que podem vir desde o projeto, dos componentes de *hardware* e *software* utilizados, da assistência técnica local ou remota, do pessoal próprio ou terceirizado das operadoras, entre

outras. Uma forma de proteção é pela observação de padrões de comportamento, tal como fazem as operadoras de cartões de crédito, mas esses métodos requerem um grande esforço computacional e também apresentam limitações.

Nas redes nacionais (ou *backbones*) baseadas em redes óticas de grandes operadoras o acesso indevido às informações é mais complexo. A proteção lógica requer a utilização de ferramentas de controle de acesso e análise de vulnerabilidades. As fragilidades tanto podem estar no projeto do *software* quanto no do *hardware* utilizados e podem passar despercebidos. Os fluxos de informação transportados são muito volumosos e heterogêneos. É mais difícil estabelecer seus padrões de comportamento, o que dificulta sua proteção.

No que tange aos cabos submarinos, a coleta de dados é possível, embora árdua. Os cabos estão no fundo do mar, com suas grossas armaduras para proteger as frágeis fibras óticas do ambiente agressivo, e às vezes utilizam dispositivos alimentados em alta tensão. Assim, é muito mais cômodo espionar alhures.

Voltando aos *backdoors* e mecanismos de *upstream*, esses pontos de escuta (*taps*) podem estar não apenas na internet, mas em quaisquer redes, mesmo nas mais insuspeitas. Para uma rede de TV a cabo, por exemplo, é possível fazer captura seletiva de dados para fins de controle de qualidade (QoS) ou de interceptação legal (LI): um protocolo de descoberta de ponto de controle permite localizar o equipamento do usuário (UE) de interesse e a partir daí pode-se fazer a coleta dos dados correspondentes em distintos dispositivos da rede.

A dificuldade de detectar *backdoors* é que só quem os projetou sabe como ativá-los. Assim, ficam inativos e passam despercebidos nos mais rigorosos testes. Na virtual impossibilidade de encontrá-los, algumas técnicas têm sido propostas para dificultar seu funcionamento, como sugerido por Adam Waksman, da Universidade Columbia, nos EUA[64]. Nesse caso, o princípio é tentar embaralhar os meios que são utilizados para sua ativação, que podem ser ligados ao tempo de funcionamento ou a códigos de sinalização enviados ao dispositivo.

É importante ressaltar que a topologia e a segurança das redes de telecomunicações no Brasil são, se não exatamente, ao menos bastante similares às de suas congêneres internacionais. É também importante ter em mente que uma eventual violação da segurança numa rede local (de usuário), numa rede de acesso ou no backhaul não viabilizaria por si só ações como as reveladas por Snowden.

IV. 3. Como proteger as redes

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) tem se empenhado em realizar as políticas nacionais para a segurança da informação e das comunicações. No entanto, tem concentrado seus esforços particularmente nas tecnologias de informação utilizadas nos órgãos e entidades da administração pública federal, direta e indireta. Assim, a segurança das comunicações tem merecido menos

64 Silencing Hardware Backdoors http://www.cs.columbia.edu/~simha/preprint_oakland11.pdf.v. pág. 41 a 43.

atenção, fato agravado pela dificuldade de separação entre o público e o privado. As redes de comunicações são integradas, além de que no Brasil o setor público utiliza extensivamente as redes das operadoras privadas.

Por conseguinte, temos de fomentar medidas que estimulem a melhoria da confidencialidade do setor de telecomunicações nas políticas nacionais segurança da informação e das comunicações, em especial quando se tratar de comunicações governamentais. Não existe padrão universalmente aceito sobre quem deve implementar tais políticas. Alguns países têm agências de segurança abrangentes [por exemplo: *Korean Internet and Security Agency* (KISA), na Coréia do Sul] outros delegam tais atribuições ao regulador das telecomunicações ou ainda as repartem entre distintas entidades. O importante, em qualquer caso, é que as responsabilidades estejam bem definidas, de maneira que não fiquem lacunas em descoberto.

O arcabouço para uma segurança adequada das telecomunicações governamentais deve incluir, no mínimo, os padrões técnicos nacionais para a segurança da informação e das comunicações baseados nas normas ABNT da série 27000 e, em particular, da Rec. X.1051 da UIT-T (*Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*).

Pode-se prever de início apenas uma certificação voluntária, que poderia mais tarde tornar-se obrigatória, pelo menos para as grandes operadoras, ao fornecerem soluções de redes e de serviços para comporem a infraestrutura de suporte a comunicações do governo. Deve-se, ainda,

buscar a colaboração com o setor acadêmico, institutos de pesquisa e consultorias especializadas em segurança para a formulação das políticas e regulamentações de segurança das comunicações, cuidando de acompanhar a evolução internacional do setor.

Algumas recomendações técnicas mínimas, aplicáveis às tecnologias atuais de redes (sujeitas à evolução), incluem o uso da arquitetura de segurança IPSec, que foi concebida para prover respostas para questões tais como criptografia de dados (confidencialidade), integridade, autenticação entre pares e gerenciamento de chaves criptográficas que serão utilizadas na proteção dos dados transmitidos (geração de forma segura e renovação).

Deve-se prever, também, a proteção contra ataques de falsificação de endereços, utilização de protocolos de coleta e exportação de informação de fluxos para detecção de anomalias de tráfego associadas a ataques de negação de serviço, a separação entre redes (consideradas seguras ou inseguras, confiáveis ou não confiáveis), a filtragem de conexões levando-se em conta informações de estado, além do controle de acesso administrativo aos elementos críticos de interconexão de redes. Tudo isso deve ser feito através de protocolos e algoritmos padronizados.

Entre ações preventivas que não podem ser ignoradas, está a certificação de equipamentos de telecomunicações atendendo a aspectos de segurança humana, física e lógica. Entre padrões relevantes, podem ser mencionados os critérios do *Common Criteria Recognition Arrangement*

CCRA,[65] que definem distintos perfis de proteção para diferentes categorias de equipamentos de informática ou de telecomunicações.

Além disso, o Estado deveria avaliar a conveniência de adotar medidas para que o ciclo completo de desenvolvimento e produção de hardware e software dos equipamentos e demais componentes dos sistemas de suporte às comunicações governamentais fosse supervisionado. O objetivo é ter orientação sobre como construir um sistema com garantia de segurança em todo o seu ciclo de vida. A confiança justificada de que o sistema funciona como previsto e está livre de vulnerabilidades concebidas, intencionalmente ou não, ou inseridas como parte do sistema a qualquer momento durante o ciclo de vida. Essa confiança é alcançada por atividades de garantia de sistema, que incluem um conjunto planejado e ordenado de atividades multidisciplinares para alcançar as medidas de segurança aceitável sobre sistema e gerenciar o risco de vulnerabilidades exploráveis.[66]

Outra área relevante é a proteção da infraestrutura crítica de informação e comunicação. Nesse particular, a Anatel tem alguma experiência, à vista de suas responsabilidades assumidas no Subgrupo Técnico de Segurança de Infraestruturas Críticas de Telecomunicações (SGTSIC – Telecomunicações) do GSI/PR. Encontra-se hoje em execução o Projeto de Segurança de Infraestruturas Críticas de Telecomunicações (SIEC), que inclui o desenvolvimento de um sistema informático orientado a identificar e avaliar os riscos que possam afetar a segurança das redes brasileiras de telecomunicações.

---

[65] http://www.commoncriteriaportal.org/ccra
[66] AEP-67 Ed. 1 (2010) *Engineering For System Assurance In Nato Programmes*

Em complemento ao SIEC, encontra-se em fase avançada de elaboração o Regulamento sobre Gestão de Risco das Redes de Telecomunicações e Uso de Serviços de Telecomunicações em Situações de Emergência e Desastres.

Com relação à prevenção e resposta às ameaças e incidentes, as grandes operadoras de telecomunicações dispõem de Equipes de Resposta a Incidentes de Segurança (CSIRTs) e Centros de Operação de Segurança (SOCs). No entanto, há pouca coordenação entre eles e CSIRTs de outros setores (por exemplo, bancos ou o CERT.br[67]), bem como carência de procedimentos preestabelecidos para tratar de casos de ataques cibernéticos envolvendo as redes de telecomunicações. Em geral, espera-se uma pronta resposta a ameaças e incidentes, qualquer que seja o horário ou o local geográfico em território nacional.

Finalmente, a segurança da informação e das comunicações não pode ser obtida com os esforços de um país isolado, pois as redes são integradas e as ameaças tendem a ter caráter global. Para que seja efetiva, a coordenação internacional deve ser institucionalizada, tanto no governo quanto no setor privado. Nesse particular, as organizações internacionais do setor têm papel essencial.

---

[67] O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br) do Comitê Gestor da Internet no Brasil (CGI). É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à internet brasileira.

IV. 4. Marco Civil da Internet

O projeto de Marco Civil da Internet (MCI), PL nº 2.126, de 2011, foi encaminhado pelo Poder Executivo ao Congresso Nacional em 24 de agosto de 2011. A proposta, submetida à apreciação da sociedade entre outubro de 2009 e maio de 2010, por meio de consulta pública[68], teve como inspiração os princípios de governança e uso da internet, aprovados pelo Comitê Gestor da Internet no Brasil (CGI.br).

Nesse contexto, pretende disciplinar os direitos e deveres dos usuários da internet bem como dos agentes econômicos que concorrem para a oferta de serviços na rede, notadamente os provedores de conexão e de conteúdo.

Em 12 de setembro de 2013, por meio da Mensagem nº 391/2013, foi solicitado pelo Poder Executivo que fosse atribuído à matéria o regime de urgência constitucional, conferindo-se, a partir do dia 13 de setembro de 2013, o prazo de 45 dias para sua apreciação na Câmara dos Deputados. Após chegar a um consenso sobre o texto final, a Câmara aprovou o relatório do MCI no dia 25 de março deste ano, que está agora sob análise do Senado Federal.

IV.4.1. Da Proposta

Uma das vulnerabilidades à segurança e à privacidade das comunicações brasileiras trafegadas na internet é intrínseca à própria

[68] A referida consulta pública, patrocinada pelo Ministério da Justiça, ocorreu em duas etapas: na primeira, questionou-se quais temas deveriam integrar um marco regulatório para a internet no Brasil; na segunda, com base nas contribuições recebidas na etapa anterior, uma minuta de anteprojeto foi apresentada, e sujeita a comentários e sugestões.

topologia atual de sua infraestrutura. Isso porque, o tráfego de dados originado e terminado no Brasil pode ter seu roteamento realizado fora do País, principalmente nos Estados Unidos, onde se concentram os servidores centrais da internet[69].

Em outros termos, uma informação originada em um ponto do território nacional com destino a outro – seja um correio eletrônico, o acesso a um *site* de notícias brasileiro ou o *download* de um aplicativo de um provedor nacional – pode trafegar por equipamentos localizados no exterior, facilitando seu monitoramento por agentes externos.

Nesse sentido, cumpre reproduzir as considerações apresentadas pelo Presidente da Anatel, João Batista de Rezende, por ocasião de audiência pública realizada pela CI no último dia 10 de outubro:

> "Porém, se a convergência traz benefícios econômicos, oferece dificuldades a serem superadas pela legislação brasileira. Questões como direitos autorais, privacidade e segurança na internet, neutralidade da rede e acesso à infraestrutura de dados – presentes no projeto de lei que institui o marco civil da internet – deverão ser discutidas com atenção pelo parlamento brasileiro.
>
> Além disso, a convergência midiática implica pensar, também, na segurança do Estado contra atos de espionagem cibernética. **A atual topologia da internet faz com que o tráfego mundial de dados passe pelos Estados Unidos. Tanto poder facilita os atos de esplonagem sobre informações estratégicas, o que se tornou um problema para o Brasil e outros países.**
>
> Embora não seja viável para o Brasil fechar o mercado da internet, como tentam a China e alguns países islâmicos, é

[69] Segundo estudo disponibilizado pelo *site* especializado Teleco, aproximadamente 14% do tráfego de internet direcionado aos Estados Unidos compreende os fluxos de comunicação entre países latino-americanos. Disponível em: http://www.teleco.com.br/emdebate/katzroux01.asp.

> **preciso trabalhar para trazer pontos de tráfego para o território brasileiro, permitindo proteger as informações que circulam pelo País.** Deve-se, também, exigir a democratização da governança da internet, permitindo que outros países participem das decisões que dizem respeito à rede." (grifo nosso)

A partir do cenário descrito, aventou-se uma sugestão que poderia ser incorporada ao PL nº 2.126, de 2011, com o objetivo de mitigar a vulnerabilidade descrita: a determinação de que todo tráfego de internet originado e terminado no Brasil seja trocado localmente. Para tanto, haveria necessidade de inclusão de dispositivo que obrigasse as empresas que provêm serviços de conexão à internet a assegurar que o tráfego simultaneamente originado e destinado a pessoas localizadas no Brasil ficasse confinado, prioritariamente, a redes dentro do território nacional.

A proposta exigiria das operadoras de telecomunicações investimentos na interligação de redes dentro do país, o que poderia gerar efeitos positivos para a segurança e privacidade das comunicações brasileiras trafegadas na internet. Todavia, essa medida certamente causaria, por um lado, uma desotimização das redes, com aumento de custos e de ineficiências, ao criar uma espécie de "internet do Brasil" e, por outro lado, significaria um "engessamento legal" no tocante à evolução das redes, num setor em que as mudanças decorrentes da evolução tecnológica ocorrem em ciclos cada vez mais curtos.

Parte V – PROVIDÊNCIAS ADOTADAS PELO GOVERNO BRASILEIRO

V.1. Inquérito instaurado pela Polícia Federal

O Departamento de Polícia Federal (DPF) instaurou inquérito policial para comprovar a materialidade e identificar a autoria de crimes supostamente praticados, relacionados ao episódio de espionagem de brasileiros, inclusive autoridades públicas, com destaque para a Presidente da República, Dilma Rousseff, pela *National Security Agency* (NSA) dos Estados Unidos da América (EUA).

A instauração do procedimento ocorreu em atenção ao Aviso Ministerial nº 32/2013, do Ministério das Comunicações (MC), visto às fls. 04/05 dos autos, que externou ao Ministro da Justiça sua preocupação em relação às notícias veiculadas pela imprensa, dando conta da existência de uma rede de vigilância global, que teria entre seus alvos as comunicações eletrônicas e telefônicas originadas ou recebidas no Brasil.

No referido Aviso, o Ministro das Comunicações informou ter solicitado da Agência Nacional de Telecomunicações (Anatel) adoção de providências para esclarecimento das denúncias veiculadas, em particular no que se refere à alegação de que as noticiadas ações de inteligência teriam sido viabilizadas pela existência de parcerias corporativas entre empresas estadunidenses e empresas brasileiras de telecomunicações.

Diante disso, foi instaurado o IPL nº 10/2013-COIAN/COGER, por Portaria de 09 de julho de 2013, vista às fls. 02/03

dos autos, da lavra do Delegado de Polícia Federal Carlos Eduardo Miguel Sobral, Chefe do Serviço de Repressão a Crimes Cibernéticos da Coordenadoria de Polícia Fazendária da Polícia Federal.

De acordo com essa portaria, é necessário apurar se houve, ou está havendo, a interceptação ilegal das comunicações em território nacional; se esse procedimento contou com a participação de pessoas físicas ou jurídicas, brasileiras ou estrangeiras, que atuam em território nacional; e, ainda, se há acordos comerciais ou corporativos para troca de dados ou informações relacionadas a comunicações ocorridas no Brasil, firmados entre empresas nacionais e grupos ou governos estrangeiros.

A portaria apontou como supostas condutas típicas as descritas nos arts. 13 e 14 da Lei nº 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), e 10 da Lei nº 9.296, de 24 de julho de 1996, que *regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal*, transcritos a seguir.

> •Lei nº 7.170, de 1983:
>
> **Art. 13.** Comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou grupo estrangeiro, ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos.
>
> Pena: reclusão, de 3 a 15 anos.
>
> *Parágrafo único.* Incorre na mesma pena quem:
>
> I - com o objetivo de realizar os atos previstos neste artigo, mantém serviço de espionagem ou dele participa;

II - com o mesmo objetivo, realiza atividade aerofotográfica ou de sensoreamento remoto, em qualquer parte do território nacional;

III - oculta ou presta auxílio a espião, sabendo-o tal, para subtraí-lo à ação da autoridade pública;

IV - obtém ou revela, para fim de espionagem, desenhos, projetos, fotografias, notícias ou informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, de instalações ou de sistemas de processamento automatizado de dados, em uso ou em desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devem permanecer em segredo.

•Lei nº 7.170, de 1983:

Art. 14. Facilitar, culposamente, a prática de qualquer dos crimes previstos nos arts. 12 e 13, e seus parágrafos.

Pena: detenção, de 1 a 5 anos.

•Lei nº 9.296, de 1996:

Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

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

No intuito de apurar a materialidade de suposto delito e identificar sua autoria, as autoridades policiais procederam às seguintes diligências preliminares:

1) requerimento de cópias de depoimentos e documentos prestados ou apresentados nas Comissões de Relações Exteriores e Defesa Nacional, tanto da Câmara dos Deputados quanto do Senado Federal (fls. 11/12 dos autos);

2) requerimento de informações à Anatel, acerca das providências determinadas pelo Ministro das Comunicações, a que alude o Aviso Ministerial nº 00032/2013-MC;

Na sequência, foi juntada aos autos, a Informação nº 220/2013-SRCC/CGPFAZ/DICOR, do Agente de Polícia Federal Luciano d'Escragnolle Cardoso (fls. 15/42). Provavelmente resultante de uma diligência interna da Polícia Federal, essa Informação definiu a linha de investigação, ou seja, ela foi preponderante para as diligências seguintes.

Esse relatório destaca, primeiramente, notícias dos jornais O Globo e *The Guardian*, que revelaram o esquema de espionagem, empreendido pela NSA.

Em seguida, destaca as possíveis fontes das informações obtidas clandestinamente pela NSA: cabos submarinos e satélites geoestacionários, utilizados pelo Brasil para tráfego das comunicações telefônicas e telemáticas, e empresas de telecomunicações que atuam no território nacional.

Por fim, apoiado em matérias jornalísticas, assinala os programas computacionais que a NSA teria usado para levar a efeito suas ações de inteligência: *Fairview* e *X-Keyscore*.

Em 13 de agosto de 2013, assumiu a presidência do inquérito o delegado de Polícia Federal Luiz Augusto Pessoa Nogueira (fl. 43), que

deu continuidade às diligências investigativas, decididas no despacho de fl. 45:

> 1) intimação dos representantes no Brasil de empresas de serviços de internet e *e-mail* – Google, Facebook, Microsoft, Yahoo, e Apple – para prestarem depoimento, tendo sido convidado para acompanhar as oitivas o representante do Comitê Gestor da Internet no Brasil, Hartmut Richard Glaser;
>
> 2) intimação dos representantes de empresas brasileiras de telecomunicações – GVT, CTBC, Telefônica, Oi, Tim, Claro, Vivo, etc. – para prestarem esclarecimentos, tendo sido convidado representante da Anatel para acompanhar as oitivas;
>
> 3) determinação para colher o depoimento de Glenn Greenwald, protagonista das matérias jornalísticas que veicularam a existência da espionagem internacional.

De acordo com o termo de fls. 50/55, Greenwald afirmou que as informações vazadas por Edward Snowden seriam resultado de um projeto mundial de interceptação de comunicações telefônicas e telemáticas, realizado pelo governo dos Estados Unidos da América, por meio da NSA e de empresas contratadas por ela. Disse, ainda, que algumas das informações são sobre estratégias comerciais de empresas brasileiras e outras teriam relação com decisões governamentais. Alertou que a espionagem empreendida pela NSA tem objetivos econômicos, além de servir para fiscalizar as ações do governo brasileiro, mas não soube citar

nenhum exemplo específico, nem mesmo quando perguntado especificamente sobre os setores de aviação militar, nuclear e petrolífero.

Revelou, por igual, que tem em seu poder conteúdo obtido clandestinamente de comunicações havidas entre autoridades governamentais brasileiras, inclusive a Presidente Dilma Roussef. Assegurou que ainda há muito a ser divulgado por Edward Snowden. Apontou que a empresa americana de telecomunicações AT&T estaria envolvida na operação espionagem e que a firma de consultoria Booz Allen trabalha na análise dos dados obtidos clandestinamente.

No mais, confirmou o teor de seu depoimento perante a CPI, em que acusou as empresas Google, Facebook, Skype, Microsoft, Apple, etc. de terem acordo com a NSA, pelo qual permitem àquele órgão do governo estadunidense acesso às informações e aos conteúdos das comunicações telemáticas dos usuários dos seus serviços de correio eletrônico.

Na sequência, às fls. 80/83, nova diligência:

> 1) requisição de informações ao Superintendente de Fiscalização da Anatel, para esclarecer: a) se a AT&T tem acordo operacional com empresas de telefonia que operam no Brasil; b) se é possível a interceptação de comunicação telefônica realizada no Brasil, sem o auxílio das operadoras brasileiras; c) de que modo se dá o uso dos cabos submarinos no caso de ligações telefônicas e comunicações telemáticas (fls. 80/81). Posteriormente, em complemento, requisitou mais

esclarecimentos: d) se a Anatel faz auditoria ou fiscaliza a utilização dos cabos submarinos para verificar a ocorrência de interceptação clandestina das comunicações; e) se, tecnicamente, as interceptações das comunicações podem ser feitas nos cabos submarinos por onde trafegam e se é possível verificar se houve a interceptação (fls. 82/83);

2) requisição ao Instituto nacional de Criminalística do Departamento de Polícia Federal, no sentido de elaborar informação técnica, a ser apresentada até o dia 28/10/2013, sobre questionamentos que fez em apartado;

3) requerimentos de colaboração remetidos à Rede Nacional de Ensino e Pesquisa, Centro de Tecnologia da Informação do Ministério da Ciência e Tecnologia, Universidade de Brasília (UnB), Universidade de Campinas (Unicamp), Universidade Federal de Minas Gerais (UFMG), e Fundação de Amparo à Pesquisa do Estado de São Paulo – FAPESP, no sentido de responderem, até 01/11/2013, os questionamentos que fez em apartado;

4) intimação das empresas proprietárias dos cabos submarinos utilizados pelo Brasil, Brasil Telecom Cabos Submarinos Ltda, AT&T Global Network Services Brasil Ltda e Latin America Nautilus Brasil Ltda, para prestarem esclarecimentos;

5) intimação das empresas proprietárias dos satélites utilizados pelo Brasil, Hispamar Satélites S/A, Telesat Brasil Capacidade de satélites Ltda e Star One S/A, para prestarem esclarecimentos;

6) determinação de oitiva dos presidentes mundiais da Yahoo, Microsoft, Apple, Google e Facebook, mediante cooperação jurídica internacional;e

7) por intermédio do mesmo instrumento, oitiva do presidente da AT&T e de Edward Snowden.

As diligências indicadas nos itens 6 e 7 decorreram das informações prestadas pela Anatel, em atendimento à diligência determinada pela Polícia Federal, constantes do apenso ao IPL nº 10/2013-COIAN/COGER.

Noutra oportunidade, a Anatel, em atendimento à diligência descrita no item 1, esclareceu que Embratel, Telefônica e TIM têm acordo operacional com a AT&T, com o propósito de estabelecer procedimentos para a complementação de chamadas telefônicas internacionais, sendo que tais acordos contêm cláusulas específicas de segurança e confidencialidade e não incluem nenhuma espécie de cooperação, por parte das operadoras brasileiras, no que diz respeito à coleta de informações sobre as chamadas telefônicas (fls. 84).

Alertou que é possível haver interceptação clandestina das comunicações telefônicas sem o consentimento das operadoras brasileiras,

bastando a atuação de um funcionário ou de pessoa com conhecimento técnico, acesso ao sistema e munido dos equipamentos necessários para realizar a escuta ilegal.

Constam do IPL os termos dos depoimentos prestados por Alexandre Marques Esper, representante da Microsoft (fls. 85/87); Diogo de Lima Gualda, do Yahoo (fls. 88/89); Marcel Leonardi, do Google (fls. 90/92); Bruno Magrani de Souza, do Facebook (fls. 93/95); e Pedro Sérgio Murari Pace, da Apple. Em síntese, os depoentes afirmaram que não possuem estrutura de armazenamento de dados (*datacenters*) no Brasil; que muitos desses equipamentos ficam nos Estados Unidos da América e que, em tese, o governo estadunidense poderia requisitar informações neles guardadas, inclusive de brasileiros, com suporte na legislação sobre vigilância de inteligência estrangeira (FISA), combinada com o *Patriot Act*. Afirmam, todavia, desconhecer que as respectivas matrizes tenham fornecido informações à NSA.

Os ofícios relativos aos requerimentos de colaboração a que alude o item 8 constam às fls. 177/185, sendo que os questionamentos submetidos às entidades de ensino e pesquisa são os seguintes: a) se a existência de *datacenters* no Brasil, para armazenamento de dados e conteúdos das comunicações telemáticas dos usuários residentes no País, garantiria que o acesso da matriz americana somente fosse possível com a permissão da subsidiária brasileira que os administraria; b) se, nesse caso, seria possível identificar o acesso ou tentativas de acesso por parte da matriz americana; c) se é possível fazer a interceptação das comunicações interferindo nos cabos submarinos ou nos satélites por onde trafegam as informações.

Na fl. 186, consta Despacho do Delegado de Polícia Federal Luiz Augusto Pessoa Nogueira, determinando:

a) expedição de carta precatória para oitiva dos representantes da Telefônica/Vivo e da AT&T Brasil;

b) intimação dos representantes da Claro/Embratel, Oi e Latin America, para prestarem depoimento no dia 28 de outubro de 2013;

c) requisição ao Instituto de Criminalística da Polícia Federal (INC/DPF), para que elabore nota técnica versando sobre as fls. 109/121 do apenso;

d) solicitação de compartilhamento de informações de posse desta CPI e, ainda, das Comissões de Relações Exteriores do Senado Federal e da Câmara dos Deputados;

e) solicitação de reinquirição do jornalista Glenn Greenwald, para que responda às seguintes perguntas:

1 – O que o depoente sabe dizer, de concreto, em relação à espionagem americana contra a Presidente Dilma Rousseff? O que foi interceptado, e-mail ou ligação telefônica?

2 – Qual o conteúdo dessa interceptação?

3 – Houve envolvimento de algum funcionário da Presidência da República?

4 – Houve participação de empresa de telefonia, de internet ou de estrutura de comunicação (cabos, fibras óticas, etc)?

5 – O depoente afirmou ao "Fantástico" que, além da Presidente Dilma Rousseff, assessores foram espionados. Quais?

6 – Qual o conteúdo da comunicação interceptada desses assessores?

7 – Em relação à espionagem contra a Petrobrás, quem foi o alvo das interceptações?

8 – Qual o teor das comunicações interceptadas?

9 – Houve envolvimento de algum funcionário da Petrobrás? Houve participação de empresa de telefonia, de internet ou de estrutura de comunicação (cabos, fibras óticas, etc)?

As perguntas 7 a 9 são feitas também em relação ao Ministério das Minas e Energia.

Em petição de fls. 191/192, a Oi informa que a Gerência de Ações Restritas da companhia fica localizada no Rio de Janeiro/RJ, sendo responsável pelo setor o Sr. João Roberto Menezes Ferreira.

Às fls. 194/196, consta petição da Telefônica informando que as funcionárias responsáveis por interceptações telefônicas residem em São Paulo/SP. A operadora antecipou, não obstante, que não fez nenhuma interceptação sem a devida autorização judicial.

Às fls. 204/205 consta termo de depoimento de Nelson de Sá, Gerente Executivo de Segurança Tecnológica da TIM, que esclareceu, em síntese, o seguinte: que o cabeamento utilizado pela TIM para ligações internacionais pertence a outras empresas; que por isso a TIM não tem como garantir a segurança das comunicações, após a saída da transmissão; que nunca teve conhecimento de interceptações clandestinas de seus usuários dentro da estrutura da empresa; que não é possível a interceptação de ligação de usuário da TIM com interlocutor no exterior, por autoridade policial ou inteligência de país estrangeiro, sem o conhecimento da companhia; que se o alvo for o interlocutor que está no exterior, a TIM não terá conhecimento da interceptação; que desconhece que a empresa tenha recebido requisição de autoridade americana, no sentido de interceptar ligações de seus usuários; que os dados das comunicações ficam armazenados em *datacenters* localizados no Rio de Janeiro e em São Paulo e que é tecnicamente impossível que a matriz italiana acesse esses dados sem conhecimento e autorização da TIM Brasil.

Às fls. 206/207, consta termo de depoimento prestado por João Leonardo da Silva Gomes Ferreira, Diretor Executivo da Level 3 Brasil, que esclareceu, em síntese, o seguinte: que pode afirmar, com convicção, que os dados dos usuários brasileiros da Level 3 Brasil, armazenados em *datacenters* no território nacional, não são acessados pela matriz americana – Level 3 Inc. – sem o conhecimento da Level 3 Brasil; que não existe a possibilidade técnica de acesso remoto pela Level 3 Inc e que a Level 3 Brasil nunca recebeu pedido da matriz no sentido de fornecer dados armazenados nos *datacenters* localizados em território nacional.

Às fls. 208/209, consta termo de depoimento de Guilherme Preston Krug, Gerente Jurídico da Nextel, que, em síntese, esclareceu: que a empresa possui *datacenters* no Brasil, não armazena conteúdo de comunicações de voz; que é impossível a interceptação clandestina de ligações dos usuários da Nextel; que a operadora nunca recebeu pedido da controladora americana acerca de dados de usuários brasileiros e que a matriz não tem qualquer ingerência sobre os dados dos usuários brasileiros, sendo impossível sua entrega a órgão de governo estrangeiro sem o conhecimento e a permissão da Nextel Brasil.

No que tange à requisição de nota técnica ao INC/DPF, pode-se ver que o objeto são as concessões de rádio à Embaixada Americana, sendo que o Delegado de Polícia Federal faz os seguintes questionamentos às fls. 212/213):

a) a que se destinam essas rádios? Como podem ser empregadas?

b) é possível a utilização dessas rádios para interceptação de comunicações telefônicas ou telemáticas?

c) é possível verificar, mediante varredura nos locais próximos a essas rádios, se há eventual emprego inadequado desses equipamentos?

Até a conclusão deste Relatório, não vieram a esta CPI outras informações sobre o Inquérito Policial a cargo da Polícia Federal.

Antecipando a análise que será feita adiante, pode-se observar que a Polícia Federal terá dificuldade para comprovar a materialidade do delito, nem havendo que se falar, por isso, em indícios de autoria.

V.2. Expectativa de desfecho do inquérito da Polícia Federal

Depreende-se das peças constantes do inquérito levado a efeito pela Polícia Federal, para apurar possível conduta criminosa relacionada ao episódio de espionagem que deu ensejo à instauração desta CPI, que é improvável a comprovação da materialidade do suposto delito. Crime é fato. Existe crime quando o agente pratica uma conduta típica, sem estar coberto por dirimentes, como legítima defesa, estado de necessidade ou exercício regular de direito.

No caso dos tipos aventados pela Polícia Federal – arts. 13 e 14 da Lei de Segurança Nacional, e 10 da Lei nº 9.296, de 1996 –, os crimes são submetidos à lei brasileira se as condutas tiverem sido praticadas no Brasil, não se aplicando o critério de extraterritorialidade previsto no art. 7º, II, *b*, do Código Penal – ter o crime sido praticado por brasileiro –, visto que não se verifica o requisito a que alude a alínea *b* do § 2º do mesmo dispositivo legal – ser o fato punível também no país em que foi praticado. Isso porque a legislação sobre vigilância de inteligência estrangeira, combinada com o *Patriot Act*, dá, em tese, amparo à ação praticada em território estadunidense.

Independentemente disso, há mesmo dificuldade em delinear a conduta criminosa supostamente praticada. E, como dissemos, crime é conduta.

Mais difícil, ainda, a identificação de autoria.

Os depoimentos colhidos nos autos do inquérito são todos, infelizmente, muito evasivos. Até então, a Polícia Federal sequer tinha ideia de onde teria sido efetuada a interceptação clandestina: se no território brasileiro, nos cabos submarinos, nos satélites geoestacionários ou se as informações foram simplesmente cedidas pelas empresas de serviços de internet, a partir de servidores localizados nos Estados Unidos da América.

Por tudo isso, o inquérito dificilmente terá êxito na obtenção de elementos suficientes para a propositura de eventual ação penal, ainda que novas linhas de investigação sejam estabelecidas a partir do cumprimento das diligências supervenientes.

Parte VI – CONCLUSÕES E RECOMENDAÇÕES

VI.1. Conclusões e recomendações em relação à atividade de inteligência

No campo da Inteligência, esta CPI pôde constatar a vulnerabilidade em que se encontra o país diante da espionagem proveniente de outros Estados, de organizações e empresas, sobretudo, estrangeiras. Uma segunda constatação é de que espionagem continuará sendo conduzida, goste-se dela ou não.

Assim, é fundamental que, para lidar com a espionagem internacional, o Brasil desenvolva mecanismos de proteção do conhecimento e de segurança cibernética. Investimentos em inteligência e, sobretudo, em contrainteligência, com ênfase no desenvolvimento de tecnologias próprias e nacionais e de quadros capacitados para o tema. A valorização dos profissionais de inteligência e a percepção de que esses atuam em prol do Estado e da sociedade é aspecto fundamental para o fomento da atividade de inteligência no Brasil.

Ademais, convém que se promova, entre os brasileiros, uma cultura de segurança e inteligência. A sociedade, os formadores de opinião e as autoridades têm que ter consciência de que, neste mundo cada vez mais competitivo, em que a espionagem cresce paralelamente ao desenvolvimento tecnológico nas relações entres os homens, cada indivíduo é responsável pela proteção ao conhecimento e por sua segurança, enquanto ao Estado compete a defesa dos interesses da

sociedade e a proteção aos conhecimentos sensíveis. Para isso servem os serviços secretos.

Atividade de inteligência e democracia são plenamente compatíveis. De fato, a inteligência mostra-se de grande importância para o assessoramento do processo decisório, particularmente nas esferas mais estratégicas de Estado e de governo. Uma vez que lida com informação e, portanto, com poder, a atividade de inteligência necessita de controle. E o controle dos serviços secretos passa a ser função também do parlamento, que não pode fugir dessa importante tarefa.

Para a garantia de um efetivo controle dos serviços secretos no Brasil, é fundamental que se regulamente a atividade de inteligência de maneira mais clara. A reforma na legislação de inteligência, entretanto, deve se dar, em conformidade com a Constituição de 1988, por meio de iniciativa do Poder Executivo, ficando o Parlamente limitado em muitos aspectos. Em termos de competência legislativa do Congresso Nacional, percebemos como de suma importância que se dê continuidade ao processo de aprovação da PEC nº 67, de 2012.

Essencial, ainda, que o trabalho da CCAI e do Congresso se torne mais efetivo nesse domínio. Para isso, a implementação da CCAI sob o novo Regimento é uma ação importante para o Poder Legislativo em 2014, que já está em curso. Com isso, ter-se-á melhor percepção do SISBIN e da própria atividade de inteligência e, ainda, mecanismos de fiscalização e controle mais abrangentes, eficientes e eficazes.

Os fatos tornados públicos por Edward Snowden sobre a espionagem internacional, pelo jornalista Glenn Greenwald e, ainda, pelos trabalhos desta CPI assinalam profunda vulnerabilidade do Estado brasileiro e de nossa população a ações de espionagem. Também parece claro que estas vão continuar ocorrendo.

Assim, diante do problema e da constatação de fragilidade em que se encontram a sociedade e o Estado brasileiro, percebe-se, no âmbito da Inteligência, a necessidade de mais investimentos e do aprimoramento do aparato brasileiro de contrainteligência. Apenas com mais contrainteligência e com o fomento a uma cultura de inteligência, segurança e proteção ao conhecimento, no setor público e na área privada, é que os brasileiros conseguirão fazer frente à ameaça da espionagem internacional.

Iniciativas importantes já foram tomadas para aprimorar a atividade de inteligência no Brasil. Entretanto, muito ainda há a ser feito. Busca-se apresentar aqui, de forma objetiva, algumas recomendações para o setor de inteligência.

VI. 1.1. Publicação da Política Nacional de Inteligência (PNI)

Documento norteador da comunidade de inteligência brasileira, a Política Nacional de Inteligência foi produzida, no âmbito do Poder Executivo, por um grupo interministerial de trabalho, apresentada ao então Presidente Luís Inácio Lula da Silva e por ele encaminhada à apreciação do órgão de controle externo do Congresso Nacional – a CCAI.

Apreciado pelo Poder Legislativo, o projeto de PNI foi devolvido ao Executivo com sugestões, estando pronto para ser editado pelo Presidente da República no final de 2010. Entretanto, até a conclusão do presente Relatório (março de 2014), a PNI não havia sido publicada pela Presidente Dilma Rousseff. Desse modo, o país permanece sem uma política que oriente a atuação dos serviços secretos brasileiros.

Recomenda-se, assim, que seja publicada o quanto antes a Política Nacional de Inteligência brasileira e, a partir dela, seja elaborada uma Estratégia Nacional de Inteligência e planos nacional e setorial de inteligência. Enquanto isso não ocorrer, os serviços secretos do país permanecerão sem orientação clara de como agir, correndo-se sempre o risco de, com isso, ver os órgãos de inteligência extrapolando suas funções, cometendo arbitrariedades (e até ilegalidades) e trabalhando em prol de governos, e não do Estado e da sociedade.

VI. 1.2. Investimento em contrainteligência

Se existe uma afirmação que pode ser feita sobre a espionagem internacional é que esta continuará e, de fato, mostrar-se-á mais intensa com o desenvolvimento de recursos tecnológicos que permitam a operação no ambiente virtual. Essa espionagem, feita por governos, empresas e organizações não pode ser objeto de qualquer regulamentação internacional, pois é atividade típica do sistema internacional anárquico.

Assim, iniciativas de se propor um regime internacional para regular o recurso à espionagem por parte de governos é, na melhor das hipóteses, utópica e ingênua. O direito internacional dificilmente alcançará o ofício dos espiões.

Diante dessa realidade, o que o Estado brasileiro deve fazer é investir em contrainteligência. Isso envolve mais recursos para os serviços secretos, aquisição e desenvolvimento de equipamentos, capacitação de recursos humanos e, ainda, estabelecimento de legislação que dê amparo ao setor de inteligência e permita a seu pessoal atuar em defesa do Estado e da sociedade.

VI.1.3. Maior dotação orçamentária para a comunidade de inteligência

Enquanto permanecer pífia a alocação orçamentária para a ABIN e outras organizações responsáveis pela atividade de inteligência, só se pode esperar que o Brasil permaneça vulnerável a toda a forma de espionagem, tanto no meio físico quanto no ambiente virtual. Daí a necessidade de maior dotação orçamentária para o setor de inteligência.

VI.1.4. Criação de agência brasileira de inteligência de sinais

Com os avanços tecnológicos por que passa a sociedade internacional, é premente a criação de uma agência brasileira de inteligência de sinais, para operar no ambiente virtual tanto na busca de dados negados de interesse do Brasil quanto na proteção dos ativos nacionais nessa área. Note-se que esta agência não pode ter apenas caráter defensivo.

Outra observação importante diz respeito ao fato de que a proposta de criação de uma agência nesses moldes deve ser originária do

Poder Executivo, por determinação constitucional. Não cabe, assim, proposição legislativa originária do parlamento para criar órgãos da administração pública.

VI.1.5. Estabelecimento de uma Política Nacional de Inteligência de Sinais, de uma estratégia e de planos nacional e setorial

Para a implementação de medidas concretas de proteção e defesa, com o objetivo de que o país fique mais seguro nesse campo cibernético, é essencial que se estabeleça uma Política Nacional de Inteligência de Sinais (PNIS), que se coadune com a PNI, a Política Nacional de Defesa (PND) e outras políticas públicas. Essa medida requer um amplo debate, do qual participem o Poder público e a sociedade civil.

A Política estabelece os objetivos. É um documento norteador das atividades e organizações do setor. A Estratégia, por sua vez, dispõe sobre os caminhos que se pretende seguir para se alcançar os objetivos. Com uma Política e uma Estratégia, planos deverão ser traçados para definir que procedimentos devem ser adotados, por quem e em que prazos, para alcançar os objetivos.

VI.1.6. Criação de uma comissão temporária, no âmbito do Senado Federal, para propor reformas na legislação brasileira de inteligência

Percebe-se também a necessidade de ampla reforma na legislação brasileira de inteligência. Para isso, recomenda-se a criação, no âmbito do Senado Federal, de comissão temporária para estudar o tema, propor uma agenda de discussões e, finalmente, apresentar projetos

legislativos de reforma do arcabouço normativo brasileiro sobre inteligência.

VI.1.7. Aprovação da PEC nº 67, de 2012

Dentre as reformas no arcabouço normativo brasileiro, medida relevante é a aprovação da PEC nº 67, de 2012, que eleva a atividade de inteligência ao nível constitucional, estabelecimento um sistema de inteligência consentâneo com o modelo democrático e que opere em defesa do Estado e da sociedade. A referida PEC, que traz, ainda, mais garantias aos cidadãos e aos setores de inteligência em suas atividades de produção e proteção ao conhecimento, e dispõe sobre mecanismos de controle dos serviços secretos, será um marco para o desenvolvimento da inteligência no Brasil. Recomenda-se, portanto, a urgente aprovação da PEC nº 67, de 2012.

VI.1.8. Aprofundamento dos mecanismos de controle externo da atividade de inteligência

Certamente, grande êxito alcançado enquanto esta CPI conduzia seus trabalhos foi a aprovação da Resolução nº 2, de 2013, do Congresso Nacional. A referida Resolução 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". Estabelece objetivos e competências da Comissão, sua composição, regras de funcionamento e relações com os entes controlados.

Aprovado o Regimento Interno da CCAI, deve-se, a partir de então, estimular os trabalhos do referido órgão de controle e, por meio dele, conforme dispõe a própria Resolução nº 2, 2013-CN, promover reformas na legislação de inteligência e fomentar a atividade dentro dos preceitos democráticos e sobre controle constante, permanente, funcional e finalístico realizado pelo Congresso.

VI.2. Conclusões em relação ao inquérito instaurado pela Polícia Federal

Conforme consta da nossa análise do inquérito levado a efeito pela Polícia Federal, é improvável a comprovação da materialidade do delito e, consequentemente, da indicação de autoria. Nesse sentido, só existe crime quando o agente pratica uma conduta típica, sem estar coberto por dirimentes, como legítima defesa, estado de necessidade ou exercício regular de direito. Esse enquadramento, para o caso em análise, não se verifica.

No caso dos tipos aventados pela Polícia Federal – arts. 13 e 14 da Lei de Segurança Nacional, e 10 da Lei nº 9.296, de 1996 –, os crimes são submetidos à lei brasileira se as condutas tiverem sido praticadas no Brasil, não se aplicando o critério de extraterritorialidade previsto no art. 7º, II, *b*, do Código Penal – ter o crime sido praticado por brasileiro –, uma vez que não se verifica o requisito a que alude a alínea *b* do § 2º do mesmo dispositivo legal – ser o fato punível também no país em que foi praticado. Isso porque a legislação sobre vigilância de inteligência

estrangeira, combinada com o *Patriot Act*, dá, em tese, amparo à ação praticada em território estadunidense.

Independentemente disso, há mesmo dificuldade em delinear a conduta criminosa supostamente praticada. Não havendo a comprovação da materialidade, não há como prosperar o inquérito a cargo da Polícia Federal, nem há razão para esta CPI avançar nessa investigação. Diante disso, os objetivos da CPI ficam voltados para o aprimoramento dos sistemas de segurança das comunicações e de contrainteligência.

VI.3. Recomendações em relação à segurança das comunicações

VI.3.1. Ações no universo institucional

VI.3.1.1. Elaboração de uma Estratégia Nacional de Segurança Cibernética

Unanimidade entre os convidados à CPI, é mais urgente do que a elaboração de uma Estratégia Nacional de Segurança Cibernética, que delineie, dentre outras questões, as principais medidas de segurança cibernética para o Estado brasileiro e que englobe ações coordenadas entre os setores público e privado.

Tendo em vista que a segurança cibernética é cada vez mais considerada como uma questão nacional, horizontal e estratégica, que afeta todos os níveis da sociedade, uma estratégia de segurança cibernética nacional é importante ferramenta para melhorar a segurança e a resiliência

da infraestrutura e dos serviços nacionais. É uma abordagem de alto nível, de cima para baixo, que estabelece uma série de objetivos e prioridades nacionais que devem ser alcançados em um período de tempo específico.

As primeiras estratégias nacionais de segurança cibernética começaram a aparecer durante os primeiros anos da década anterior. Um dos primeiros países a reconhecer a segurança cibernética como uma questão estratégica nacional foram os Estados Unidos. Em 2003, os EUA publicaram a Estratégia Nacional para Segurança no Ciberespaço. Era uma parte da estratégia nacional global para a Segurança Interna, que foi desenvolvida em resposta aos ataques terroristas de 11 de setembro de 2001.

Embora o Ministério da Defesa tenha publicado a Estratégia Nacional de Defesa, em que ações de domínio cibernético constam como objetivo prioritário, restritas, portanto, e como não poderia deixar de ser, ao setor militar e à defesa cibernética, e que em seguida foi publicada a Política Cibernética de Defesa[70], também do Ministério da Defesa, caberia

---

[70] Política Cibernética de Defesa, estabelecida pela Portaria Normativa nº- 3.389/MD, de 21 de dezembro de 2012. O objetivo é orientar as atividades de defesa cibernética, no nível estratégico, e de guerra cibernética, nos níveis operacional e tático, no âmbito das Forças Armadas. As diretrizes serão aplicadas nos grandes eventos que serão sediados no país até 2016. Com a nova política, o Ministério da Defesa (MD) busca assegurar o uso efetivo do espaço cibernético (preparo e emprego) pelas Forças Armadas e impedir ou dificultar sua utilização contra os interesses do país. Deverão ser criados e normatizados processos de segurança cibernética para padronizar os procedimentos de defesa da rede. Deverão também ser estabelecidos programas e projetos para assegurar a capacidade de atuar em rede com segurança. A portaria também prevê a criação do Sistema Militar de Defesa Cibernética (SMDC), que contará com a participação de civis e militares da Marinha, do Exército e da Aeronáutica. É atribuição do SMDC coordenar e integrar as ações de defesa cibernética, no âmbito do MD, nas áreas de inteligência, ciência e tecnologia, operacional, doutrina e recursos humanos. A implementação e

ao governo brasileiro elaborar uma Estratégia Nacional abrangente, que reunisse ações para todas as esferas da segurança cibernética, inclusive para o setor privado.

Entende-se que uma Estratégia Nacional deva, no mínimo:

- definir claramente o âmbito e os objetivos da estratégia, bem como a definição de requisitos para segurança cibernética;

- assegurar a participação de todos os departamentos governamentais, reguladoras nacionais, autoridades e outros organismos públicos, de forma que todas as preocupações sejam ouvidas e tratadas;

- garantir a entrada e participação de representantes da indústria, universidades e do cidadão;

- colaborar com outros Estados, em especial com os do Mercosul e da Unasul, para garantir cooperação transfronteiriça e que a segurança cibernética seja tratada de uma forma coerente com o entorno de segurança do Brasil;

---

gestão do novo sistema é responsabilidade do Estado-Maior Conjunto das Forças Armadas (EMCFA).

- reconhecer que, devido ao constante desenvolvimento e evolução do ciberespaço, a estratégia terá que ser um documento dotado de flexibilidade e mudança;

- ter ciência de que tal evolução não significa apenas ameaças emergentes e novos riscos, mas também oportunidades para melhorar e aumentar o uso das tecnologias da informação e comunicação para o governo, a indústria e os cidadãos;

- considerar o trabalho que tem sido feito até agora para melhorar o nível de segurança nacional, evitando a duplicação de esforços e concentrando-se em novos desafios.

Para se ter uma melhor dimensão da importância do tema, 14 países da União Europeia e outros 10 nações de outras regiões do globo já publicaram suas estratégias de segurança cibernética. Abaixo listamos alguns extratos de estratégias nacionais adotadas por alguns países selecionados e o ano em que foram divulgadas[71]:

- Estônia (2008): sua estratégia nacional enfatiza a necessidade de um ciberespaço seguro em geral e concentra-se em sistemas de informação. As medidas recomendadas

[71] National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace. European Network and Information Security Agency (ENISA), 2012.

são de caráter civil e focam em regulamentação, educação e cooperação.

- Finlândia (2008): a base da estratégia é uma visão de segurança cibernética como um problema de segurança de dados e como uma questão de importância econômica que está intimamente relacionada com o desenvolvimento da sociedade da informação finlandesa.

- Eslováquia (2008): garantir a segurança da informação é tido como sendo essencial para o funcionamento e desenvolvimento da sociedade. Portanto, o objetivo da estratégia é desenvolver um quadro abrangente. Os objetivos da estratégia estão focados principalmente na prevenção, bem como a disponibilidade e sustentabilidade.

- República Checa (2011): os objetivos essenciais da estratégia de segurança cibernética incluem a proteção contra as ameaças a que os sistemas e tecnologias de informação e comunicação estão expostos, e a mitigação das potenciais consequências em caso de um ataque contra as TIC. A estratégia se concentra principalmente no livre acesso aos serviços, à integridade e à confidencialidade dos dados do ciberespaço da República Checa e é coordenado com outras estratégias e conceitos relacionados.

- França (2011): a estratégia nacional francesa se concentra na capacitação de sistemas de informação para

resistir a eventos no ciberespaço que poderiam comprometer a disponibilidade, integridade e confidencialidade dos dados. A França ressalta tanto meios técnicos relacionados com a segurança dos sistemas de informação e de luta contra a cibercriminalidade quanto o estabelecimento de uma ciberdefesa.

- Alemanha (2011): concentra-se na prevenção e repressão de ataques cibernéticos e também na prevenção de falhas de TI, especialmente quando infraestruturas críticas estão em causa. A estratégia define o terreno para a proteção de estruturas de informação críticas. Ele explora os regulamentos existentes para esclarecer se poderes adicionais são necessários para garantir a manutenção dos sistemas de TI na Alemanha, por meio de prestação de funções básicas de segurança certificados pelo Estado.

- Lituânia (2011): tem como objetivo determinar os objetivos e tarefas para o desenvolvimento de informações eletrônicas, a fim de garantir a confidencialidade, integridade e acessibilidade da informação e serviços prestados no ciberespaço eletrônico, a salvaguarda de redes de comunicações eletrônicas, os sistemas de infraestrutura crítica contra incidentes e os ciberataques, a proteção dos dados pessoais e da privacidade. A estratégia também define as tarefas, que, quando implementadas, permitirão total segurança do ciberespaço e entidades que operam nele.

- Luxemburgo (2011): reconhecendo a penetração das TIC, a estratégia afirma que a prioridade é evitar quaisquer efeitos adversos sobre a saúde e a segurança pública ou na economia. Menciona-se também a importância das TIC para os cidadãos e a sociedade e para o crescimento econômico. A estratégia é baseada em cinco linhas de ação, que podem ser brevemente resumidas como: proteção das infraestruturas críticas e resposta a incidentes; modernização do quadro legal; cooperação nacional e internacional; educação e conscientização, e promoção de normas.

- Países Baixos (2011): a Holanda tem como objetivo garantir segurança e confiabilidade para as TIC contra abusos e interrupções em larga escala, e, ao mesmo tempo, reconhece a necessidade de proteger a abertura e a liberdade da internet. A Holanda inclui uma definição de segurança cibernética na estratégia como sendo "cibersegurança é estar livre de perigo ou dano causado pelo abuso, rompimento ou queda das TIC, que podem causar limitação da disponibilidade e confiança das TIC sobre a confidencialidade da informação armazenada ou dano à integridade da informação".

- Reino Unido (2011): a abordagem está concentrada sobre os objetivos nacionais ligados à evolução da segurança cibernética, fazer do Reino Unido a maior economia da inovação, de investimento e de qualidade no domínio das TIC e por este ser capaz de explorar

plenamente o potencial e benefícios do ciberespaço. O objetivo é combater os riscos do ciberespaço como ciberataques de criminosos, terroristas e Estados, de modo a torná-lo um espaço seguro para os cidadãos e empresas.

VI.3.1.2. Criação de uma agência para segurança cibernética

Diversos convidados presentes à CPI defenderam a necessidade de que as ações relacionadas à segurança cibernética devessem ser centralizadas num único órgão. A exemplo de outros países que já implementaram órgãos específicos para a segurança cibernética, cabe ao Brasil discutir a possibilidade de criar uma agência no âmbito da administração pública federal para segurança cibernética.

Em vista da distribuição descoordenada dos assuntos relacionados à segurança cibernética pelo governo brasileiro, o governo não tem uma visão de conjunto do assunto e ações mais eficazes tendem a não ser executadas. A inexistência de uma instituição central responsável compromete ainda a tomada de posições interna e externamente.

Alternativamente à criação de um novo órgão, poder-se-ia aproveitar a estrutura de órgão já existente, modificando suas atribuições, para lhe conferir capacidade de atuar, com independência, sobre o tema em sua totalidade e em estreita coordenação com as agências reguladoras setoriais envolvidas nos mais diversos temas que englobam a segurança cibernética.

Dessa forma, propõe-se que o Estado desde já se organize de forma a discutir as possibilidades institucionais que levem à centralização institucional da segurança cibernética na estrutura do governo brasileiro. É importante que se conceda a um órgão governamental específico a atribuição de responsabilidades sobre os temas de segurança cibernética e segurança das infraestruturas críticas nacionais. Caberia a esse órgão da administração pública federal a organização do setor cibernético brasileiro, a responsabilidade de propor políticas e regulamentos voltados para a totalidade da segurança cibernética, com exceção, preferencialmente, dos aspectos relacionados à defesa e guerra cibernética – que devem restar ao Ministério da Defesa – tirando proveito dos ganhos sinérgicos da atuação em conjunto.

Estados Unidos, Reino Unido, Alemanha, Coréia do Sul e Japão são alguns dos países que já adotaram comandos unificados para a segurança cibernética. Seus modelos devem ser extensamente analisados pelo Estado brasileiro.

No Reino Unido, por exemplo, o *Office of Cyber Security and Information Assurance* (OCSIA), vinculado diretamente ao Primeiro-Ministro, foi criado após a publicação da Estratégia de Segurança Cibernética de 2009, e tem como atribuições auxiliar na determinação de prioridades, direcionamento estratégico e coordenação do programa de segurança cibernética do governo. O OCSIA ainda busca identificar e trabalhar com áreas que apresentam falhas, insuficiências ou estão buscando fazer frente às ameaças cibernéticas, estendendo sua autoridade para agências governamentais, cidadãos e empresas.

VI.3.1.3. Fomento a Pesquisa, Desenvolvimento e Inovação, combinando ações de investimento em empresas, universidades e ICT para a geração de sistema de Segurança Cibernética

Em alguns depoimentos coletados pela CPI, ficou claro que a construção de estratégias de segurança, defesa e defesa ativa cibernética passa pela necessidade de altos investimentos em pesquisa, desenvolvimento e inovação. Recomenda-se, portanto, ao Poder Executivo, que avalie a pertinência de enviar esforços nesse sentido, observando alguns passos que normalmente são seguidos mundo afora, a saber:

a) Identificar tecnologias nas quais as pesquisas devem se focar;

b) Contratar empresas que serão responsáveis pelo desenvolvimento das competências nas áreas indicadas;

c) Incentivar a criação de *startups* e identificar recursos humanos que serão contratados por estas grandes empresas;

d) Estabelecer programa de viabilização dos resultados da pesquisa acadêmica em efetivos produtos conduzidos por empresas preferencialmente nacionais;

e) Incentivar empresas internacionais detentoras de tecnologias de interesse do Estado brasileiro dispostas a se estabelecer em território nacional com transferência de tecnologia para produtos;

f) Estabelecer centros de inovação e criação de empresas para setores específicos;

g) Programar programa de incentivo a retenção dos recursos humanos no Brasil e atração de novos;

h) Instituir centros propulsores de inovação e criação de empresas para setores específicos;

i) Criar programa de incentivo a empresas internacionais detentoras de tecnologias, de interesse do Estado brasileiro, dispostas a se estabelecer em território nacional com transferência de tecnologia para produtos de TIC e SIC.

Pode-se criar, assim, um processo auto-alimentado, no qual grandes empresas fomentam a criação de pequenas empresas - mais ágeis com o foco bem delimitado - que criar suas próprias tecnologias, e que terão como primeiro cliente o governo. Quando estas pequenas empresas começam a produzir seus produtos, estes são ofertados no mercado privado.

Assim sendo, a criação das ferramentas, métodos e processos tanto para a segurança, quanto para defesa e defesa ativa, terão que ser contínuos. Nesse sentido, cada ator terá que desenvolver competências visando objetivo previamente definido. Por outro lado, o governo passa a ter papel fundamental por meio do comprometimento de aquisição das tecnologias, do estabelecimento de infraestrutura de inovação, da declaração de missão via ações que permitam:

a) Desenvolver tecnologias críticas para a segurança cibernética (*hardware* e *software*);

b) Estruturar o ecossistema digital de segurança cibernética em uma atmosfera motivada para o desenvolvimento e inovação;

c) Fortalecer grupos de pesquisa na área;

d) Incrementar núcleos de pesquisa e desenvolvimento, que integre as diversas agências do governo;

e) Definir ação orçamentária que permita estabelecer uma perspectiva de investimento em segurança cibernética.

VI.3.1.4. Ações para reforçar a Segurança Nacional em redes de telecomunicações que fazem uso do espectro de radiofrequências

O espectro de radiofrequências é um recurso escasso, considerado um bem público do Estado brasileiro. Este serve como um meio físico fundamental, assim como as redes cabeadas, para o tráfego de comunicações públicas ou privadas, incluindo aquelas do mais alto caráter estratégico e sigiloso.

O espectro é utilizado por meio de equipamentos de telecomunicações que estabelecem enlaces de radiocomunicação para os mais diversos serviços e finalidades. Estes incluem sistemas de comunicações que vão desde o radioamador, segurança pública, comunicações aeronáuticas, marítimas, exército, exploração da terra, pesquisas espaciais, sistemas comerciais e públicos via satélite até o cotidiano e atualmente mais presente na vida dos cidadãos brasileiros, pela sua expressiva penetração, que é o Serviço Móvel Pessoal (SMP).

A gestão ineficaz do espectro de radiofrequências nacional seria uma acentuada vulnerabilidade à Segurança Nacional em telecomunicações. Portanto, o Estado deve, em atendimento aos preceitos da Lei n.o 9472, de 1997 (Lei Geral de Telecomunicações) garantir à Anatel os recursos humanos, orçamentários e tecnológicos necessários e essenciais à gestão eficaz do espectro de radiofrequências.

VI. 3.1.5. Uso do poder de compra (Lei nº 12.349, de 2010) adicionados de uma política geral de PD&I para segurança cibernética, o que resultará na construção de uma nova indústria de segurança e defesa cibernética em torno de ações de governo.

No contexto da segurança e da defesa de sistemas governamentais, priorizar a aquisição de hardware/softwares nacionais e certificados se torna uma questão estratégica.

VI.3.1.6. Segurança das infraestruturas críticas nacionais

O Estado e o setor privado têm, ainda que de maneira tímida e insuficiente, com diferentes níveis de prioridade, âmbito e estados de maturidade, investido na proteção das infraestruturas críticas (IC). No entanto, a maior parte destes planos são isolados (por entidade) e não estão devidamente enquadrados num âmbito nacional ou internacional.

Entendem-se por infraestruturas críticas não apenas as estruturas físicas, mas também os serviços, bens e sistemas, que se forem interrompidos ou destruídos total ou parcialmente, poderão provocar impactos social, ambiental, econômico, político, internacional ou à

segurança do Estado e da sociedade. Este impacto poderá ser em um ou mais campos, simultaneamente ou não.

A Resolução do GSI Nº 002, de 24 de outubro de 2007, após aprovação dos Ministros que integram a CREDEN e dos Comandantes Militares de Força, propôs ao Presidente da República incluir o tema Segurança de Infraestrutura Crítica (SIEC) em área de sua competência e instituir o Grupo Técnico de Segurança de Infraestrutura Crítica (GTSIEC) visando implementar medidas e ações relacionadas à questão, iniciando pelos setores de energia, transporte, água e telecomunicações

Na sequência, o Decreto nº 6.371, de 12 de fevereiro de 2008, atendeu à sugestão da CREDEN, constituindo-se, assim, no marco legal para as atividades relacionadas com a segurança de infraestruturas críticas, incluindo os serviços.

A Estratégia Nacional de Defesa (END) de igual maneira aborda o tema e propõe que o incremento do nível de Segurança Nacional passa pela proteção das infraestruturas críticas nacionais. Além do mais, a Estratégia atribui aos Ministérios da Defesa, Minas e Energia, Transportes, Integração Nacional e das Comunicações, a missão de adotarem medidas para a segurança das infraestruturas críticas nas áreas de energia, transporte, água e telecomunicações.

Nessa ação estratégica, coube ao GSI a missão de coordenação, avaliação, monitoramento e redução de risco.

Assim, sugere-se ao Poder Executivo avaliar a pertinência de:

a) Reforçar a implementação do Guia de Referência para a segurança das infraestruturas críticas da informação, publicado em novembro de 2010 pelo Gabinete de Segurança Institucional.

b) Determinar o nível de interdependência entre as infraestruturas críticas dos diversos setores da economia, em especial, dos setores de energia, transportes, comunicações e financeiro.

c) Obter informações sobre as vulnerabilidades das infraestruturas críticas (inclusive as infraestruturas críticas de informação), excetuando-se informações confidenciais, estratégicas e críticas de autenticação e uso sob proteção legal, para permitir gerir os riscos que possam afetar a segurança das infraestruturas críticas.

d) Fomentar a implementação de sistemas que permitam identificar, analisar, avaliar e tratar os riscos conjuntos das infraestruturas críticas nacionais sejam elas públicas ou privadas.

e) Avaliar a atribuição a órgão governamental de um sistema nacional de proteção das infraestruturas críticas nacionais.

f) Reforçar os requisitos de segurança das infraestruturas críticas de forma a aumentar sua capacidade de resistir a ataques cibernéticos desenvolvendo para isso legislação ou regulação apropriada aplicável aos setores público e privado.

g) Especificar melhor a distribuição das tarefas e responsabilidades entre as agências governamentais de forma a alcançar uma organização mais eficiente da diante das ameaças cibernéticas.

h) Dotar os Ministérios e as agências com atribuições de resguardar as infraestruturas críticas nacionais de recursos humanos, financeiros e tecnológicos para a consecução de tais objetivos.

i) Ampliar, tendo em vista que parte significativa da infraestrutura crítica nacional pertence ao setor privado, os níveis de coordenação entre os setores público e privado é vital para reduzir as vulnerabilidades atuais.

j) Atentar não somente para as ameaças virtuais, mas também para proteção física das infraestruturas críticas nacionais.

k) Manter normatização brasileira atualizada com as recomendações internacionais.

Para além disso, convém recordar que os membros da comunidade internacional terão que trabalhar em conjunto para rastrear e tratar as ameaças cibernéticas que ultrapassam fronteiras. Os países também terão que trabalhar em conjunto para compartilhar dados técnicos no sentido de manter atualizadas suas defesas cibernéticas. *Hackers*, por exemplo, rotineiramente compartilham informações sobre novas técnicas que podem penetrar as estruturas de defesa. As nações precisam fazer o mesmo para proteger as suas próprias infraestruturas de TI, a mesma estrutura de TI, que afeta todo o globo.

Enquanto muitos analistas acreditam que tratados globais são um fator essencial para o desenvolvimento de uma política sólida de segurança cibernética global, alguns também sugerem a criação de medidas de fortalecimento da confiança no ambiente cibernético (*confidence building measures*) como alternativas aos tratados globais, ou como medida paliativa, já que tratados são vistos como não verificáveis, inaplicáveis e impraticáveis.

Qualquer que seja o arranjo é unânime o entendimento de que as ameaças cibernéticas devem ser tratadas no plano multilateral sob o risco de tornarem medidas exclusivamente internas ineficazes. Isto posto, cabe ao governo brasileiro estabelecer prioridades de atuação em política externa que busque formas de organizar o ambiente internacional que preze pela segurança cibernética e pela soberania das nações.

O Brasil deve cooperar intensamente com organizações regionais e internacionais e com outros países de forma bilateral, tanto para capacitar-se por meio de troca de experiências internacionais e informações compartilhadas, como para criar redes de relacionamento que auxiliem na construção de confiança mútua no cenário internacional.

O País também precisa oferecer equipes de resposta a incidentes, capazes de cooperar e atuar internacionalmente a qualquer momento, dando volume e concretude técnica aos mecanismos políticos e diplomáticos de atuação.

VI.3.2. Ações no universo das pessoas

É certo que, por melhor que seja um planejamento, seu sucesso dependerá da sua adoção por parte pessoas a que ele se dirige, isto é, no presente caso, aos usuários de sistemas de informação. Assim, é essencial que sejam implementadas, por órgãos competentes do Poder Executivo, campanhas e ações que disseminem a cultura de segurança digital na população brasileira como um todo.

VI.3.2.1 Promover a cultura de segurança digital

É essencial aumentar a consciência sobre segurança da informação entre usuários individuais de computadores e pequenas e médias empresas, informando-os sobre ameaças existentes no ciberespaço e ampliando o conhecimento sobre segurança dos computadores e outros dispositivos informáticos.

VI.3.2.2 Criar iniciativa nacional de informação para o público em geral

Essa iniciativa deve ser baseada em plataforma *online*, contendo informações claras sobre os casos de ameaças cibernéticas e como os usuários da internet podem fazer para tornar suas atividades na rede mais seguras. Um exemplo interessante de iniciativa semelhante é o *Get Safe online*, no Reino Unido.

VI.3.2.3 Desenvolver cartilhas educativas para diversos públicos alvos, tanto para o setor público quanto para o setor privado.

VI.3.2.4 Coordenar a distribuição de informação sobre ameaças e organizar campanhas de cooperação e trocas de informações entre os setores.

VI.3.2.5 Promover cursos de capacitação em diferentes níveis para agentes públicos e privados.

VI.3.2.6 Criar incentivos nas universidades públicas e privadas para formar profissionais em segurança cibernética.

VI.3.2.7 Modernizar a grade curricular das Universidades de Engenharia de Telecomunicações e Redes do País adequando-a à necessidade de um maior estímulo ao desenvolvimento de tecnologia nacional em

telecomunicações e, principalmente, à ampliação da consciência técnica quanto a aspectos de Segurança Nacional em telecomunicações;

VI.3.2.8 Criar uma escola ou universidade de segurança cibernética, ou estimular a criação de centros universitários sobre segurança cibernética tanto no domínio das ciências humanas quanto nas exatas.

VI.3.2.9 Estabelecer convênios de cooperação com as principais institutos e centros de segurança cibernética no mundo, como IMPACT/ITU, Cooperative Cyber Defence Centre of Excellence (CCD CoE), em Tallinn, Estônia.

VI.3.2.10 Promover, no âmbito da administração pública, concursos de testes de segurança para investigar possíveis vulnerabilidades, a exemplo como é realizado pelo TSE para testes da urna eletrônica.

VI.3.2.11 Promover exercícios de ataque e defesa cibernética com a participação de agentes públicos e privados de forma a capacitar o pessoal humano para ações reais.

VI.3.2.12 Participar de exercícios de simulação internacionais como forma de intercambiar experiências com outros Estados e Centros de Segurança. Segundo estudos publicados recentemente, embora muitos gestores de segurança da informação percebam a importância de participar de exercícios nacionais e internacionais, muitos poucos profissionais participam efetivamente de tais simulações.

VI.3.2.13 Treinar os gestores de sistemas em medidas de segurança e identificação de riscos.

VI.3.2.14 Desenvolver o potencial de mobilização militar e nacional para assegurar a capacidade dissuasória e operacional relacionadas a Segurança Cibernética

VI.3.2.14.1. Elaborar e manter atualizado um banco de talentos de pessoal de interesse para a mobilização em prol da Segurança Cibernética;

VI.3.2.14.2. Adequar as necessidades de mobilização do pessoal a ser empregado na Segurança Cibernética ao SINAMOB;

VI.3.2.14.3. Elaborar Plano de Mobilização de Equipamento, Instalações e Pessoal, com respectivos custos em consonância com a Lei de Mobilização Nacional;

VI.3.2.14.4. Realizar levantamento sistemático de equipamentos, instalações e pessoal passíveis de serem mobilizados em prol da Segurança Cibernética, quando necessário

VI.3.2.14.5. Realizar campanhas nacionais de educação sobre Segurança Cibernética, visando à Mobilização Nacional, para elevar o nível de conscientização da sociedade brasileira.

VI.3.3 Ações no universo das tecnologias

No âmbito das tecnologias, também se recomenda ao Poder Executivo enviar esforços para:

VI.3.3.1 Desenvolver algoritmos nacionais de criptografia

Um dos pontos centrais da segurança na internet é a criptografia, que tem como objetivo: confidencialidade, integridade, autenticação e irretratabilidade sobre mensagem a ser trocada. Assim sendo, é necessário o uso de programas de criptografia que atendem os objetivos descritos anteriormente através da implementação de algoritmos matemáticos, tornando-a ilegível para aquele que não possui a chave de decodificação no destino.

Recorrente na CPI foi a constatação da necessidade de se desenvolver programas de criptografia nacionais capazes de atender aos requisitos de proteção dos órgãos do governo, das empresas estatais e das maiores empresas privadas brasileiras. Tais programas devem garantir a interoperabilidade entre os sistemas e evitar o isolamento digital.

Para que seja possível esse desenvolvimento são necessárias políticas específicas de fomento e investimentos.

VI.3.3.2 Desenvolver hardwares nacionais de comunicação

Pelo menos no âmbito governamental deveriam ser priorizados o uso de dispositivos nacionais que tenham sido auditados e certificados, garantindo uma maior segurança e independência de tecnologias estrangeiras.

A indústria nacional deve ser estimulada para atingir nível de maturidade tecnológica de padrão internacional, buscando competitividade em qualidade, custo e compatibilidade tecnológica com outras redes de comunicações internacionais.

VI. 3.3.3 Investir na segurança da nuvem no País

A segurança cibernética ganha mais importância no cenário de crescente desenvolvimento das tecnologias de computação em nuvem que é uma tendência mundial.

Nos EUA, por exemplo, o governo Obama criou o posto de CIO – *Chief Information Officer* – pessoa responsável por pensar, planejar, orientar e articular toda a estratégia e operações federais de TIC e suas aplicações. Em 2010, o alvo era fechar, até 2015, 800 dos 2.094 *datacenters* federais. Quarenta por cento dos *datacenters* serão fechados porque novas formas de coletar, processar, conectar, compartilhar e preservar dados estão disponíveis e permitem, através de seu uso criativo e inovador, realizar muito mais com muito menos, em termos de investimento em informática e sistemas de informação em rede e da capacidade de processá-los e preservá-los de forma segura.

Vê-se, pois, que a construção de um ambiente digital seguro depende do pleno controle sobre a rede de comunicações digitais e do tráfego de aplicações nesta rede. É, portanto, imperativo que o país tenha o controle do domínio da tecnologia de nuvem e de sistemas de proteção para esse ambiente. Porém, a lógica do modelo em nuvem mantém a produção e desenvolvimento tecnológico no país de origem do fornecedor, o que fragiliza as iniciativas locais de prover segurança e desestimula o desenvolvimento tecnológico.

Nesse sentido, as oportunidades de simplificação de infraestrutura e ganhos de escala nos sistemas de informação e seu

desenvolvimento, manutenção e evolução, criadas por infraestrutura e *software* como serviço, na nuvem, deveriam ser combinadas com a necessidade de mais e melhor governança como apontadas pelo relatório do TCU.

VI.3.3.4. Investir na produção e comercialização de *softwares* brasileiros, em especial antivírus e para troca de mensagens.

É necessário o fomento da indústria e da academia de forma a permitir o desenvolvimento de *softwares* nacionais, de forma independente dos grandes centros produtores mundiais de tecnologia.

É imperioso, por igual, o estabelecimento de programa de pesquisa e desenvolvimento, com código e bibliotecas totalmente nacionais, em particular para aplicação na administração pública federal em geral e no Ministério da Defesa, em especial. Além disso, a definição de um processo de homologação e certificação dos *softwares* e ratificado por Órgão da Administração Pública.

Uma política com esse intuito, além de fomentar a expertise brasileira no tema, também possibilitará a geração de empregos e de divisas através do comércio local.

VI.3.3.5. Estimular o desenvolvimento de produtos brasileiros para monitoramento e proteção dos níveis de segurança.

Ainda como forma de tornar o país independente de equipamentos e soluções estrangeiras, que por vezes fragilizam nossa segurança cibernética, deve-se investir no desenvolvimento de produtos

para monitoramento das redes e em ferramentas de análise de vulnerabilidades dos ativos de TI e da rede, garantindo ao mesmo tempo competitividade internacional em termos de custo e qualidade.

VI.3.3.6. Investir no lançamento de cabos óticos submarinos do Brasil para outras regiões com vistas a diminuir a dependência dos Estados Unidos para comunicação com outras partes do globo.

VI.3.4 Ações no universo dos processos

Em maio de 2011, o Tribunal de Contas da União informava que havia "uma total ausência de comprometimento dos altos escalões com a área de Tecnologias da Informação e Comunicação (TIC), do governo federal". O TCU vem analisando a infraestrutura e os sistemas de informação de governo sob várias perspectivas e de forma sistemática desde 2007.O interesse do Tribunal e sua influência sobre os negócios federais de informática vêm de longe; houve um aumento de 15 vezes no número de decisões do TCU sobre "contratações de TIC" entre 1995 e 2010. Isso dá uma ideia da importância que o Tribunal credita às tecnologias de informação e comunicação e suas aplicações nos serviços e na gestão pública.[72]

Em estudo de 2010, o TCU levantou que mais da metade das instituições públicas fazia *software* de forma amadora; mais de 60% não tinham na prática política e estratégia para informática e segurança de informação, e 74% não tinham nem mesmo as bases de um processo de

---

72 http://interessenacional.uol.com.br/index.php/edicoes-revista/estamos-sendo-observados-e-dai/

gestão de ciclo de vida de informação. Ainda, 75% não gerenciavam incidentes de segurança de informação, como invasão de sites e sistemas e perdas ou pior alteração de dados, e 83% não faziam ideia dos riscos a que a informação sob sua responsabilidade estava sujeita.

O relatório aponta ainda que quase 90% dos órgãos não classificavam a informação, o que significa que a instituição está sob provável e permanente caos informacional. Como se isso não bastasse, quase 100% dos órgãos da administração direta e indireta não tinham um plano de continuidade de negócio em vigor. O que quer dizer que se o lugar fosse atingido por uma pane elétrica grave, enchente, raio ou incêndio, a comunidade-alvo de seus serviços poderia ficar semanas sem ser atendida e haveria descontinuidades muito sérias do ponto de vista da história da informação no governo e nos serviços públicos.

Ademais, o relatório informa que quase metade dos órgãos não designou um comitê de gestão para TIC, e quase 60% dos altos gestores das organizações não estabeleceram objetivos de gestão e uso para a área de TIC e, finalmente, 76% não estabeleceram indicadores de desempenho para a área. No estudo seguinte, publicado em fins de 2012, pouca coisa havia mudado: o número de instituições capazes de gerir incidentes de segurança de informação, por exemplo, caiu em 1/3.

Em 2012, dando continuidade ao trabalho de acompanhamento da situação da governança de tecnologia da informação na administração pública federal, o TCU realizou nova auditoria, examinando os aspectos de liderança, estratégias e planos, cidadãos, sociedade, informações e conhecimento, pessoas, processos, e resultados. Disso resultou o Acórdão

nº 2585/2012 – TCU – Plenário,[73] que emitiu uma série de recomendações visando a introduzir melhorias na área, especificamente providências para melhoria do planejamento estratégico institucional e de TI; medidas para aumentar o número de servidores da área de informática nas instituições públicas e a capacitação dos responsáveis pelas atividades de gestão e fiscalização de contratos.

As ações que aqui sugerimos, com o objetivo de construir a necessária cultura de governança de TI no País, são baseadas nas recomendações contidas na radiografia realizada pelo TCU, adaptadas de modo a serem aplicáveis não só a instituições governamentais, mas, de maneira geral, às empresas brasileiras que se interessarem. É certo que poucas empresas têm porte para adotar todas as ações especificadas, mas muitas podem adotar algumas delas.

VI.3.4.1. Implementar instrumentos de planejamento estratégico institucional e de tecnologia da informação, dando-lhes ampla divulgação;

VI.3.4.2. Identificar os processos críticos de negócio e designar formalmente os gestores responsáveis pelos sistemas de informação que dão suporte a esses processos, à semelhança das orientações da ABNT NBR ISO/IEC 38500;

VI.3.4.3. Definir e formalizar metas de governança, como parte do plano diretor de tecnologia da informação da instituição, baseadas em parâmetros

---

73 http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D500BE942EEF7793E040010A89001367

de governança, necessidades de negócio e riscos relevantes, atentando para as metas legais de cumprimento obrigatório e as orientações da ABNT NBR ISO/IEC 31000;

VI.3.4.4. Ampliar a oferta de ações de capacitação em planejamento e gestão de contratos de tecnologia da informação;

VI.3.4.5. Elaborar plano de gestão de recursos humanos para o sistema de administração dos recursos de informação e informática;

VI.3.4.6. Manter ações que estimulem a capacitação de pessoal interessado em aperfeiçoar a governança de tecnologia da informação.

VI.3.5. Ações na Área Legislativa

VI.3.5.1 Projeto de Lei que dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiros a organismos estrangeiros.

Esta Comissão Parlamentar de Inquérito propõe a apresentação de Projeto de Lei do Senado **(ANEXO I),** com o objetivo de regulamentar o fornecimento de dados de cidadãos ou empresas brasileiros a organismos estrangeiros.

As pessoas naturais e jurídicas brasileiras têm direito à inviolabilidade e ao sigilo do fluxo de suas comunicações pela Internet, bem como à inviolabilidade e ao sigilo de suas comunicações privadas armazenadas, em ambos os casos salvo por ordem judicial. Ao mesmo tempo, faz-se necessário assegurar o livre fluxo de informações entre

autoridades governamentais e tribunais estrangeiros para a investigação e persecução de atos ilícitos, respeitando-se esses direitos.

Um dos principais problemas apurados por esta CPI diz respeito à falta de controle e de transparência a respeito das requisições de dados de pessoais naturais e jurídicas brasileiras por autoridades governamentais e tribunais estrangeiros. Com este PLS, espera-se suprir essa lacuna e permitir que o Poder Judiciário brasileiro exerça o controle necessário sobre esses procedimentos, divulgando de forma transparente essas requisições.

VI.3.5.2 Política Nacional de Segurança Cibernética

Em um país com dimensões continentais como o Brasil, a proteção do ciberespaço deve ser encarada de forma estratégica pelo Estado, pois desempenha papel essencial, tanto para a segurança e soberania nacional, como para a integração cultural e o desenvolvimento econômico.

Assim, entendemos que o país deve discutir e elaborar uma Política Nacional de Segurança Cibernética, com a participação de todos os órgãos envolvidos, de todas as esferas de poder. Diante disso, propomos ao Poder Executivo que seja criado Grupo de Trabalho com vistas a elaborar uma proposta de Política Nacional de Segurança Cibernética. A esse grupo caberia elaborar proposta de criação e adequação de legislação federal a fim de amparar as atividades de Segurança Cibernética, definindo atribuições, estabelecendo responsabilidades e reconhecendo autoridades para o exercício das atividades relacionadas à Segurança Cibernética.

VI.3.5.3 Criação de ações orçamentárias para viabilizar atividades de Segurança Cibernética

Propomos que o Poder Executivo inclua no próximo Projeto de Lei Orçamentária a ser encaminhado ao Congresso Nacional a criação de ações orçamentárias específicas destinadas a viabilizar as atividades de segurança cibernética.

ANEXO I

Projeto de Lei do Senado nº, de 2014

Dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiros a organismos estrangeiros.

O CONGRESSO NACIONAL decreta:

Art. 1º Esta Lei dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiros a organismos internacionais.

Art. 2º O fornecimento de dados relativos ao fluxo de comunicações, ou de comunicações privadas armazenadas, de cidadãos brasileiros ou de empresas brasileiras, para autoridade governamental ou tribunal estrangeiros, deverá ser previamente autorizado pelo Poder Judiciário brasileiro, observados, conforme o caso, os requisitos da Constituição Federal, da Lei Federal 9.296/96 e de tratados internacionais aplicáveis dos quais o Brasil seja signatário.

§ 1º. Sem prejuízo dos demais requisitos legais, o requerimento formulado por autoridade governamental ou tribunal estrangeiros deverá conter, sob pena de inadmissibilidade:

I – fundados indícios da ocorrência do ilícito;

II – justificativa motivada da imprescindibilidade dos dados solicitados para fins de investigação ou instrução probatória; e

III – período ao qual se referem os dados.

§ 2º. Salvo expressa previsão legal ou salvo expressa determinação judicial fundamentada em contrário, a autorização mencionada no *caput* somente poderá ser concedida após comunicação, pelo Poder Judiciário, ao cidadão ou à empresa cujos dados foram solicitados pela autoridade governamental ou tribunal estrangeiros, com informações que permitam o contraditório e a ampla defesa em juízo.

§ 3º. O Poder Judiciário deverá elaborar e publicar semestralmente relatório de transparência de requisições formuladas por autoridades governamentais e tribunais estrangeiros, a respeito de dados relativos ao fluxo de comunicações, ou de comunicações privadas armazenadas, de cidadãos brasileiros ou de empresas brasileiras, indicando o número, a natureza das requisições e se os dados foram ou não fornecidos.

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

JUSTIFICAÇÃO

As pessoas naturais e jurídicas brasileiras têm direito à inviolabilidade e ao sigilo do fluxo de suas comunicações pela Internet, bem como à inviolabilidade e ao sigilo de suas comunicações privadas armazenadas, em ambos os casos salvo por ordem judicial. Ao mesmo tempo, faz-se necessário assegurar o livre fluxo de informações entre autoridades governamentais e tribunais estrangeiros para a investigação e persecução de atos ilícitos, respeitando-se esses direitos.

Um dos principais problemas apurados por esta CPI diz respeito à falta de controle e de transparência a respeito das requisições de dados de pessoais naturais e jurídicas brasileiras por autoridades governamentais e tribunais estrangeiros. Com este PLS, espera-se suprir essa lacuna e permitir que o Poder Judiciário brasileiro exerça o controle necessário sobre esses procedimentos, divulgando de forma transparente essas requisições.

SENADO FEDERAL
SECRETARIA DE COMISSÕES

Reunião:15ª Reunião da CPIDAESP
Data: 09 de abril de 2014 (quarta-feira), às 14 horas
Local: Ala Senador Alexandre Costa, Plenário nº 13
CPI DA ESPIONAGEM - CPIDAESP

Assinam o Projeto:

TITULARES	SUPLENTES
Bloco Parlamentar da Maioria(PV, PSD, PMDB, PP)	
VAGO	1. Eunício Oliveira (PMDB)
Ricardo Ferraço (PMDB)	2. VAGO
Benedito de Lira (PP)	3. VAGO
Sérgio Petecão (PSD)	
Bloco de Apoio ao Governo(PSOL, PT, PDT, PSB, PCdoB)	
Vanessa Grazziotin (PCdoB)	1. Eduardo Suplicy (PT)
Walter Pinheiro (PT)	2. Lídice da Mata (PSB)
Anibal Diniz (PT)	
Bloco Parlamentar Minoria(PSDB, DEM)	
Pedro Taques (PDT)	1. VAGO
VAGO	
Bloco Parlamentar União e Força(PTB, PRB, PSC, PR)	
Eduardo Amorim (PSC)	1. Antonio Carlos Rodrigues (PR)
VAGO	

SENADO FEDERAL
Fl. nº 1041

ANEXO II

Resumo das audiências públicas realizadas

3ª Reunião, realizada no dia 17/09/2013 (ANP)

Objeto: Audiência pública com a Sra. Magda Chambriand, Diretora-Geral da Agência Nacional do Petróleo, Gás Natural e Biocombustíveis.

No dia 17 de setembro de 2013, a CPI da Espionagem, em conjunto com a Comissão de Assuntos Econômicos e Comissão de Relações Exteriores e Defesa Nacional, mediante Requerimento nº 6/2013, de autoria do Senador Ricardo Ferraço, Requerimento nº 56/2013, de autoria do Senador Randolfe Rodrigues e Requerimento nº 90/2013, também de autoria do Senador Randolfe Rodrigues, ouviu a Sra. Magda Chambriand, Diretora-Geral da Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP). O objetivo da audiência pública, conforme anotado nos Requerimentos, foi discutir acerca das denúncias sobre a possível espionagem em relação à Petrobrás.

Sra. Magda Chambriand iniciou sua exposição ressaltando que o banco de dados de exploração e produção da ANP não está ligado à internet e não funciona no prédio principal da agência. Informações acerca do banco podem ser obtidas no endereço eletrônico www.bdep.gov.br.

Explicou que o banco de dados armazena dados de exploração e produção de petróleo de gás coletados em 7,5 milhões de quilômetros

quadrados de bacias sedimentares. Esses dados foram coletados pela ANP, pelas empresas petrolíferas e por empresas de aquisição de dados. Já recebeu a visita de muitos órgãos governamentais, que tiveram ciência de seu funcionamento.

A seguir, a convidada explicou o que é o banco de dados. Trata-se de uma informação, que compõe o patrimônio do País, mantido e patrocinado pelo Governo. O objetivo do banco de dados é preservar e disseminar informações e dados técnicos, além de promover e regular as atividades da indústria do petróleo. Ressaltou que se armazenam dados brutos, sem qualquer interpretação. A interpretação é feita caso a caso.

Os dados técnicos são: dados geológicos, geofísicos, sísmicos, geoquímicos, aerolevantamentos e levantamentos terrestres gravimétricos e magnetométricos. Incluem-se os perfis de poços, os testes de poços, dados relativos a amostras e testemunhos coletados nos poços perfurados nas bacias sedimentares terrestres e marítimas.

Segundo a Lei do Petróleo, trata-se de parte do ativo petrolífero da União, sendo obrigação da ANP organizar e manter o acervo de informações e dados técnicos relativos às atividades reguladas.

A convidada esclareceu que é disponibilizado dado público, que é o dado adquirido em área da União. Nos casos de dados adquiridos por empresas de serviços, trata-se de um dado não exclusivo, mas garantida à empresa uma confidencialidade. A confidencialidade permite que e empresa possa vender esse dado durante certo tempo, mas por ser não exclusivo, outras empresas podem ter acesso a ele.

Os dados públicos são comprados diretamente da ANP, regulados pela Portaria ANP nº 114/2000. São vendidos por preços módicos, constituindo receita da agência, que garante a autossuficiência do

banco. Além das cotas gratuitas para universidades, brasileiros residentes no Brasil e empresas constituídas sob as leis nacionais podem ter acesso a esses dados.

Já os dados não exclusivos podem ser comprados da empresa de aquisição de dados, durante seu período de confidencialidade. O dado confidencial, adquiridos pelas empresas de petróleo, não são vendidos pela ANP. Trata-se de levantamentos sísmicos que uma empresa adquire em uma área contratada pela ANP e em um bloco adquirido e protegido por contrato ou poços perfurados. O período confidencialidade pode variar de dois a dez anos.

A convidada explicou que o banco de dados é extenso e é operado pelos funcionários da ANP e pela empresa terceirizada Capgemini, que pratica serviços de apoio à fitoteca e à operação. Ressaltou que os funcionários da empresa terceirizada são analistas de sistema, não tem habilidade para interpretar dados e não têm acesso ao dado passado por um sistema capaz de decodificar informações úteis para serem interpretadas. Possuem empresas de serviços de secretariado, recepção, limpeza e segurança.

Para interpretar as informações nos bancos de dados, Sra. Magda Chambriand afirmou que são usados *software* da Oracle, além de informações, *softwares* e máquinas da IBM, *softwares* de acesso ao banco de dados, Halliburton Access e link.

Explicou, ainda, que a disponibilização dos dados segue o seguinte procedimento: realiza-se o pagamento de uma DARF acessada no *site* da agência e os dados são gravados em DVD, HD externo ou disponibilizados para *download* em uma área sem conexão ao sistema principal.

Quem mais acessa os dados são as empresas de petróleo. Atualmente, contabilizam 44 empresas associadas, entre ela a Petrobrás. Os dados mais acessados são aquisições sísmicas, perfil de poço, pasta de poço e programas não sísmicos. Para as licitações, a ANP prepara um pacote de dados de informações.

Pra concluir, a convidada afirmou que a segurança de informações está em conformidade com os preceitos exigidos, possuindo uma sala-cofre. Há um núcleo de informática responsável pelo monitoramento e pela adequação do ambiente computacional do banco, de acordo com a Instrução Normativa nº 6, de 2013. Entretanto, frisou que a segurança é garantida por possuir um banco de dados desconectado da internet.

Encerrada esta primeira parte, a convidada foi questionada pelos parlamentares. A sequência foi iniciada pelo Relator da CPI, o Senador Ricardo Ferraço, que indagou o seguinte à Sra. Magda:

Pergunta 1 (Senador Ricardo Ferraço). Diante das denúncias do Sr. Snowden sobre a violação dos sistemas da ANP, foi questionado à convidada se haveria simetria, igualdade de oportunidades e isenção das informações no leilão do Campo de Libra.

Resposta da Sra. Magda: asseverou que os dados estão disponíveis em igualdade de oportunidades a todas as empresas. Ademais, a ANP controlou quantas empresas entraram no banco de dados e pediram acesso às informações para o leilão de Libra. Por fim, ressaltou que se trata de um dado público, o dado sigiloso será a interpretação dada por cada empresa.

Pergunta 2 (Senador Ricardo Ferraço). Questionou se não houve violação do sistema de informação e proteção que acarretasse desigualdade de oportunidades entre os participantes do leilão.

Resposta da Sra. Magda: disse que a igualdade é plena. Qualquer cidadão domiciliado no Brasil e toda empresa constituída sob leis brasileiras pode ir ao banco de dados buscar as informações. Ainda, a Petrobrás, apesar de ser operadora mandatária da licitação de Libra, com 30%, também necessitou adquirir os dados na ANP.

Pergunta 3 (Senador Randolfe Rodrigues). Perguntou qual é a atual empresa administradora do banco de dados da ANP. E como era feita essa administração antes de 2009.

Resposta da Sra. Magda: reafirmou que o banco de dados é administrado pelos servidores da ANP, além de contar com o apoio da empresa terceirizada de informática analítica Capgemini. Até 2009, a ANP trabalhava com um *software* da empresa Halliburton, de Dick Cheney, Vice-Presidente americano. Posteriormente, afirmou que a ANP ainda faz uso desse *software*.

Comentário (Senador Randolfe Rodrigues). Senador diz que por ser usado o *software* da empresa Halliburton, a inviolabilidade do banco de dados não é tão evidente, como afirmou a Sra. Magda. Ainda, ressaltou que, segundo denúncia do Sr. Snowden, os dados violados foram os fornecidos pela Petrobrás.

Resposta da Sra. Magda: explicou que para exploração e produção de petróleo são necessários *softwares*, e não há essa tecnologia

brasileira. E que apenas responderia pelos dados da ANP, a violação aos dados da Petrobrás saía de sua competência.

Pergunta 4 (Senador Roberto Requião). Afirmou que, em sua concepção, está clara a violabilidade do banco de dados da ANP, considerada por ele uma invasão insistente e consistente. Ressaltou que a Landmark geriu os dados da Petrobrás com *software* da Halliburton e, consequentemente, teve acesso a esses dados por dez anos. Ademais, fez referência ao furto de computadores da Petrobrás ocorrido em 2008, que estavam sendo transportados pela empresa de container também vinculada ao Vice-Presidente Cheney.

Sobre o leilão do Campo de Libra, o senador questionou seu formato, dizendo que favorece os Estados Unidos. Além disso, questionou o leilão, entendendo que se trata da entrega da área ao cartel internacional. Assim, declarou sua preocupação focada no desempenho da agência e a necessidade de estabelecimento de contraditório nas oitivas.

Resposta da Sra. Magda: explicou que a nova visão do Campo de Libra se deu com o levantamento sísmico, não exclusivo, adquirido recentemente pela empresa de aquisição de dados chamada CGG Veritas. O campo era muito maior do que as suposições da agência.

Sobre a estrutura da ANP, os funcionários são brasileiros concursados, cedidos de instituições públicas. Atualmente, conta-se com cinco diretores, todos concursados e indicados pela presidente da República, com processo de aprovação no Senado Federal. Ressaltou que

o trabalho é focado no interesse público e nacionalismo. Aplicam a política sancionada por lei, pelo Governo Federal. Mostrou investimentos que a agência faz em pesquisa e desenvolvimento, além da importância das parcerias tecnologias para o crescimento do Brasil.

Sobre o Campo de Libra, elucidou que é uma área de grande extensão, sendo necessário o trabalho de mais de uma empresa, por ser um grande desafio operacional, logístico, econômico e financeiro. O campo distancia-se 200 Km da costa brasileira, com demanda de poços que poderão alcançar 7 mil metros de profundidade e lâminas de água que podem ser superiores a 2 mil metros, com horizontes de sal de 2 km.

Pergunta 5 (Senador Ricardo Ferraço). Perguntou se a ANP armazena dados em nuvem.

Resposta da Sra. Magda: disse não fazem esse tipo de armazenamento.

Pergunta 6 (Senador Pedro Simon). O Senador leu uma carta escrita por Sr. Gabrielli, ex-presidente da Petrobrás, que demonstra sua preocupação com os leilões de petróleo, em especial com o leilão do Campo de Libra. Afirmou que diante das dúvidas e suspeitas de espionagem, o Governo deveria suspender o leilão do Campo de Libra.

Resposta da Sra. Magda: disse que as áreas Iara, Lula, Sapinhoá e Júpiter foram licitadas pela ANP. No caso de Franco, é uma cessão onerosa, devolvida à ANP pela Petrobrás, área BS-500.

Da mesma forma a área de Libra foi devolvida, proveniente do contrato BS-4, assinado com a ANP, liderado pela Shell. A empresa Shell, em parceria com a Petrobrás, descobriu Atlanta e Oliva e devolveu o restante da área que contém Libra. Posteriormente, sob a expectativa de que a área se tratava de uma bacia de gás, a área foi licitada, sem nenhum lance ofertado. Portanto, Libra se tornou área da União.

Pergunta 7 (Senador Flexa Ribeiro). Questionou se o leilão do Campo de Libra está sendo realizado segundo o regime de partilha estabelecido pela Lei 12.531, de 2010. Em caso afirmativo, como foi escolhido e qual será o critério de seleção da proposta vencedora? Ademais, questionou a possibilidade de diminuição da porcentagem da União do petróleo excedente, que poderia ficar abaixo dos 40% que o sistema de partilha garante.

Pediu explicações à convidada sobre o fato ocorrido em 2007, quando o geólogo da ANP, Sr. Paulo Araripe, trabalhou na agência e estava, ao mesmo tempo, contratado por uma consultoria do setor petroleiro.

Por fim, fez referência à pergunta deixada pelo Senador Aloysio Nunes: se uma empresa pode adquirir os dados da ANP de forma lícita, por que recorreria à espionagem?

Resposta da Sra. Magda: Sobre a negociação do contrato de partilha, afirmou que cabe a ANP implantar a política do Governo Federal. Assim, será a primeira área assinada sob regime de partilha de produção, assinatura realizada pelo Ministério de Minas e Energia.

Esclareceu que 15 bilhões de barris é uma quantia minimizada de produção do campo de Libra. E os ganhos não se limitam a produção. A participação governamental será de 75%, composta por *royalties*, imposto de renda, contribuição social e parcela de óleo para a União. A quantia corresponderá a R$900 bilhões em 30 anos.

A respeito da tabela de partilha, a Lei de Partilha determina que seja um único parâmetro de oferta. Mas as participações governamentais se alteram com a oscilação do preço do óleo. Consideram-se todos os parâmetros: produtividade, eficácia do projeto, variação do preço do petróleo. Assim, como a lei diz que o parâmetro será único, a resolução do CNPE determina que esse único parâmetro será uma célula da tabela que refletirá um situação média, configurada por uma variação.

Sobre a denúncia do funcionário que trabalhou na agência e estava, ao mesmo tempo, contratado por uma consultoria do setor petroleiro, afirmou que foi aberta uma sindicância, com julgamento realizado fora da ANP, na Controladoria-Geral da União. Disponibilizou cópia do processo, se for de interesse dos Senadores. Ressaltou a transparência no julgamento dos processos da agência.

Sobre o questionamento do Senador Aloysio Nunes, afirmou que não há necessidade de se recorrer a métodos não convencionais para obtenção de dados.

Pergunta 8 (Senadora Vanessa Grazziotin). Explicou que obteve informação de que o leilão do Campo de Libra não seria referente a lotes, e sim do campo como um todo. Desta forma, perguntou por que a

imprensa estava fazendo referência a informações privilegiadas de um e outro bloco.

Resposta da Sra. Magda: esclareceu que não há segundo lote no campo de Libra, será apenas um, sem nenhum segredo.

Pergunta 9 (Senador Eduardo Suplicy). Diante das denúncias de espionagem, sugeriu a suspensão do leilão do Campo de Libra.

Passando ao questionamento à convidada, perguntou se, com a suspensão do leilão, seria mais adequado novas regras, garantindo a igualdade de informações, ou a Petrobrás assumir a exploração direta do campo?

Por fim, perguntou à convidada se a espionagem não afetou o leilão.

Resposta da Sra. Magda: disse acreditar que as denúncias de espionagem em nada afetam o leilão de Libra. Reafirmou seu compromisso com o desenvolvimento nacional.

Pergunta 10 (Senador Inácio Arruda). Ressaltou a importância da ANP e a boa condução realizada pela Sra. Magda Chambriand. Definiu que dois assuntos foram abordados na audiência pública: a questão da espionagem brasileira e a exploração da área do pré-sal. Diante da complexidade da questão do setor minerário, o senador pediu maiores esclarecimentos sobre o regime de partilha, se é bom para o Brasil.

Sobre a decisão de se realizar o leilão do campo de Libra, defendeu que se trata de uma decisão da Presidente da República e do Conselho Nacional do Petróleo. É uma questão de natureza política, mas serão considerados apenas os aspectos técnicos.

Resposta da Sra. Magda: a convidada explicou que em 2008, foi criado um grupo interministerial que estudou o pré-sal. Dentre as conclusões, o regime de concessão tinha parâmetros econômicos para jazidas com porte menor do que as encontradas no pré-sal. A partir dessa conclusão, desenvolveu-se o estudo da licitação de partilha. Almeja-se uma participação governamental maior do que a definida nos contratos de concessão, na ordem de 75%.

Comentários do Senador Wellington Dias. Abordou a modelagem do sistema de partilha, em detrimento do regime de concessão. Ainda, discorreu sobre a participação mínima da Petrobrás em 30% e o interesse político acerca do tema. Elogiou a atuação da Sra. Magda Chambriand e afirmou que não há necessidade do cancelamento do leilão por motivos de espionagem americana.

4ª Reunião, realizada no dia 18/09/2013 (Petrobrás)

Objeto: Audiência pública com a Sra. Maria das Graças Silva Foster, Presidente da Petrobras.

A reunião foi presidida pela Senadora Vanessa Grazziotin, presentes, como membros da CPIDAESP, os Senadores Ricardo Ferraço, Benedito de Lira, Walter Pinheiro, Aníbal Diniz, Eduardo Suplicy, Lídice da Mata e Antônio Carlos Rodrigues.

A reunião foi realizada em conjunto com a Comissão de Assuntos Econômicos (CAE) e a Comissão de Relações Exteriores e Defesa Nacional (CRE).

Participaram dos debates a Senadora Vanessa Grazziotin e os Senadores Sérgio Souza, Walter Pinheiro, Delcídio do Amaral, Valdir Raupp, Pedro Simon, Eduardo Suplicy e Inácio Arruda.

A Sra. Maria das Graças Silva Foster tratou inicialmente da política de segurança empresarial da Petrobras. Explicou que a política de segurança empresarial faz parte da rotina da companhia, é elaborada por seus diretores e aprovada por seu conselho de administração. Destacou que a importância dessa política é observada por toda a hierarquia da companhia.

Sobre o conteúdo dessa política, considerou como ponto mais relevante a formação de uma cultura de segurança empresarial, que na Petrobras se inicia já no dia de admissão de um empregado. Notou que a formação de uma cultura de segurança empresarial há muito é tratada como

fator prioritário pela Petrobras, e afirmou que o primeiro a proteger as informações da companhia é o empregado.

Em seguida, explicou que na Petrobras a segurança empresarial é tratada de forma preventiva, o que implica prontidão contínua de resposta a incidentes, emergências e crises.

Destacou, então, duas das oito diretrizes da política de segurança empresarial da Petrobras:

> "- assegurar que as ações de segurança empresarial minimizem as ameaças por parte de pessoas ou organizações, em especial as externas ao Sistema Petrobras;
>
> - garantir que aspectos de segurança empresarial sejam sempre considerados no planejamento e na implementação de novos empreendimentos".

Após, falou sobre ataques cibernéticos. Informou que é um assunto discutido de forma sistemática na companhia e apresentou dados sobre incidentes reportados. Comentou que são diversos os motivos dos ataques, que podem se a ligar a atitudes de simples diversão ou a objetivos criminosos.

Ao iniciar o tópico da segurança da informação, enfatizou ser este um ponto em que a Petrobras investe e possui qualificação profissional.

Quanto ao investimento, informou o valor de R$ 3,9 bilhões para 2013, parte dos R$ 21,2 bilhões previstos pelo plano de negócios e gestão da companhia para o período de 2013 a 2017. Para ilustrar o significado da quantia, apontou que é quase equivalente ao previsto pelo mesmo plano para projetos e implantação da área de gás e energia e da área internacional somados.

Quanto aos profissionais qualificados, informou que a companhia dispõe de 3.114 especialistas nas áreas de tecnologia da informação e de telecomunicações, dos quais 243 são mestres e doutores.

A etapa seguinte da exposição abordou o Centro Integrado de Processamento de Dados (CIPD) da Petrobras, localizado no Rio de Janeiro. A Presidente da companhia apresentou imagens do centro e revelou-o como um dos pontos de orgulho da empresa.

Explicou que lá estão concentrados os principais bancos de dados e aplicações da companhia, que armazenam seu conhecimento explícito. Discorreu sobre a segurança do local, cujo acesso é restrito a poucos especialistas e controlado por diversas barreiras de proteção, e sobre a segurança da informação lá contida, que é armazenada com criptografia quando considerada crítica.

Afirmou que o CIPD é gerenciado pela própria Petrobras, sendo também atendido por 36 empresas de segurança da informação. Forneceu a listagem dessas empresas, destacando serem 14 norte-americanas e 16 brasileiras. Comentou, ainda, sobre a confiabilidade do CIPD, com disponibilidade certificada de 99,98% do tempo, e apresentou sua sala de operações de segurança, onde há o monitoramento ininterrupto e em tempo real da rede.

Sobre o envio de dados à Agência Nacional de Petróleo (ANP), distinguiu os dados geofísicos de perfilagem de poços e relatórios dos dados sobre indícios de petróleo e informações rotineiras de perfurações em andamento. Os primeiros não transitam pela internet: são enviados à ANP em meio físico ao término de cada aquisição sísmica, poço ou período exploratório. Já os dados sobre indícios de petróleo ou informações rotineiras de perfurações em andamento são constantemente

enviados pela internet à ANP, que, por sua vez, os torna públicos imediatamente. Mencionou ainda que, por haver transmissão pela internet, a Petrobras, logo após informar à ANP, comunica ao mercado a descoberta não comercial de indícios de acumulação de hidrocarbonetos.

A expositora descreveu também a rede de comunicação da companhia com suas unidades internacionais. Primeiro notou que a Petrobras tem ativos em 21 países, ilustrando seu caráter internacional. Em seguida, informou que a comunicação entre essas unidades e o CIPD é feita por circuitos dedicados alugados de concessionárias públicas com dados criptografados, quando pertinente. Duas ligações não usam circuitos dedicados, mas conexões protegidas via internet com túneis criptografados: uma com a Turquia e outra com a Líbia. Citou ainda as dez empresas de telecomunicação – de várias nacionalidades – e as três de criptografia – todas norte-americanas – que atendem a Petrobras nesse ponto.

Em seguida, detalhou o modelo corporativo a respeito de dados, informações e conhecimento. Pelo modelo, afirmou que conjuntos de dados isolados normalmente não possuem significado claro. Precisam ser trabalhados ainda em um longo ciclo, no qual o conhecimento corporativo é decisivo. Além disso, destacou que o modelo requer o aprimoramento e a atualização constante desses dados. Após explicar o modelo, demonstrou-o com o histórico da companhia.

Sobre a possibilidade de vazamento de dados, assim se pronunciou:

"Nós temos, então, hoje, uma discussão em torno do que possa ter vazado em algum ponto da Petrobras, já que o nosso nome – Petrobras – foi mostrado numa apresentação de PowerPoint num programa ao qual damos muito crédito, evidentemente, na TV Globo, o Fantástico, e depois

na imprensa, vimos o nosso nome ali, – Petrobras – o que nos causou, certamente, no mínimo, um grande desconforto."

"Não sabemos, definitivamente, se vazou, o que vazou, mas incomoda de forma profunda você assistir ao nome da sua empresa num programa que respeitamos e admiramos. Mas o fato é que o pacote de dados para Libra está à venda na Agência Nacional do Petróleo e hoje é o último dia para que seja feita a aquisição desse pacote."

Observou que as 42 empresas que atuam no setor são atendidas pelo mesmo grupo de fornecedores de bens e serviços que atendem a Petrobras. A indústria do petróleo é interligada e a gestão faz a diferença, concluiu.

Por fim, destacou que o ritmo das explorações é ditado pelo Governo e que existe margem de controle, inclusive para se considerar a nascente indústria nacional.

Encerrada esta primeira parte, foram formuladas perguntas pelos parlamentares. A sequência foi iniciada pelo Relator da CPI, Senador Ricardo Ferraço.

Pergunta 1 (Senador Ricardo Ferraço). Após a divulgação da denúncia, que providências a Petrobras adotou para verificar os ataques relatados? Qual seria o interesse da NSA na Petrobras?

Resposta da Sra. Maria das Graças Silva Foster: informou ter se reunido, no início do dia seguinte à divulgação da denúncia, com o gerente executivo, Sr. Álvaro, e sua equipe de técnicos que trabalham nas áreas de inteligência e de segurança empresarial, para tratarem do assunto. Constatou-se não haver necessidade de um levantamento exaustivo naquele

momento, pelo fato de que o processo de segurança existente na Petrobras ser, por sua própria natureza, exaustivo. Assim sendo, na reunião, onde se discutiu o assunto em profundidade, foi afirmado que não havia, em 2012 e 2013, nenhum registro anormal. A tecnologia que possuem, que consideram de ponta, não identificou nenhum ataque ao sistema.

Pergunta 2 (Senador Ricardo Ferraço). Considerando que existe um conjunto de informações que são estratégicas, dentro do conjunto tecnológico do Programa de Capacitação Tecnológica em Águas Profundas (Procap), o que é domínio exclusivo da Petrobras e o que é domínio compartilhado? Em síntese, quais informações interessariam aos concorrentes da Petrobras?

Resposta da Sra. Maria das Graças Silva Foster: esclareceu que a tecnologia é renovada a cada dia. Considerou que aquilo que a Petrobras tem de mais vantajoso frente aos concorrentes é a gestão de todo o processo. Neste sentido, ponderou que a empresa produz atualmente 326 mil barris de petróleo por dia no pré-sal, bem como fizeram a descoberta de Libra, que conhecem bem. Essencialmente, disse que interessaria aos concorrentes não apenas parte das informações, mas toda a Petrobras.

Pergunta 3 (Senador Ricardo Ferraço). Já houve registro de espionagem comercial? Que medidas foram tomadas para inibir tais práticas?A Petrobras possui unidade responsável pela segurança de informações e comunicações? Que meios dispõe, como se estrutura e a quem se subordina?

Resposta da Sra. Maria das Graças Silva Foster: conforme explanado, a pessoa responsável pela gestão do Centro Integrado de

Processamento de Dados da Petrobras é o Gerente Executivo Álvaro, presente à reunião. Esclareceu em sua resposta que o gerente executivo é vinculado ao diretor de engenharia da Petrobras, Sr. Figueiredo.

Pergunta 4 (Senador Ricardo Ferraço). Indagou como é tratado o conhecimento explícito da companhia e quais medidas adotadas para garantir que empregados e terceirizados preservem a segurança das informações da companhia. Como tema relacionado, considerando-se a legislação de combate ao terrorismo norte-americana, questionou como a Petrobras lida com informações estratégicas em seu relacionamento com empresas daquele país.

Resposta da Sra. Maria das Graças Silva Foster: em relação ao assunto, ponderou que fazem esforços para que a força de trabalho seja fiel à Petrobras, embora seja natural que pessoas deixem a empresa; no entanto, lembrou que, nestes casos, é impossível levarem a Petrobras. Considera que o que têm de nobre é o saber e a gestão, destacando que, na indústria do petróleo, valoriza-se muito a reputação das empresas, devendo-se honrar os termos de confidencialidade dos contratos de cooperação tecnológica.

Pergunta 5 (Senador Ricardo Ferraço). A Petrobras mantém algum vínculo com a Agência Brasileira de Inteligência (Abin)?

Resposta da Sra. Maria das Graças Silva Foster: informou que há histórico de atividades intensas e de períodos de menor proximidade. Recentemente, voltaram a ter um relacionamento mais próximo na elaboração de novos produtos com o objetivo de garantir a menor vulnerabilidade possível do sistema.

Pergunta 6 (Senador Ricardo Ferraço). Indagou se a Petrobras cumpre a Instrução Normativa GSI nº 1, bem como se segue as normas de classificação de documentos da Lei nº 12.527, de 2011, e os padrões internacionais de segurança da ISO 27.000.

Resposta da Sra. Maria das Graças Silva Foster: informou que a Lei nº 12.527, de 2011, levou a Petrobras a realizar a revisão da classificação de sua documentação. Explicou ter classificação que designa como NP1, 2, 3 e 4, na qual 3 e 4 seria aquilo que mais exige maior proteção. Quanto aos padrões de segurança, destacou que o sistema de informações está dentro da rede interna de computadores da Petrobras, sendo que o acesso ao Centro Integrado, CIPD, é restrito, sendo muito controlado.

Pergunta 7 (Senador Ricardo Ferraço). Indagou como se comportará a companhia no leilão do campo de Libra.

Resposta da Sra. Maria das Graças Silva Foster: esclareceu que, no que tange ao campo de Libra, a estratégia de participação somente poderá ser divulgada depois do dia 21. Embora existam vários técnicos na companhia atuando, cada grupo trata apenas de parte das informações. A definição da estratégia compete à Presidente e ao Diretor Formigli, Diretor de Exploração e Produção. Estas duas pessoas possuem a visão de conjunto das informações, de tal forma que somente no momento da entrega do envelope no leilão se terá notícia das informações pertinentes.

Pergunta 8 (Senador Ricardo Ferraço). Como é realizada a gestão da segurança e da informação pelas empresas com que a Petrobras

tem aliança que são sediadas no exterior, essas empresas que trabalham rede de proteção à informação?

Resposta da Sra. Maria das Graças Silva Foster: esclareceu que as empresas que trabalham com a Petrobras não conhecem o Centro Integrado, como um todo; conhecem somente o serviço para o qual foram contratadas. Além de existirem contratos firmados, quem realiza a governança da rede integrada de computadores do sistema, desenha a arquitetura do banco e das informações é a própria Petrobras, sob a gerência do Sr. Álvaro, Gerente de TI.

Pergunta 9 (Senador Ricardo Ferraço). Considerando que as denúncias feitas pelo programa Fantástico citam o nome da Petrobras, indagou se a companhia conseguiu alguma informação adicional do que na Petrobras foi ou teria sido violado, ou se avaliam como uma fantasia.

Resposta da Sra. Maria das Graças Silva Foster: ponderou não ser pertinente a designação de fantasia para o caso. Em sua avaliação e da Petrobras, não se trata de fantasia, embora não se saiba se houve ataque, tentativa de acesso, se foi possível capturarem alguma informação.

Pergunta 10 (Senador Walter Pinheiro). Indagou se a transferência de informações parciais se dá por meio de rede ou fisicamente, por meio de HD externo ou dispositivo semelhante.

Resposta da Sra. Maria das Graças Silva Foster: afirmou que a rede interna de computadores da Petrobras não transita por meio da internet. Trata-se de sistema acessado por poucos empregados, que têm acesso controlado para poder acessar fisicamente o ambiente. É realizado o monitoramento de quem acessou, de quem trabalhou e por quanto tempo.

Os dados que designara como "conhecimento explícito da companhia" não trafegam pela rede.

Pergunta 11 (Senador Ricardo Ferraço). Ainda que não exista identificação de violação ou que a equipe de TI da companhia não tenha essa identificação, a equipe considera possível que essa violação tenha sido alcançada e nenhum tipo de vestígio tenha sido deixado pelo caminho?

Resposta da Sra. Maria das Graças Silva Foster: reafirmou que o investimento que fazem é muito alto: 4 bilhões por ano, sendo R$ 21 bilhões só em segurança, TI, e telecomunicações no período de 2013 a 2017. Avalia que a Petrobras adota as melhores práticas mundiais na área, com investimentos e aperfeiçoamentos contínuos. Em sua visão, para se acreditar que houve invasão, seria necessário um registro de invasão e amostra do que foi capturado. No entanto, não possuem essa informação.

Concluídos os questionamentos por parte do Relator, a Srª. Presidente, Senadora Vanessa Grazziotin, formulou suas perguntas, seguindo-se posteriormente ordem estabelecida pela lista de inscrição.

Pergunta 12 (Senadora Vanessa Grazziotin). Indagou se, nos anos mais recentes, houve algum caso de captura ilegal promovida por algum servidor da Petrobras, alguém que tivesse acesso ao centro de armazenamento de dados.

Resposta da Sra. Maria das Graças Silva Foster: destacou que essa pergunta foi feita nesta semana muitas vezes aos técnicos de TI da empresa, tendo como resposta o fato de que não há evidência dessa entrada no sistema e de se terem capturado informações do sistema Petrobras.

Pergunta 13 (Senador Delcídio Amaral). Solicitou que a Sra. Graça Foster avaliasse as ações visando ao adiamento do leilão de Libra, tendo em conta que muitas empresas internacionais participarão e que se trata de projeto importante para a produção de petróleo e gás no Brasil.

Resposta da Sra. Maria das Graças Silva Foster: esclareceu que não é competente para definir questões de adiamento ou suspensão do leilão, não tendo autoridade para tanto.

Pergunta 14 (Senador Valdir Raupp). Considerando que as três empresas que tratam da criptografia utilizada pela Petrobras são americanas e que a NSA provavelmente teria acesso às informações dessas empresas, indagou que medidas foram adotadas pela Petrobras em relação a esta questão, após as denúncias divulgadas pela imprensa.

Resposta da Sra. Maria das Graças Silva Foster: confirmou que três empresas americanas fazem a criptografia da Petrobras. Destacou que são empresas com grande reputação no mercado e que certamente trabalham para manter essa reputação. Informou que há discussão quanto ao uso de algoritmos brasileiros, comentando que, com certeza, no momento em que empresas brasileiras se apresentarem à Petrobras, serão consideradas, da mesma forma que sempre consideram fornecedores de bens e serviços que possam substituir produtos importados. Indagada pelo Senador Ricardo Ferraço se, no momento, não há empresa nacional que disponha dessa tecnologia, respondeu desconhecer, mas acredita não existir.

Comentário do Senador Ricardo Ferraço. Considerando as respostas dadas, disse ter notícias de que o Casnav, Centro de Análises de

Sistemas Navais, da Marinha, teria oferecido sistema criptográfico à Petrobras. Acrescentou haver indicativos de que a Inteligência da Marinha estaria habilitada à produção de sistemas criptográficos, e da mesma forma a Abin, através do CriptoGOV e do cGOV. Assim sendo, solicitou à Presidente da Petrobras que, oportunamente, procurasse confirmar estas informações.

Pergunta 15 (Senador Valdir Raupp). Tendo em conta que a Petrobras tem importado bastante petróleo, porque ainda não é autossuficiente; que há reclamação da Câmara de Comércio Brasil-Irã de que o Irã tem oferecido petróleo para a Petrobras, em condições vantajosas para o Brasil, mas que não é possível concluir essa transação, em função do embargo americano, solicitou avaliação e informações sobre o caso.

Resposta da Sra. Maria das Graças Silva Foster: confirmou a existência de discussões envolvendo o Irã, com relação a produtos brasileiros e à compra e venda de petróleo. Trata-se de discussão que a área comercial do abastecimento da Petrobras tem tido com o grupo do Irã. No entanto, disse desconhecer pressões americanas que tornassem inviável essa relação comercial. Ressalvou que podem existir, mas reafirmou não ter conhecimento de sua existência.

Pergunta 16 (Senador Valdir Raupp). A exploração do shale gas pelo Brasil tiraria nosso País da dependência do gás boliviano? Em quanto tempo isso poderá acontecer?

Resposta da Sra. Maria das Graças Silva Foster: comentou que o gás boliviano é muito importante para o Brasil, não havendo previsão de não o contratar, até 2030. Com relação ao shale gas, disse haver

informações de caráter exploratório, com estudos das bacias sedimentares brasileiras, mas, embora tenham boas perspectivas, ainda é necessário conhecer seu verdadeiro potencial.

Pergunta 17 (Senador Eduardo Suplicy). Tendo em conta o leilão de Libra a ser realizado em breve, indagou se, caso tenha ocorrido espionagem dos dados da Petrobras pela NSA, poderia ter sido obtida informação relevante para efeito de eventual vantagem das empresas norte-americanas participantes.

Resposta da Sra. Maria das Graças Silva Foster: asseverou que, considerando as várias camadas de proteção que o sistema de informações da Petrobras possui, não há nenhum registro, nenhum sinal de ataque, de violação das informações, de forma geral. Em sua visão, para se ter mais informações e mais condições que a Petrobras tem atualmente, só capturando toda a Petrobras. Assim sendo, afirmou não ter, materialmente falando, elementos para que se possa justificar não realizar o leilão por conta de potenciais ou eventuais informações que desconhece. Destacou que também a Petrobras, comprou os dados, apesar da descoberta, manifestando-se perante a Agência, como todas as outras empresas. São dados transformados em dados públicos. Concluiu afirmando que todos, teoricamente, estão em iguais condições para participar do leilão.

Encerrada a fase de perguntas, após agradecer a presença da Presidente da Petrobras, a Presidente da CPI da Espionagem, Senadora Vanessa Grazziotin, encerrou a reunião.

6ª Reunião, realizada no dia 2/10/2013 (IPEA, Exército Brasileiro e UnB)

Objeto: Audiência pública com representantes do Instituto de Pesquisa Econômica Aplicada (IPEA), do Centro de Defesa Cibernética do Exército e da Universidade de Brasília (UnB), para discutir o tema "vulnerabilidades e segurança do Estado brasileiro no setor cibernético".

.

Realizada em 2 de outubro de 2013, a audiência pública tratou do tema "vulnerabilidades e segurança do Estado brasileiro no setor cibernético", trazendo os seguintes expositores: Sr. Samuel César da Cruz Junior, pesquisador do Instituto de Pesquisa Econômica Aplicada (IPEA); Sr. José Carlos dos Santos, General e Chefe do Centro de Defesa Cibernética do Exército; e o Sr. Pedro Rezende, Professor da Universidade de Brasília (UnB).

A reunião foi presidida pela Senadora Vanessa Grazziotin, estando presentes os Senadores Eduardo Suplicy, Pedro Taques e Ricardo Ferraço.

O **Sr. Samuel César da Cruz Junior** comentou sobre conclusões de alguns estudos realizados no âmbito do IPEA, em termos de segurança cibernética. Assim, ponderou: a) a segurança cibernética não pode ser atingida de forma plena, pois o espaço virtual envolve essencialmente, sistemas de informação e comunicação e de informática, e todos esses são suscetíveis a falhas; b) em decorrência dessa característica, a segurança cibernética deve ser um objetivo permanente dos governos; c) os investimentos em segurança devem ser de grande monta, pois cada infraestrutura a ser protegida é única, requerendo recursos físicos e

humanos específicos para atender a cada uma das demandas; e d) atualmente, China e Estados Unidos são os países mais maduros no que se refere à infraestrutura de segurança.

O **General José Carlos dos Santos** explicou como o setor cibernético é entendido pelo Governo brasileiro, as relações entre as várias instituições que tratam de segurança cibernética, as vulnerabilidades do sistema brasileiro de defesa cibernética bem como comentou sobre ações desenvolvidas pelo Ministério da Defesa (MD).

"Segurança cibernética" é um termo amplo, com objetivos e ações diferenciadas. Em níveis decrescente de entendimento, tem-se:

Nível político: o foco está na segurança nacional. No nosso País, o Gabinete de Segurança Institucional (GSI) é o órgão responsável por exercer o papel regulatório, estabelecendo normas e procedimentos a serem seguidos pela administração pública federal quanto à segurança da informação;

Nível estratégico: a preocupação é a defesa cibernética. No Brasil, as decisões ocorrem no âmbito do MD e a defesa cibernética está no mesmo patamar de relevância que os setores nuclear e espacial.

Níveis operacional e tático: o foco é a guerra cibernética e é de competência exclusiva das Forças Armadas.

Para o General, o setor de segurança cibernética deve ser tratado de forma sistêmica, havendo a coordenação e integração de cinco vetores fundamentais:

Educacional voltado a recursos humanos: em sua opinião, deve ser o vetor central da estrutura, responsabilizando-se pela capacitação da mão de obra especializada – hoje em quantitativo inferior à demanda – e pela criação de uma cultura voltada à segurança da informação na

população brasileira. Dessa forma, o Ministério da Educação (MEC) deve ser envolvido;

Doutrinário: a três órgãos distintos cabe a iniciativa de desenvolvê-los: a) GSI, estabelecendo normas e procedimentos para a Administração Pública Federal; b) Ministério das Relações Exteriores (MRE), defendendo a posição do Brasil sobre o tema em foros internacionais; e c) Ministério da Justiça (MJ), na aplicação da lei penal que tipifica crimes cibernéticos bem como no desenvolvimento de novos marcos regulatórios, como o Marco Civil da Internet.

Operacional: deve haver interlocução entre várias instituições, integrando ações, por exemplo, voltadas à segurança de grandes eventos.

Científico e tecnológico: a inovação é um aspecto essencial para a segurança cibernética, a fim de que o País deixe de ser dependente da importação de tecnologias. Dessa forma, o Ministério da Ciência, Tecnologia e Informação (MCT) deve ser envolvido, já havendo consenso que esta é uma área que precisa de altos investimentos.

Inteligência: deve-se desenvolver a capacidade de organização, seleção e análise dos milhões de dados disponíveis em fontes abertas, de modo a obter informações relevantes para o planejamento de segurança.

Em seguida, o palestrante analisou as vulnerabilidades atuais do Brasil:

Dependência tecnológica: a maior parte das redes instaladas no Brasil ou dependem de equipamentos importados ou dependem de operadoras sobre as quais o País possui limitada capacidade de auditagem. Ainda que a criptografia seja de desenvolvimento nacional, se o *hardware* for de fabricação internacional, não se pode garantir que o equipamento não tenha uma "porta dos fundos" (*backdoor*) que permita a transmissão de

dados sensíveis. Nesse sentido, lembrou que os fabricantes estadunidenses são obrigados, por meio do *Communications Assistance for Law Enforcement Act* (CALEA), a embutir, em seus produtos, *software* que permita às agências de inteligência dos EUA acessar dados que trafegam na rede. A solução da dependência tecnológica é de longo prazo, porém ações de mitigação podem implementadas em menor prazo, tais como: a aplicação, em larga escala, de contêiner e gerados de chaves nacionais e a revisão da lei pátria para obrigar que alguma agência nacional tenha condições de auditar os equipamentos utilizados nas redes brasileiras.

Carência de especialistas na área de segurança cibernética: atualmente, Ministérios e Exército não possuem um número de especialistas capaz de atender toda a demanda de serviços.

Orçamento para segurança cibernética muito inferior ao de outras potências mundiais: no Brasil, o orçamento inicialmente previsto para implantação do setor cibernético dentro do Exército foi de R$400 milhões a ser executado em quatro anos, sendo tal montante reduzido em virtude de cortes orçamentários em toda esfera federal. Sabe-se que as grandes potências mundiais investem montantes na casa dos bilhões de reais. O MD estima que, somente para acelerar a implementação de projetos já em andamento, é preciso dobrar o valor originalmente previsto para o setor.

Indefinição de um arcabouço legal: assim, por exemplo, é preciso que o Congresso Nacional discuta e aprove o Marco Civil da Internet, de forma a definir a posição brasileira em relação aos recursos, aos direitos e aos deveres, tanto em relações internas quanto em foros internacionais.

Em sequência, o General trouxe informações sobre a experiência nacional no setor de segurança cibernética. O setor teve início em 2010, com a atuação um núcleo integrante do atual Centro de Defesa Cibernética (CDCiber). Afirmou que a sistemática de trabalho do MD está baseada no tripé "Governo, instituições acadêmicas e indústria nacional" tem sido bem sucedida, trazendo exemplos de ações realizadas: *workshops* junto ao MCT para definição de projetos de interesse de defesa militar, bem como de interesse civil; desenvolvimento de *softwares* nacionais, tais como antivírus, simuladores de defesa e rádios; criação de laboratório no Instituto Militar de Engenharia voltado à inteligência artificial, análise de *malware*, criptografia e computação. Em sua opinião, em termos de ações concretas, o Brasil não está em situação de defasagem em relação a outros países e, com a experiência conquistada especialmente com a organização de grandes eventos no País, apesar do orçamento restrito, já é possível se pensar num modelo para a área de segurança cibernética a ser adotado. Por fim, ressaltou a importância de que, para continuar a evoluir no setor, o Brasil precisa estruturar uma agência de coordenação e integração nacional voltada a infraestruturas e sistemas críticos, tanto em âmbito público quanto privado. Como possível modelo de agência, citou o *Department of Homeland Security* (DHS) dos EUA, o qual regula a atuação das empresas do setor privado na operação de sistemas de telecomunicações, de transporte e de distribuição de água naquele país.

O último palestrante, o **Sr. Pedro Antônio Dourado de Rezende**, abordou, de forma acadêmica, o cenário geopolítico no qual se insere o tema da segurança cibernética. Como base teórica, adotou o ponto de vista do especialista americano em tecnologia de segurança, Bruce

Schneier, trazendo questionamentos que demonstram a complexidade do assunto em tela.

A primeira dificuldade surge com o conceito de segurança, pois este possui duas dimensões distintas e não comparáveis: um *processo real* que envolve probabilidades, que manipula chances de incidentes verterem em riscos ou de riscos verterem em danos; e um *sentimento pessoal*, que envolve percepções e que ajusta condutas para a adequação aos riscos considerados. Em decorrência, inexistem calibres de comparação entre as duas dimensões e o que se vive é o "teatro da segurança". Nesse teatro, encenam-se relações entre os dois planos da segurança, sendo cenários, enredos e contextos pertencentes ao plano dos processos que envolvem probabilidades de riscos se materializarem em danos. Assim, no contexto das denúncias feitas por Snowden, o que antes eram hipóteses de extensão e escopo da espionagem daquele que está na fronteira e no domínio da tecnologia, transformou-se em realidade mediante um processo midiático em que um indivíduo, por uma questão de consciência, resolve denunciar as ações de seu país, mesmo sabendo que sua vida correria riscos. Com esse novo cenário, a perspectiva subjetiva do que se pode considerar risco adequado ou aceitável para um Estado, para um indivíduo ou para uma empresa foi alterado. Como se percebe, a segurança cibernética e, portanto, a guerra cibernética, tem seu front decisivo na psique coletiva.

O termo segurança leva à ideia de proteção: proteção a algo, contra alguém. Dessa forma, a segurança cibernética está ligada a um planejamento adequado visando a proteger a informação. E nesse ponto chega-se a outra dificuldade: o conceito de informação. Não se confundem "dado" e "informação", pois esta é fruto de um juízo valor de quem recebe

o dado por meio de algum processo sensorial, havendo um processo interno de produção de significado. Como consequência, os diversos interlocutores podem entender e valorar o dado de formas distintas, levando a situações de conflitos de interesse quanto ao que se deseja de proteção relativa à informação – sigilo *versus* transparência. Porém, em alguns casos, a confusão de conceitos pode ser conveniente a uma das partes. Por exemplo, fornecedores de tecnologia podem preferir falar em "dados" e não em "informação" a fim de que, aqueles que procuram proteção, fiquem focados nos dados, tendo sua atenção desviada dos *interesses*. Dessa forma, tais fornecedores procuram passar uma ideia de neutralidade e, em tese, de não possuírem conflito de interesse com interlocutores que vão usar tecnologia para amplificar sua capacidade de comunicação.

Se o que trafega entre os computadores são apenas dados, e a informação surge com a produção de significado realizada por uma inteligência alheia, cumpre analisar o esquema de comunicação:

Interlocutores: a comunicação ocorre, geralmente, entre dois indivíduos, A e B, separados por uma distância, existindo entre eles um canal de confiança.

Canal de confiança: a distância entre A e B pode estar no tempo ou no espaço. Quando a distância entre A e B for temporal, para que se recupere, em T+1, o dado armazenado em T, é preciso lembrar onde o canal de confiança foi guardado ou, no caso de ter sido guardado com um controle de acesso, é preciso lembrar a senha. Quando for espacial, pode ser desejável o uso da criptografia para transmissão dos dados e, para tanto, é necessária a prévia distribuição de chaves criptográficas. Com o uso da tecnologia da informação, a necessidade de um canal de confiança tornou-se ainda mais crucial para uma comunicação segura, uma vez que o suporte

físico das relações pessoais tradicionais não está mais presente. Assim, alguns pontos precisam ser considerados para a proteção adequada: a) a entrada, no esquema de comunicação, de intermediadores tecnológicos – fornecedores de *hardware e software* – que podem ter seus próprios interesses estes, frequentemente, conflitantes com o dos interlocutores;[74] e b) a citada confusão entre "dado" e "informação", que acaba por prejudicar a capacidade de distinguir o que é sentimento e o que é processo no teatro da segurança. E nesse sentido, ressaltou a existência de atores interessados em insuflar sentimentos de adequação a um contexto de riscos como suficientes.

Contexto: para que um dado represente uma informação, é preciso haver um pano de fundo prévio, alguma expectativa do que pode ser comunicado através daquele dado. Nesse sentido, o canal de confiança pressupõe um contexto, mas esse canal tem uma extensão para dentro do dispositivo tecnológico utilizado para ampliar sua capacidade de comunicação e processamento.

Criptografia: o seu uso é parte do processo que transforma dados em informação, tendo capacidade de proteger apenas parte do trajeto da comunicação, ficando a outra, de responsabilidade do usuário. Porém, o que acontece na parte do usuário é que fica responsável pela proteção ainda que esta ocorra dentro da sua plataforma computacional, com a qual, muitas vezes, desconhece os detalhes dos processos em que símbolos são manipulados para codificar a informação.

---

[74] Citou, como exemplo, o conflito entre a privacidade do usuário e a licença de uso do *software* que roda em 95% dos computadores pessoais. Ao aceitar os termos da licença, dá-se ao fornecedor daquele software o direito de entrar na máquina do usuário particular, extrair o dado que quiser e entregar para quem quiser, desde que haja um motivo legítimo. O problema surge por não haver uma definição de "motivo legítimo".

Após exposição da base teórica, o palestrante discorreu acerca da geopolítica da guerra cibernética. Em seu entender, a ciberguerra pode ser vista como uma nova forma de guerra convencional, uma contrarrevolução digital, cujo paradigma é a virtualização destrutível.

O fenômeno da popularização da Internet em todas as relações e práticas sociais faz com que estas se tornem virtualizáveis. Ademais, a Internet, ao prover muitos serviços gratuitos, acaba for transformar as próprias pessoas, sua privacidade, em mercadorias. Se no capitalismo a evolução se dá por meio da "destruição criativa", então, num ambiente de ciberguerra, a primeira coisa a ser destruída será a privacidade e, posteriormente, a soberania nacional.

Assim como a guerra nuclear era a guerra estratégica da Era Industrial, a ciberguerra é a guerra estratégica da Era da Informação. Esta se tornou uma forma de batalha massivamente destrutiva, que diz respeito à vida e morte de nações, uma forma inteiramente nova, invisível e silenciosa, que está ativa não apenas em conflitos e guerras convencionais, mas também se deflagra em atividades diárias de natureza política econômica, militar, cultural e científica.

As características da guerra cibernética são:

Contrainformação: como já mencionado, o front decisivo da ciberguerra é o da psique coletiva, com a consequente expansão da esfera militar para a esfera pública. No entanto, há atores interessados em contradizer tal afirmação, tais como empresas de *software* de proteção e agências de Governo que cuidam de cibercrime preocupadas com a intrusão da área militar nas suas atividades, havendo a tentativa de demover o público da ideia de que a ciberguerra é algo real. Também alguns veículos de informação e formadores de opinião procuram negar a

realidade da ciberguerra. Para ilustrar, trouxe o exemplo em que a Folha de São Paulo reproduziu uma tradução de uma matéria da *Associated Press*, na qual, subliminarmente, passava-se a ideia de que a Presidenta do Brasil havia enlouquecido e pretendia isolar o País da Internet. No entanto, o que pretende a governante é obter controle contra a capacidade de bloqueio da telecomunicação brasileira pela distribuição de poder nos serviços que existem hoje no arranjo nacional das telecomunicações e da informática.

Novas armas táticas: lembrou o uso de *drones* por Forças Armadas como arma tática. Atualmente, os *drones* conseguem prospectar dados, levantado padrões de comportamentos suspeitos, que podem ter um risco maior de serem terroristas. Porém, a evolução natural de tal equipamento é sua completa automatização, inclusive para a programação de alvos.

Cerco normativo: o que se vê é a radicalização das normas, justificando, por exemplo, mesmo a criação de grandes bancos de dados biométricos ou mesmo ações militares letais, numa virtual guerra contra o terror. Em sua opinião, o objetivo na ciberguerra, é que as pessoas sejam adestradas a aceitarem um governo cuja forma de controle social é o vigilantismo global.

Bloqueios: recentemente foram vistos casos de bloqueio de espaço aéreo e expulsão de diplomatas.

Sabotagens: o próprio Brasil foi como alvo de ataque, sofrendo um blecaute. Na opinião do Professor, isso indica que, provavelmente nossa rede de distribuição elétrica está se transformando em campo de treinamento para quem está desenvolvendo arma cibernética para sabotar a distribuição elétrica no Planeta.

Virtualidade: não se consegue distinguir o que é real e o que é irreal, sendo que esta compreensão fica ainda mais prejudicada por grandes interesses econômicos em afirmar a não existência de uma guerra cibernética.

Por fim, foram apresentadas sugestões a serem tomados pelo Governo brasileiro:

Aprovar legislação sobre proteção de dados, na sociedade, no Estado e em comunicações militares.

Desenvolver alternativas tecnológicas para comunicações estratégicas e de contrainteligência, e fazera a sanitização de sistemas criptográficos.

Criar agência reguladora para inteligência e cibersegurança.

Recuperar o espaço do Estado no mercado das telecomunicações para serviços específicos, impedir que o controle fique totalmente em mãos de estrangeiros.

Desenvolver vias próprias de comunicação trans/intercontinental (satélite, redes de cabos ópticos) e viabilizar o VLS.

Homologar soluções de TIC livres para uso em serviços sensíveis.

Laura Poitras, não sofrem nenhuma intimidação ao passar pelo aeroporto londrino. E, quando são paradas, o interrogatório não dura mais do que uma hora. Todavia, por ter nacionalidade brasileira, a polícia inglesa o deteve e o interrogou por quase nove horas, questionando-o sobre diversificados assuntos e ameaçando prendê-lo, caso não colaborasse com as autoridades.

A motivação nuclear, no entanto, foi a de enviar uma mensagem ao Sr. Glenn, protagonista das recentes denúncias sobre espionagem. Tendo em vista a proximidade entre eles, o governo britânico, detendo David, esperava impedir Glenn de continuar publicando matérias que revelassem algo a respeito do sistema espionário arquitetado pelo grupo de países denominado "Five Eyes".[77] David acredita que sua detenção também serviu como forma de intimidar outros jornalistas que estão atuando nesse tema.

Essa segunda razão coaduna, inclusive, com um fato ocorrido na mesma época da detenção de David: a invasão do jornal "The Guardian", momento em que computadores e discos rígidos foram quebrados e "limpados". Mesmo assim, isso não obstaculizou o jornalista Glenn de prosseguir com seus relatos.

Quanto à postura tomada pelo Itamaraty neste incidente, o Sr. David a reputou aquém do esperado, na medida em que ela não ofereceu qualquer garantia futura para brasileiros que possam vir a passar pelo que ele passou.

Em seguida, a CPI passou a palavra ao Sr. Glenn Greenwald, que expôs, primeiramente, sua missão como jornalista. Apoiado na ideia de transparência e conscientização, ele disse que seu objetivo profissional é o

---

[77] *Five Eyes* ou "Cinco Olhos" é o grupo composto pelos EUA, Canadá, Reino Unido, Austrália e Nova Zelândia.

7ª Reunião, realizada no dia 9/10/2013 (Glenn Greenwald, e David Miranda)

Objeto: Audiência pública com o Srs. Glenn Greenwald, jornalista do jornal britânico "The Guardian", e David Miranda.

No dia 9 de outubro de 2013, a CPI da Espionagem,[75] mediante Requerimento nº 13/2013, de autoria do Senador Ricardo Ferraço, ouviu o jornalista Glenn Greenwald e seu companheiro, o Sr. David Miranda. O objetivo da audiência pública, conforme anotado no Requerimento, foi discutir e colher informações sobre as denúncias de eventual espionagem conduzida pela Agência de Segurança Nacional (NSA) dos EUA, e conhecer do ocorrido com o Sr. David, vítima de ação duvidosa da Polícia Metropolitana Britânica.

Falou em primeiro lugar o Sr. David Miranda. Alegou que sua detenção no aeroporto de Heathrow, em Londres, ocorrida no dia 18 de agosto de 2013, com base na Lei Antiterrorismo 2000,[76] teve duas principais motivações.

A primeira, o simples fato de ser brasileiro. Segundo ele, outras pessoas que também estão trabalhando com matérias sobre espionagem desenvolvida pela NSA, a exemplo da jornalista americana

---

[75] Criada conforme o Requerimento nº 811, de julho de 2013-SF, de autoria da Senadora Vanessa Grazziotin (PCdoB/AM) e outros Senadores, para, no prazo de cento e oitenta dias, investigar "a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal",

[76] Terrorism Act 2000, aprovado pelo Parlamento do Reino Unido.

de informar o público sobre o que os EUA vêm fazendo quanto à intimidade da população brasileira e mundial.

Nesse sentido, informou que suas reportagens se baseiam em documentos obtidos com Edward Snowden, sua fonte principal. Salientou que há parcerias com outros jornalistas do mundo, como foi o caso de matérias exibidas em parceria com jornalistas da TV Globo, fruto dessa cooperação.

Sublinhou que, devido ao volume e à complexidade dos documentos que possui, seu método de trabalho é o de compreender determinada parte da história e, assim, torná-la pública. Ele não fica à mercê do desfecho completo. Dessa maneira, à medida que as coisas acontecem, o Sr. Glenn as externaliza para a sociedade.

Em segundo lugar, alertou para o contexto em que estão sendo elaboradas as recentes reportagens. Há, nos dias atuais, uma verdadeira guerra contra o jornalismo investigativo, promovida, principalmente, pelos EUA e seus aliados (Inglaterra, Canadá, Austrália e Nova Zelândia). Esses países combatem a liberdade de imprensa e atribuem as atividades de jornalistas do jaez denunciativo como típicas de nações antidemocráticas, como a China, Irã ou Síria.

Diante disso, argumentou ser extremamente importante que os países beneficiários das últimas denúncias, como é a situação do Brasil, tenham ou desenvolvam um programa de proteção aos jornalistas e às sua fontes. Isso dará mais segurança e liberdade para que repórteres possam investigar os fatos relacionados à espionagem americana.

Por fim, falou do real motivo por que os EUA e aliados espionam certos países. A intenção é menos o combate ao terrorismo e a proteção nacional do que a obtenção de vantagens econômicas e aumento

do poderio estratégico. Segundo ele, o combate ao terrorismo é, na verdade, apenas o argumento utilizado para justificar a espionagem.

Encerrada esta primeira parte, os convidados foram questionados pelos parlamentares. A sequência foi iniciada pelo Relator da CPI, o Senador Ricardo Ferraço, que indagou o seguinte ao Sr. Glenn:

Pergunta 1 (Senador Ricardo Ferraço). No caso de quebra das comunicações por parte do Canadá, é mencionado um programa chamado Olympia. Existem mais informações sobre como este programa funciona, já que o que foi fornecido é muito superficial?

Resposta do Sr. Glenn: asseverou que todas as informações concernentes ao referido programa já foram publicadas. Futuras informações podem estar contidas no conjunto de documentos que possui, mas ainda estão sob análise. Acrescentou que a profundidade com que são abordados alguns assuntos depende da quantidade de documentos e informações disponíveis sobre eles. Assim, caso haja mais detalhes sobre o funcionamento do programa Olympia, isso será divulgado.

Pergunta 2 (Senador Ricardo Ferraço). É possível haver a antecipação de alguma denúncia futura à esta CPI, neste momento?

Resposta do Sr. Glenn: disse não haver planos para publicar material nos próximos dias que envolva o Brasil. O que existe são novidades acerca da espionagem desenvolvida pelo Canadá, a serem publicadas na mídia canadense .

Pergunta 3 (Senador Ricardo Ferraço). Dessa forma, não há mais denúncias ou informações a serem publicadas sobre o Brasil?

Resposta do Sr. Glenn (por David Miranda): reafirmou que, por ora, não há reportagem que inclua o Brasil. No entanto, existem muitos documentos para serem sopesados, e pode ser que haja algo relevante sobre nosso país e mereça ser publicado.

Pergunta 4 (Senador Ricardo Ferraço). Há evidências de denúncias importantes que possam revelar a violação de cidadãos brasileiros ou, então, informações estratégicas que foram obtidas sobre companhias brasileiras que realizarão manobras econômicas importantes nos próximos dias, a exemplo do Programa FX2, de reaparelhamento da Força Aérea Brasileira, e o leilão do campo de Libra, a ser feito pela ANP?

Resposta do Sr. Glenn: reiterou já ter publicado tudo o que sabia.

Pergunta 5 (Senador Ricardo Ferraço). Tendo em vista as recentes alegações da Sras. Maria das Graças Foster, Presidente da Petrobrás, e Magda Chambriard, Diretora-Geral da ANP, no sentido de não ter havido violação alguma de empresas brasileiras, oriunda de espionagem estrangeira, como o Sr. Glenn avalia essas afirmações? Quais são os elementos de violação não apenas da Petrobrás e da ANP, mas também de informações estratégicas da Defesa Nacional?

Resposta do Sr. Glenn: apesar de não saber mais nada sobre espionagem contra a Petrobrás, sustentou que o sistema de espionagem dos EUA é o mais forte do mundo, sendo difícil haver uma rede protetiva contra ela.

Pergunta 6 (Senador Ricardo Ferraço). Baseando-se na intervenção do Senador Pedro Taques, o Senador Ricardo Ferraço indagou ao Sr. Glenn se é possível colocar à disposição da CPI todos os documentos que atualmente encontram-se em seu poder, a fim de que a Comissão possa analisá-los com mais acuidade. Lembrou que, apesar de haver a possibilidade de mandado de busca e apreensão de tais documentos, o STF entende que esse pedido ofende o art. 5, XI da CF/88, que assegura a inviolabilidade domiciliar também a estabelecimento profissional.

Resposta do Sr. Glenn (por David Miranda): disse que esse pedido é inviável. Primeiro, porque são documentos sensíveis e contém informações de vários países, podendo ser configurado o crime de traição e Glenn ser impedido de voltar a seu país. Em segundo lugar, seu método de trabalho consiste em analisar cautelosamente cada documento e, assim, não pode dispor de seu objeto de análise de maneira incauta. Recordou os parlamentares que ele está fazendo jornalismo de muito risco, e que vem sofrendo ameaças pelos governos americano e inglês. É preciso que jornalismo e Estado se mantenham separados, para que cada um cumpra seu papel livremente.

Pergunta 7 (Senadora Vanessa Grazziotin). A Senadora Vanessa Grazziotin, aproveitando a temática, disse que as últimas espionagens divulgadas sobre o Ministério de Minas e Energia e a Petrobrás mostram uma apresentação de dados, realizada pela NSA contra a empresa brasileira. Na opinião do Sr. Glenn, os documentos demonstram que a NSA e as outras agências de espionagem fizeram apenas apresentações ou há ações diretas relacionadas à Petrobrás?

Resposta do Sr. Glenn (por David Miranda): informou que existem apresentações e ações contidas nos documentos, mas, no momento, não foram encontradas quaisquer ações diretas contra a Petrobrás. Edward Snowden saberia mais detalhes sobre esse assunto. Para isso, entretanto, teriam de ser-lhe assegurados proteção e asilo no Brasil. Quanto a isso, o Senador Ricardo Ferraço anuiu com o Sr. David e garantiu asilo a Edward Snowden, caso ele concorde em contribuir com a CPI.

Pergunta 8 (Senador Ricardo Ferraço). É evidente que os interesses canadenses no Brasil vão além do setor mineral, mesmo sendo este um dos ramos mais relevantes. Mas há que se lembrar da recente disputa entre duas importantes companhias internacionais: a brasileira Embraer e a canadense Bombardieu. Nesse passo, existem informações de que o governo canadense utilizou a espionagem para obter informações contra a Embraer, no intuito de fornecer vantagens comerciais ou tecnológicas para a Bombardieu?

Resposta do Sr. Glenn: disse que em artigo publicado no dia 7 de outubro, o jornal "The Guardian" demonstrou a correlação entre agências de espionagem e empresas. Conforme colocado por esse jornal, esses dois setores se reúnem pelo menos duas vezes ao ano.

Pergunta 9 (Senador Ricardo Ferraço). Um ex-funcionário de grande escalão do serviço secreto canadense afirmou ao "The Guardian" que os trabalhos desvendados no Brasil seriam apenas exercício de espionagem e que o país não é alvo real investigação. Na opinião do Sr. Glenn, essa afirmação é verdadeira?

Resposta do Sr. Glenn: asseverou que não é possível acreditar numa afirmação como essa. Seria muita ingenuidade crer que o Ministério de Minas e Energia foi apenas alvo de um exercício para que o serviço secreto canadense testasse suas habilidades espionárias.

Pergunta 10 (Senador Ricardo Ferraço). O Sr. Glenn sabe como as informações brasileiras são capturadas pelo sistema de espionagem estrangeiro? Elas são interceptadas nas saídas internacionais ou são colhidas onde os cabos brasileiros aportam?

Resposta do Sr. Glenn: afirmou que há documento publicado que relata como os cabos são invadidos pela NSA. Porém, não é detalhado qual cabo a NSA invade exatamente.

Pergunta 11 (Senador Ricardo Ferraço). Existem evidências de espionagem tradicional por meio de interceptações telefônicas realizadas diretamente nas redes de Telecom? Qual o nível de envolvimento das empresas brasileiras de telecomunicações?

Resposta do Sr. Glenn: redarguiu que não é possível afirmar, neste instante, algo sobre isso. É necessário averiguar se nos documentos que possui há alguma informação acerca das empresas brasileiras de telecomunicações e espionagem estrangeira.

Pergunta 12 (Senador Ricardo Ferraço). Há evidências de participação de empresas internacionais, que atuam no Brasil, no esquema de espionagem estrangeiro, a exemplo da AT&T?

Resposta do Sr. Glenn: afirmou que há matérias publicadas que explicam o sistema usado pela NSA contra outros países. Em síntese, a

NSA desenvolve um programa de cooperação com uma grande empresa de telecomunicação. Esta, por sua vez, faz acordos com empresas estrangeiras, permitindo o acesso a dados de cidadãos e de empresas estrangeiras. Disse que uma dessas empresas que participaram do programa com a NSA foi a AT&T. Assentou que várias empresas brasileiras possuem contrato com a AT&T, mas ele não pode afirmar que é a AT&T a empresa que coleta os dados e repassa para a NSA. Aliás, é esta a informação mais protegida da NSA: quais as empresas fazem parte do programa de cooperação.

Pergunta 13 (Senador Ricardo Ferraço). Há indícios de outros países, além dos integrantes do grupo "Five Eyes", estarem usando a inteligência de comunicações para fins de espionagem?

Resposta do Sr. Glenn: informou que existem três grupos que se relacionam com a NSA. O primeiro é o "Five Eyes", que exerce a função de espionagem e, ao que parece, não é espionado. Este grupo compreende os EUA, o Canadá, a Inglaterra, a Austrália e a Nova Zelândia. O segundo, é composto por alvos da NSA, mas que, às vezes, trabalham em conjunto com ela. É o caso, por exemplo, de Alemanha, França, Espanha e Itália. Um terceiro conjunto, e aqui se situa o Brasil, é preenchido apenas pelos alvos da NSA. Todavia, ele não sabe dizer se há outros países espionando o Brasil, além do Canadá, dos EUA e da Inglaterra.

Pergunta 14 (Senador Ricardo Ferraço). Há algum indício de quebra de dados criptografados durante as investidas recentes de espionagem?

Resposta do Sr. Glenn: asseverou que há indícios sobre essa ruptura de informações criptografadas, mas que elas não se referem ao

Brasil especificamente. Salientou, todavia, que ao se quebrar determinada informação secreta da internet, isso fragiliza o sistema, o que pode impactar futuramente o Brasil.

Pergunta 15 (Senador Ricardo Ferraço). V. Sa. ainda mantém contato com o Sr. Snowden?

Resposta do Sr. Glenn: afirmo que mantém contato com o Sr. Snowden, quase diariamente.

Pergunta 16 (Senador Ricardo Ferraço). É possível o Sr. Snowden contribuir para esta CPI, de forma mais objetiva, já que ele é a fonte primária das informações?

Resposta do Sr. Glenn: embora não possa falar pelo Sr. Snowden, o Sr. Glenn acredita que ele saiba mais detalhes sobre as espionagens desenvolvidas pelos EUA e aliados. Repisou, todavia, a necessidade de ele estar protegido para poder divulgar tais informações. Caso interesse à CPI, o Sr. Snowden pode ser contactado por meio de seu advogado, cujo endereço eletrônico é público e está disponível na internet.

Tendo em vista esta informação, o Senador Ricardo Ferraço manifestou a necessidade de serem formalizados dois requerimentos: um para o advogado do Sr. Snowden, para que consulte-o sobre a possibilidade de teleconferência com esta CPI; e outro para a missão diplomática da Rússia, país em que está asilado Snowden, com o fito de solicitar autorização do embaixador para esta interlocução.

Pergunta 17 (Senadora Vanessa Grazziotin). Em relação ao "Five Eyes", existe um acordo de cooperação entre os países componentes ou eles agem de maneira individual/

Resposta do Sr. Glenn: disse que há tanto colaboração entre os países do "Five Eyes" como atuação individual em tópicos específicos. Informou que este grupo se reúne com frequência para compartilhar informações capturadas mediante espionagem.

Pergunta 18 (Senador Ricardo Ferraço). Há cooperação de pessoa física ou jurídica com a espionagem dos EUA, isto é, empresas como Google, Facebook ou Skype têm relação com a NSA?

Resposta do Sr. Glenn: afirmou que um artigo publicado por ele já tratou desse tema. Reconheceu que muitas dessas empresas negaram ter relação ampla com a NSA. Mas ponderou que essa negativa se referiu ao fato de que a NSA não tem acesso ilimitado aos seus bancos de dados. O acesso é permitido apenas na dimensão em que a lei autoriza. Sucede que a lei dos EUA possui limites claros para cidadãos americanos, e quase não os têm para estrangeiros. Em verdade, para a espionagem estrangeira ser autorizada, basta que a NSA vá ao Tribunal Secreto e apresente seu programa de investigação que a ordem será concedida. Na prática, não há filtro algum.

Pergunta 19 (Senador Ricardo Ferraço). Qual a capacidade do Brasil em termos de contrainteligência e de proteção cibernética?

Resposta do Sr. Glenn: embora não seja perito, afirmou que existem várias propostas interessantes sendo desenvolvidas, não só no Brasil, mas também na Europa, para construir servidores independentes dos

EUA. Hoje, a raiz do problema é a internet depender, em grande parte, de servidores norte-americanos.

Pergunta 20 (Senadora Vanessa Grazziotin). V. Sa. já foi vítima de ameaças ou de algum tipo de intimidação?

Resposta do Sr. Glenn: reafirmou que, por trabalhar com jornalismo de alto risco, já sofreu várias ameaças, sobretudo do governo britânico. Este, aliás, informou que está em andamento uma investigação criminal contra ele, tendo por base as matérias lançadas nos últimos dias.

Pergunta 21 (Senadora Vanessa Grazziotin). Recentemente, o escritor búlgaro-germânico, Ilija Trojanow, foi detido em Miami pela companhia aérea American Airlines. V. Sa. tem informações sobre este caso?

Resposta do Sr. Glenn: disse que conhece o Sr. Ilija Trojanow e que ele é muito respeitado no meio jornalístico. Esclareceu que sua detenção se deu em razão da agressividade com que denunciou o sistema de espionagem da NSA contra a Alemanha.

Encerradas as perguntas, a Senadora Vanessa Grazziotin pediu que fosse elaborado um requerimento solicitando ao Itamaraty informações mais detalhadas sobre o incidente de detenção do Sr. David Miranda.

Após a aprovação de requerimentos, a Presidente da CPI da Espionagem, Senadora Vanessa Grazziotin, encerrou a audiência pública.

8ª Reunião, realizada no dia 15/10/2013 (Polícia Federal e Anatel)

Objeto: Audiência pública com a presença dos senhores José Alberto de Freitas Iegas, Diretor de Inteligência da Polícia Federal, e João Batista de Rezende, Presidente da Anatel.

No dia 15 de outubro de 2013, sob a Presidência da Senadora Vanessa Grazziotin, a CPI da Espionagem ouviu o Sr. José Alberto de Freitas Iegas, Diretor de Inteligência da Polícia Federal, e o Sr. João Batista de Rezende, Presidente da Anatel.

Após a abertura dos trabalhos, a Presidente da Comissão, Senadora Vanessa Grazziotin, apresentou breve síntese dos resultados obtidos pela CPI até o momento, no que tange às audiências públicas. Dentre as propostas ouvidas, destacou: que seja dada particular atenção ao marco civil da internet, em especial as questões da neutralidade, dos direitos do usuário e da governança; a criação da Agência de Segurança Cibernética, voltada para a proteção dos dados de defesa estratégica do Brasil; a utilização obrigatória de *softwares open source* no governo central, empresas estratégicas e estrutura de defesa; a obrigação da Anatel homologar somente o uso de roteadores sem *backdoor* pelas empresas de telecomunicações; a criação e estímulo à rede segura para tráfego de dados; e a proibição de participação em licitações de empresas que descumprirem legislação de proteção de dados pessoais. Destacou que estas propostas estão alinhadas com relatório aprovado pela União Europeia, bem como com as propostas apresentadas pela Presidenta Dilma Rousseff em seu discurso proferido na ONU.

O primeiro convidado a fazer uso da palavra foi o **Sr. José Alberto de Freitas Iegas**. Informou que, no âmbito da Polícia Federal, foi instaurado inquérito policial para investigar a possível quebra do sigilo das comunicações brasileiras e, a pedido do Diretor-Geral, Dr. Leandro Coimbra, entregou cópia integral do inquérito à CPI.

Com base nas denúncias em investigação, constatou a necessidade de aprimoramento do sistema de comunicação do Governo Federal, bem como da legislação da área de inteligência, especialmente no que tange às atividades relacionadas ao antiterrorismo.

No que diz respeito à atuação das empresas de tecnologia, afirmou que a maioria colabora com as investigações da Polícia Federal e cumpre integralmente as ordens judiciais recebidas. No entanto, algumas, em especial a Google, impõem obstáculos, alegando que, como a matriz está nos Estados Unidos, seria necessária a obtenção de ordem emanada de autoridade judiciária americana.

Como conclusão de sua exposição, destacou que há vulnerabilidades na área de informação, considerando o fator humano o mais importante, devendo ser objeto de investimento contínuo e especial atenção.

Em seguida, a CPI passou a palavra ao **Sr. João Batista de Rezende**, Presidente da Anatel, que tratou da confidencialidade no uso de redes de telecomunicações no Brasil e das ações realizadas pela Anatel em relação às notícias divulgadas pela imprensa após as revelações feitas por Edward Snowden.

O ponto de partida de sua explanação foi o direito à inviolabilidade da intimidade das pessoas, assim como a inviolabilidade do

sigilo das comunicações telefônicas e de dados, tendo como única exceção o cumprimento de ordem judicial, para fins de investigação criminal ou instrução processual penal. Neste sentido, frisou que a Anatel não armazena nem realiza interceptação de dados de ligações telefônicas, dados pessoais ou troca de informações na forma de e-mail ou mensagens.

A seguir, tratou das dimensões estratégicas da Internet e das telecomunicações, com foco na governança da Internet. Informou que há várias questões importantes relacionadas ao tema, que devem ser abordadas no marco civil, destacando as seguintes: comércio eletrônico, tributação e direitos do consumidor; direito à privacidade e à intimidade dos cidadãos; liberdade de expressão e direito à informação; inovação, novos modelos de negócios e defesa da concorrência; inclusão digital e massificação dos serviços; e segurança cibernética. Em sua opinião, o marco civil é uma oportunidade para analisar questões referentes à defesa das informações estratégicas do Estado.

No que diz respeito à mecânica das comunicações globais, explicou que para que usuários possam realizar chamadas internacionais ou utilizar seus terminais em *roaming*, são necessários acordos de interconexão internacional entre empresas brasileiras de telecomunicações e empresas em outros países. No momento da interconexão, há troca de informações de sinalização entre as operadoras, incluindo: número de origem, número de destino, duração e horário da chamada. Estes dados saem do país por canais como cabos submarinos ou satélites. Tendo em vista que as principais empresas da Internet são dos Estados Unidos, há concentração de tráfego e das receitas do setor naquele país. Em sua visão, o desequilíbrio do tráfego aumenta a vulnerabilidade das comunicações de brasileiros.

Após esta visão geral do mercado, passou a explanar sobre a atuação da Anatel em relação aos fatos divulgados pela imprensa. Neste sentido, informou que a agência iniciou procedimento de fiscalização, enviando uma série de perguntas para as principais empresas de telecomunicações para que fosse possível analisar as fragilidades nas redes, tendo por fundamento o fato de que as prestadoras são responsáveis pela inviolabilidade do sigilo das comunicações em toda a sua rede, bem como pela confidencialidade dos dados e informações. Destacou que este trabalho está sendo realizado em conjunto com a Polícia Federal.

Os principais temas abordados nos questionamentos foram os seguintes: 1) Política de controle de acesso a informações; 2) Controles de acesso (físico e remoto); 3) Política de proteção contra códigos maliciosos e vírus; 4) Procedimentos de *backup* e recuperação de dados e informações; 5) Contratos internacionais de *Roaming* e Interconexão; 6) Procedimentos e registros quanto a incidentes de segurança, Centros de Operações de Segurança (SOC) e coordenação com outros centros; e 7) Ações específicas em resposta à divulgação das notícias sobre a suposta espionagem feita pela *National Security Agency* (NSA).

Da análise das respostas recebidas, constatou-se que:

a) Todas as empresas consultadas afirmam possuir controle de acesso, embora nem todas sigam normas internas ou padrões e normas de órgãos certificadores;

b) Nem todas mantém controle de acesso por meios de autenticação (senhas e *logins*);

c) Todas afirmaram que utilizam *software* específico de proteção e segurança tanto nas estações quanto nos servidores, e possuem

equipamentos programados para atuar em períodos pré-determinados de periodicidade para a varredura;

d) Todas as empresas afirmaram possuir rotinas de *backups*, embora nem sempre o local de armazenamento dos dados esteja no Brasil;

e) Algumas operadoras brasileiras mantêm contratos que normatizam os procedimentos de completamento de chamadas internacionais em território brasileiro e em território estrangeiro (interconexão e *roaming*); esses acordos são cobertos por cláusulas específicas de segurança e confidencialidade, não incluindo qualquer aspecto de cooperação por parte das prestadoras brasileiras no que diz respeito à coleta de informações de chamadas ou de usuários brasileiros.

f) Praticamente todas as empresas informaram que não existiram ocorrências ou suspeitas de violação dos sistemas ou redes de telecomunicações nos últimos três anos que colocassem em risco dados críticos. Nas tentativas de invasão detectadas, todas foram devidamente bloqueadas pelos sistemas de segurança implantados e tratavam de dados institucionais ou servidores utilizados para testes.

g) Quanto às ações específicas sobre a suposta espionagem da NSA, as prestadoras responderam, por meio do Sinditelebrasil, que "nenhuma prestadora de serviços de telecomunicações associada provê ou facilita informações que possam quebrar o sigilo de seus usuários, salvo mediante ordem judicial na forma da lei brasileira". Além disso, em função das denúncias, apenas uma prestadora informou ter realizado procedimentos de auditorias extraordinárias, nas quais não foram detectadas qualquer anormalidade ou atividade suspeita.

Por ocasião da apresentação na CPI, a documentação recebida encontrava-se em análise pelos técnicos da Anatel. Também haviam sido

encaminhadas para a Polícia Federal e para a Agência Brasileira de Inteligência, atendendo a solicitações recebidas.

Algumas medidas preventivas e reativas foram citadas, com destaque para o projeto de Segurança de Infraestruturas Críticas de Telecomunicações (SIEC), com foco inicial nos grandes eventos internacionais. Outras medidas citadas foram: a) Desenvolvimento de Regulamentação para Mitigação de Desastres, que inclui o Gerenciamento de Riscos em Redes de Telecomunicações; b) Implantação da Gerência da Porta 25, com impacto na redução de *spams*; c) Regulamentos de Qualidade para redes de banda larga fixa e móveis, com monitoramento da disponibilidade operacional e de parâmetros técnicos por uma entidade externa independente; e d) atuação, em cooperação, com diversos organismos internacionais.

Como conclusão de sua apresentação, destacou a necessidade de investimentos para se mitigar riscos de espionagem no Brasil. Citou números relacionados ao Serviço de Inteligência dos EUA, que possui 107 mil funcionários e um orçamento de US$ 52,6 bilhões. Por fim, indicou cinco dimensões a serem abordadas em relação à segurança cibernética: 1) Medidas legais, relacionadas ao aprimoramento da legislação, tendo em conta as atividades ilícitas cometidas nas redes de TIC em âmbito nacional e internacional; 2) Medidas técnicas e processuais, voltadas para a promoção da segurança e gestão de riscos, incluindo esquemas de certificação, protocolos e normas; 3) Estruturas institucionais, destacando-se proposta de criação de uma agência cibernética, que pudesse abranger vários setores, uma vez que, na visão do expositor, trata-se da segurança do Estado brasileiro; 4) Capacitação, incluindo estratégias e mecanismos de formação de pessoal; e 5) Cooperação internacional.

Encerrada esta primeira parte, os convidados foram questionados pelos parlamentares. A sequência foi iniciada pelo Relator da CPI, Senador Ricardo Ferraço, que indagou ao Sr. José Alberto de Freitas Iegas, da Polícia Federal, nos seguintes termos:

Pergunta 1 (Senador Ricardo Ferraço). O Departamento de Inteligência da Polícia Federal foi surpreendido com as denúncias trazidas a público pelo Sr. Snowden ou existiam evidências de que isso poderia estar acontecendo?

Resposta do Sr. José Alberto de Freitas Iegas: afirmou que foram, sim, surpreendidos. No entanto, esclareceu que espionagem e contraespionagem não é atribuição finalista da Polícia Federal.

Pergunta 2 (Senador Ricardo Ferraço). – A Polícia Federal dispõe de informação e conhecimento de que existam bases da Agência de Segurança Nacional dos Estados Unidos funcionando na Capital, Brasília, ou em outras cidades, como foi denunciado há algum tempo por alguns veículos de comunicação?

Resposta do Sr. José Alberto de Freitas Iegas: asseverou não ser verdadeira a notícia de que há bases americanas instaladas em Brasília, como foi veiculado pela imprensa. Afirmou, ainda, que não existe nenhuma base dos Estados Unidos trabalhando em conjunto com a Polícia Federal, da forma como foi divulgado.

Pergunta 3 (Senador Ricardo Ferraço). Existe algum tipo de parceria entre o Departamento de Polícia Federal e a Agência de Segurança Nacional do governo norte-americano?

Resposta do Sr. José Alberto de Freitas Iegas: informou não haver e nunca ter existido parceria entre a Polícia Federal e a NSA. Há cooperação com a Embaixada dos Estados Unidos, assim como existe com vários outros países, no aspecto de troca de informações, cooperação e capacitação, sempre relacionadas à área criminal e à área de antiterrorismo.

Pergunta 4 (Senador Ricardo Ferraço). Como se dá a interação do Departamento de Polícia Federal e outros órgãos que lidam com crimes e segurança cibernética de nações com as quais o nosso País mantém relações amistosas? Há alguma estrutura semelhante nos países vizinhos?

Resposta do Sr. José Alberto de Freitas Iegas: informou que a Polícia Federal possui um núcleo especializado em crimes cibernéticos. Acrescentou que há em torno de 17 ou 18 adidâncias no exterior – na América do Sul, México, Estados Unidos e Europa – que atuam na troca de informações e na interação com outros países e organismos internacionais, em função de vários acordos e tratados firmados pelo Governo brasileiro, com transparência, jamais com ações voltadas à espionagem ou contraespionagem, mas com foco na apuração de crimes.

Pergunta 5 (Senador Ricardo Ferraço). É possível afirmar que temos um nível significativo de segurança para fazer frente às ameaças cibernéticas? O que seria necessário para melhorar nossa capacidade de proteção?

Resposta do Sr. José Alberto de Freitas Iegas: considerando os altos investimentos realizados pelos Estados Unidos na área de tecnologia da informação, desde a criação da Internet, o convidado opinou pela necessidade do Brasil realizar investimentos constantes, capacitação e aprimoramento permanente na área de tecnologia e segurança. Acredita haver redes relativamente seguras, tendo citado, no âmbito da Polícia Federal, a existência de algumas redes criptografadas, que fazem com o fluxo de informações seja seguro. Mas considera não ser possível afirmar que as redes estejam protegidas, de forma absoluta.

Pergunta 6 (Senador Ricardo Ferraço). No inquérito que V. Sª coordena, foi ouvido o correspondente do *The Guardian*, o Sr. Glenn Greenwald?

Resposta do Sr. José Alberto de Freitas Iegas: afirmou que ele foi ouvido, tendo, inclusive, sido entregue cópia do depoimento à CPI. No entanto, esclareceu que o Sr. Glenn Greenwald apenas apresentou informações genéricas, que não foram contundentes na elucidação dos fatos. Acrescentou que o foco das investigações é descobrir se ocorreu quebra ilegal do sigilo das comunicações, sendo esta a questão criminal a ser apurada.

Pergunta 7 (Senador Ricardo Ferraço). V. Sª considerou que as denúncias ou os detalhamentos das denúncias são superficiais ou mesmo fantasiosas?

Resposta do Sr. José Alberto de Freitas Iegas: sem desqualificar as informações prestadas pelo jornalista, que considera importantes para alertar quanto às vulnerabilidades de nossos sistemas,

esclareceu que, para fins de investigação criminal, que é o foco da Polícia Federal, as informações prestadas não foram contundentes, mas um pouco superficiais.

Pergunta 8 (Senador Ricardo Ferraço). Após considerar que o correspondente do *The Guardian*, de certa forma, é uma fonte secundária de informações, sendo a fonte primária o Sr. Snowden, questionou se a Polícia Federal dispõe de adido militar na Embaixada do Brasil na Rússia e se o inquérito em curso está considerando a hipótese de ouvir o Sr. Snowden.

Resposta do Sr. José Alberto de Freitas Iegas: informou que a Polícia Federal não dispõe de adido militar na Embaixada do Brasil na Rússia, mas que, por meio de cooperação internacional, a Polícia Federal está tentando realizar a oitiva do Sr. Snowden. Acrescentou que esta oitiva é uma das prioridades do inquérito.

Pergunta 9 (Senador Ricardo Ferraço). Que tipo de providência concreta foi realizada pelo Departamento de Polícia Federal para que o Governo brasileiro possa, através de suas estruturas, ouvir o Snowden?

Resposta do Sr. José Alberto de Freitas Iegas: esclareceu que a tentativa de realizar a oitiva do Sr. Snowden está sendo feita por intermédio do Ministério da Justiça e do Ministério das Relações Exteriores, através de acordos e tratados internacionais, utilizando-se de meios diplomáticos.

Pergunta 10 (Senador Ricardo Ferraço). Questionou se a oitiva do Sr. Snowden poderia ser considerada uma diligência definitiva para que o inquérito possa ser concluído, perguntando, também se há data para sua conclusão.

Resposta do Sr. José Alberto de Freitas Iegas: informou que não há data para conclusão do inquérito. Há questões técnicas que precisam ser esclarecidas e diligências que a Anatel tem realizado. Apesar de não considerar que estejam reféns da oitiva do Sr. Snowden, considera que ele certamente tenha conhecimento de detalhes técnicos importantes, que facilitariam as investigações e trariam novos elementos ao inquérito policial.

Pergunta 11 (Senador Ricardo Ferraço). Indagou se, ainda que o inquérito não seja dependente da oitiva do Sr. Snowden, ela se constituiria em um fato determinante para a se apurar as denúncias com maior profundidade.

Resposta do Sr. José Alberto de Freitas Iegas: confirmou que a oitiva do Sr. Snowden é um fato determinante e uma providência importantíssima para o prosseguimento do inquérito.

Pergunta 12 (Senador Ricardo Ferraço). Não há prazo para conclusão do inquérito? O inquérito, quando é constituído, não possui prazo definido?

Resposta do Sr. José Alberto de Freitas Iegas: esclareceu que há um prazo inicial de 30 dias, mas que já houve pedido de prorrogação por mais 30 dias. Acrescentou que, diante da necessidade de realização de novas diligências, a Polícia Federal tem solicitado

prorrogação de prazo ao Ministério Público e à Justiça, que têm concedido. Asseverou, no entanto, que tem a intenção de concluir o inquérito o mais breve possível, mesmo que com ressalvas, se houver impedimento e não possa ser realizada a oitiva do Sr. Snowden.

Comentários do Relator, Senador Ricardo Ferraço. Ao concluir os questionamentos formulados ao Sr. José Alberto de Freitas Iegas, externou sua impressão de que há coincidência de interesses entre o inquérito conduzido pela Polícia Federal e as informações almejadas pela CPI. Reconheceu que as denúncias feitas pelo Sr. Glenn Greenwald são contundentes, importantes; no entanto, avaliou que não trouxeram à Comissão elementos suficientes para responder questões importantes, tais como: houve violação das comunicações da Presidente Dilma? Houve quebra das comunicações da Petrobras? De que maneira foi violado? Como foi violado?

Resposta do Sr. José Alberto de Freitas Iegas: Anuiu plenamente com as ponderações do Relator, acrescentando, por sua vez, que faltam dados e informações que possam confirmar as denúncias, sendo elas superficiais.

A seguir, o Relator formulou perguntas ao **Sr. João Batista de Rezende**, Presidente da Anatel, nos seguintes termos:

Pergunta 13 (Senador Ricardo Ferraço). Em sua primeira pergunta dirigida ao Presidente da Anatel, o Relator tratou do marco civil da Internet. Em suas palavras: "De que maneira o novo marco civil poderá contribuir objetivamente para a construção de redes que possibilitem maior

segurança para o nosso País? Na avaliação de V. Sª e da Anatel, isso é uma questão de legislação ou de investimento em torno de estruturas que possam dar ao nosso País a condição de melhorar a sua capacidade de proteção e de reação, considerando a vida real como ela é, considerando que vamos continuar convivendo com esse tipo de violação? Como o novo marco civil poderá contribuir objetivamente para inibir a espionagem ou a violação?"

Resposta do Sr. João Batista de Rezende: afirmou que, em sua visão, o sistema de proteção de dados e informações estratégicas do Estado concretiza-se muito mais do ponto de vista operacional do que em função do marco civil. No entanto, considera que as relações entre pessoas no Brasil e as empresas transnacionais, especificamente Google e Facebook, podem ser melhor regulamentadas, com aprimoramento do entendimento de responsabilidades e deveres desses grupos em nosso país.

Pergunta 14 (Senador Ricardo Ferraço). O Relator perguntou se os questionamentos que foram conduzidos pela Anatel às nossas companhias Telecom até o momento seriam satisfatórios. Contextualizou sua pergunta, comentando ter sido dito à CPI, pelo Sr. Glenn Greenwald, que uma das possibilidades de informações terem sido violadas ou vazadas seria como decorrência da existência de parcerias ou alianças entre empresas de telecomunicações no Brasil e companhias de outros países, sobretudo norte-americanas. Indagou se há algum indicativo neste sentido.

Resposta do Sr. João Batista de Rezende: informou que, até o momento, não há nenhum tipo de indício que leve a concluir que há colaboração ou envio de informações para organismos de espionagem.

Acrescentou que, em sua opinião, não haverá em documento algum, formal, a declaração de que alguém estaria colaborando com espionagens. Lembrou que os documentos coletados foram enviados para a Polícia Federal, que poderá aprofundar nas apurações. Novamente interpelado pelo Relator sobre o assunto, reiterou a resposta dada.

Pergunta 15 (Senador Ricardo Ferraço). Dirigindo-se aos dois convidados, concluiu seus questionamentos, solicitando que externassem suas avaliações sobre o estado da arte e o atual nível de desenvolvimento da segurança cibernética em nosso País, com informações sobre o que está sendo realizado e o que deveria ser feito, tendo em conta as ações no mesmo sentido de outros países, que, como o Brasil, buscam protagonismo internacional.

Resposta do Sr. João Batista de Rezende: opinou ser necessário investir mais em rede de tecnologia e em *softwares*. Além disso, acredita ser importante a criação de um organismo que coordene as várias entidades que trabalham com segurança cibernética: o Ministério da Defesa, o Gabinete de Segurança Institucional da Presidência, o Ministério de Ciência e Tecnologia, bem como as agências que atuam na área. Citou o exemplo dos Estados Unidos, onde ocorreu, após o atentado terrorista de 11 de setembro, a criação de uma agência para coordenar as demais agências, atuando em diversas frentes, tais como as áreas diplomática e operacional. Indagado pelo Relator se essa integração no Estado brasileiro hoje não existe, respondeu que, em sua opinião, a reflexão sobre estas questões estão, agora, iniciando.

Resposta do Sr. José Alberto de Freitas Iegas: corroborou a afirmação do Presidente da Anatel no que tange à necessidade de grandes

investimentos em tecnologia, incluindo satélites próprios, e investimentos constantes em capacitação. Vislumbra a criação de uma agência que possa coordenar outras organizações, nos moldes da ANS americana, como uma possibilidade para assessorar diretamente a Presidência da República.

Concluídos os questionamentos por parte do Relator, Senador Ricardo Ferraço, a Srª. Presidente, Senadora Vanessa Grazziotin, formulou suas perguntas, nos seguintes termos:

Pergunta 16 (Senadora Vanessa Grazziotin). Dirigindo-se ao Presidente da Anatel, perguntou, em relação aos questionamentos encaminhados às empresas, se todas responderam.

Resposta do Sr. João Batista de Rezende: informou que enviaram os questionamentos para as maiores empresas, que são aquelas com contratos e conexões de *roaming*. Comentou que há várias prestadoras de serviços muito pequenas, e julgaram que não seria interessante incluí-las. Em relação às empresas para as quais os questionamentos foram enviados, informou que todas responderam.

Pergunta 17 (Senadora Vanessa Grazziotin). Dirigindo-se ao Sr. João Batista de Rezende, questionou como se dá a fiscalização da Anatel nas empresas que trabalham com Internet, instaladas no Brasil, e se há fiscalização como a que ocorre com as empresas de telecomunicações.

Resposta do Sr. João Batista de Rezende: informou que, em relação à Internet, o trabalho de fiscalização refere-se a requisitos de qualidade, que é o serviço de comunicação multimídia. Não há fiscalização de conteúdo. Por fim, esclareceu que a fiscalização das empresas que

trabalham com Internet é diferente da que ocorre com as empresas de telecomunicações.

Pergunta 18 (Senadora Vanessa Grazziotin). O processo de homologação dos equipamentos de telecomunicações regulamentado pela Anatel poderia ser aperfeiçoado para contemplar a verificação e detecção das vulnerabilidades propositadamente inseridas pelo fabricante?

Resposta do Sr. João Batista de Rezende: informou que seriam necessários investimentos em tecnologia e que a Anatel se instrumentalizasse com esta finalidade, para ser possível detectar fragilidades nos *softwares*.

Pergunta 19 (Senadora Vanessa Grazziotin). Questionou se na regulamentação da Anatel está previsto que as empresas destaquem ou registrem as possíveis vulnerabilidades em seus equipamentos.

Resposta do Sr. João Batista de Rezende: em atenção à presente pergunta, e complementando a resposta anterior, esclareceu que, nas homologações, a Anatel busca verificar questões de vulnerabilidade. No entanto, como a espionagem é um processo ilegal, considera evidente que não se possa detectar facilmente vulnerabilidades propositadamente inseridas pelos fabricantes. No que tange à regulamentação, informou que não há previsão de que a própria empresa explicite eventuais vulnerabilidades de seus equipamentos, pelo fato de se partir do suposto que os *softwares* não podem trazer prejuízos à prestação dos serviços.

Pergunta 20 (Senadora Vanessa Grazziotin). Há possibilidade de a Anatel adotar um sistema de auditagem regular quanto à segurança das operadoras de comunicação?

Resposta do Sr. João Batista de Rezende: afirmou que acompanham a segurança das redes implantadas no Brasil, destacando que atuam buscando a melhor qualidade na prestação de serviços para o usuário, mas não com o objetivo de impedir processos de espionagem.

Pergunta 21 (Senadora Vanessa Grazziotin). Considerando a lei americana chamada "Ato Patriótico", que exige autorização judicial para que empresas ofereçam dados de cidadãos americanos, mas não estabelece tal requisito para estrangeiros, questiona se haveria outra forma, tecnológica ou não, de detectar o repasse de informações por parte de empresas instaladas no Brasil, seja de Internet ou de telecomunicações, para a NSA.

Resposta do Sr. João Batista de Rezende: informou que, nos procedimentos formais, não. Somente como atividade de contraespionagem, que não é objeto da Agência.

Pergunta 22 (Senadora Vanessa Grazziotin). Destacando ser este um ponto essencial, questionou ao Presidente da Anatel quais as iniciativas de contraespionagem adotadas pelo Brasil, seja pela própria Agência, seja por outro órgão.

Resposta do Sr. João Batista de Rezende: esclareceu que a Agência Nacional de Telecomunicações regula o setor. Não realiza nenhuma atividade de espionagem, nem de contraespionagem. Em relação

a eventuais atividades de proteção, busca atuação em cooperação com a Abin e a Polícia Federal.

Pergunta 23 (Senadora Vanessa Grazziotin). Partindo da indagação se é comum embaixadas pedirem instalação de antenas, a Presidente da CPI solicitou informações sobre a embaixada americana.

Resposta do Sr. João Batista de Rezende: informou ser comum que embaixadas realizem pedidos relacionados à instalação de antenas. No que tange à embaixada americana, disse que ela tem uma outorga de serviço limitado privado, com 821 estações espalhadas no Brasil. Há unidades fixas e outras móveis. Funcionam regularmente. A Anatel possui a localização e demais dados registrados. Quanto à fiscalização, informou que se dá sob o aspecto técnico, não em relação à utilização, ao conteúdo das comunicações.

Comentário da Senadora Vanessa Grazziotin: considerando as respostas, a Presidente da CPI solicitou ao Presidente da Anatel o envio dos dados referentes às instalações de antenas da embaixada americana.

Pergunta 24 (Senadora Vanessa Grazziotin). Dirigindo-se ao Sr. José Alberto de Freitas Iegas, indagou como se dá a interação entre o Departamento da Polícia Federal e outros órgãos que lidam com crimes de segurança cibernética.

Resposta do Sr. José Alberto de Freitas Iegas: informou que, em relação aos organismos nacionais, essa troca de informações é permanente. Dependendo da necessidade, há reuniões periódicas pelo Sistema Brasileiro de Inteligência, presidido pela Abin. Quando há necessidade de informação ou diligência formal fora do país para instrução

de investigações, isso ocorre por meio de cooperação com organismos internacionais de vários países que têm representação diplomática no Brasil.

Pergunta 25 (Senadora Vanessa Grazziotin). Indagou se há algum mecanismo tecnológico que seja capaz de detectar quando uma informação está sendo interceptada ou quando dados estão sendo repassados.

Resposta do Sr. José Alberto de Freitas Iegas: informou que obter esse tipo de informação é muito difícil, pois se ocorre espionagem, isso se dá de maneira clandestina.

Comentário da Senadora Vanessa Grazziotin. Considerando matéria do dia, que trata da coleta e armazenamento de listas de *e-mails* pessoais pela agência NSA, dos Estados Unidos, ponderou que, segundo o noticiário, tais ações dependem de acordos com empresas de telecomunicações instaladas ao redor do mundo e que, segundo a matéria, seriam acordos secretos.

Pergunta 26 (Senadora Vanessa Grazziotin). Indagou ao Sr. José Alberto de Freitas Iegas qual é a criptografia utilizada pela Polícia Federal e quem a desenvolveu.

Resposta do Sr. José Alberto de Freitas Iegas: afirmou desconhecer estas informações, comprometendo-se a levantá-las e repassar posteriormente para a Senadora.

Pergunta 27 (Senadora Vanessa Grazziotin). Indagou se há acordo de cooperação entre a Polícia Federal e o FBI.

Resposta do Sr. José Alberto de Freitas Iegas: afirmou não haver acordo com o FBI, mas com a embaixada americana, principalmente na área de capacitação. Indagado, asseverou que não há colaboração da Polícia Federal com eventual atuação de servidores americanos em território nacional. Comentou que, se o fazem, isso ocorre de maneira clandestina.

Pergunta 28 (Senadora Vanessa Grazziotin). O Departamento de Polícia Federal se ressente de eventual falta de coordenação de áreas de inteligência dos diferentes órgãos da administração pública federal exatamente nesse campo da contrainteligência que nós estamos abordando?

Resposta do Sr. José Alberto de Freitas Iegas: esclareceu que há um fluxo de informações e uma integração muito grande, principalmente com a Abin e com os demais órgãos de inteligência das Forças Armadas. Em sua visão, não há falta de troca de informações: pelo contrário, as trocas de informações ocorrem de modo muito adequado.

Pergunta 29 (Senadora Vanessa Grazziotin). Dirigindo-se aos dois convidados, indagou qual o percentual de tecnologia nacional nos equipamentos de segurança cibernética e inteligência de sinais utilizados hoje pela Polícia Federal, e quais informações a este respeito a Anatel possui.

Resposta do Sr. José Alberto de Freitas Iegas: Informou desconhecer o valor percentual, mas informou que, dentre as tecnologias utilizadas pela Polícia Federal, várias são nacionais.

Resposta do Sr. João Batista de Rezende: Afirmou que, no setor de telecomunicações, a maior parte dos equipamentos é estrangeiro, embora existam algumas empresas nacionais. Citou, em relação aos roteadores de Internet, que há apenas quatro ou cinco empresas no mundo que os produzem. Indagado, estimou, de forma geral, em oitenta por cento a predominância de tecnologia não nacional.

Pergunta 30 (Senadora Vanessa Grazziotin). Considerando que, no passado, o Brasil tinha uma presença forte no setor de telecomunicações, mas que, com as privatizações, a situação alterou-se radicalmente, indagou se este quadro torna nosso país mais vulnerável.

Resposta do Sr. João Batista de Rezende: esclareceu que a arquitetura da internet é que propicia as vulnerabilidades, não o fato das empresas serem de capital nacional ou estrangeiro.

Pergunta 31 (Senador Eduardo Suplicy). Após tecer considerações sobre a segurança dos novos sistemas de comunicações em presídios, notícias de ameaça de morte feita ao Governador Geraldo Alckmin e notícias de possíveis ameaças à Copa de 2014, aos jogos e às eleições, indagou se a área de inteligência da Polícia Federal está hoje cooperando com os órgãos de segurança pública do Estado de São Paulo, do Rio de Janeiro e outros.

Resposta do Sr. José Alberto de Freitas Iegas: assegurou que há cooperação entre a área de inteligência da Polícia Federal e as polícias estaduais. Explicou que, como a atividade de inteligência é uma atividade não ostensiva, muitas vezes o resultado de seu trabalho surge como uma prisão ou uma apreensão, realizada normalmente pela polícia

estadual, sendo que o trabalho de inteligência não é divulgado – e, em sua opinião, realmente não deve ser.

Durante a fase das perguntas, o Relator, **Senador Ricardo Ferraço**, deu notícia de confirmação de audiência, na Embaixada da Rússia, para que representantes da CPI, em conjunto com o embaixador, avaliem a possibilidade de teleconferência com o Sr. Snowden. Em relação à notícia, a Senadora Vanessa Grazziotin sugeriu que a oitiva do Sr. Snowden, via teleconferência, fosse feita em conjunto com a Polícia Federal, uma vez que os objetivos da CPI e do inquérito em andamento são os mesmos; e também com a Comissão de Relações Exteriores da Câmara dos Deputados, que possui pedido neste sentido.

Como palavras finais, o **Sr. João Batista de Rezende** frisou que, com o objetivo de aumentar a proteção dos dados estratégicos do Estado brasileiro, é preciso investir em tecnologia. Por outro lado, lembrou que, como atualmente todo o tráfico mundial passa pelas redes e os dados circulam pelo mundo inteiro, um sistema de espionagem eficiente, que não deixe vestígios, não requer a participação de qualquer empresa local. Em relação às investigações em andamento, a Anatel está avançando nas questões técnicas, juntamente com a Polícia Federal. Caso haja nova informação relevante, encaminhará à CPI.

Por sua vez, o Sr. **José Alberto de Freitas Iegas**, em suas palavras finais, ponderou que a principal dificuldade em se apurar se houve um ataque ou uma retirada de informações é exatamente o acesso aos provedores, o acesso aos sistemas centrais das empresas que, em regra, estão nos Estados Unidos. Em sua opinião, se os peritos da Polícia Federal

tivessem acesso às centrais dessas empresas, talvez fosse possível constatar a violação aos sistemas.

Encerrada a fase de perguntas, feitas as colocações finais dos expositores, após agradecer aos convidados, a Presidente da CPI da Espionagem, Senadora Vanessa Grazziotin, encerrou a audiência pública.

9ª Reunião, realizada no dia 22/10/2013 (segurança cibernética)

Objeto: Audiência Pública com os representantes da Cloud Security Alliance Brasil (CSA Brasil), do Comitê Gestor da Internet (CGI) e da Universidade Federal de Pernambuco (UFPE), para discutir o tema segurança cibernética.

No dia 22 de outubro de 2013, a CPI da Espionagem, com base na aprovação do Requerimento nº 19/2013, de autoria do Senador Ricardo Ferraço e conforme entendimento firmado pelos membros da Comissão, promoveu uma audiência pública para ouvir os Srs. Paulo Sérgio Pagliusi, Presidente da Cloud Security Alliance Brasil (CSA Brasil); Rafael Henrique Rodrigues Moreira, Conselheiro do Comitê Gestor da Internet (CGI); e Rodrigo Elia Assad, Professor da Universidade Federal de Pernambuco (UFPE). O objetivo desta audiência pública, conforme expôs a presidente da reunião Senadora Vanessa Grazziotin, foi debater formas de limitar a transferência de dados do Brasil para outros países e a possibilidade de sujeitar empresas estrangeiras à lei brasileira quanto ao acesso de dados de organizações e cidadãos brasileiros.

Sr. Paulo Sérgio Pagliusi

O depoente destacou pontos sobre os atos de espionagem norte-americanos a partir de uma análise técnica de cerca de seis horas de entrevistas concedidas pelo jornalista Edward Snowden. Na sequência, listou ações que considera úteis no combate ao problema.

Os recentes episódios da espionagem americana sobre Brasil e França ganharam projeção internacional e evidenciaram a existência de uma guerra por informação. Esse cenário impõe uma reflexão sobre as estratégicas dos países, pois vai além da discussão técnica de como se faz ou como se protege da espionagem.

Nesse contexto, um dos fatos que ganhou destaque foi a revelação que alguns equipamentos de computação montados nos Estados Unidos já sairiam de fábrica com dispositivos de espionagem instalados. Contudo, estratégias como essa não são inéditas. Em 1992, por exemplo, o sequestro de um representante comercial da empresa de segurança da informação suíça Crypto-AG pelo serviço de contra-inteligência militar iraniano trouxe à tona evidências de que a tecnologia de criptografia vendida pela empresa transmitia, clandestinamente, as chaves criptográficas utilizadas junto com as mensagens cifradas. Na época, dezenas de países faziam uso desse recurso, inclusive as Forças Armadas e o Ministério das Relações Exteriores brasileiros. O fato incentivou a Marinha brasileira a desenvolver seus próprios recursos de criptografia.

Outra revelação que chamou atenção é a de que as ações de espionagem alcançam algoritmos criptográficos que, até bem pouco tempo, eram considerados efetivamente seguros, em particular os protocolos TLS e o SSL. Hoje, já há programas de computador dedicados a quebrar esses tipos de protocolo. Isso leva à reflexão de que a decisão de criptografar deve ser analisada com cuidado. Como, de regra, só se codificam informações consideradas sensíveis, a criptografia acaba servindo como um chamariz a agentes mal intencionados. Uma das formas de reagir a isso é cifrar todos os dados (relevantes ou não), de forma a dificultar o trabalho

dos que tentam quebrar esses códigos. Mas é preciso utilizar chaves mais "fortes" na proteção das informações relevantes.

Prosseguindo sua análise, disse que ainda não se sabe o exato alcance do poderio da Agência de Segurança Nacional (*National Security Agency* – NSA) americana. Sabe-se apenas que eles estão à frente nas pesquisas sobre criptografia e que lidam com supercomputadores pelo menos dez anos mais avançados do que as tecnologias hoje conhecidas. As instalações da NSA na cidade de Utah contam com um *data center* avaliado em US$ 2 bilhões. Ele é capaz de armazenar um iotabyte, medida que comporta toda a informação produzida pelo ser humano nos últimos 500 anos.

Mas o cenário de espionagem mundial não é protagonizado somente pela NSA. O monitoramento da rede é uma das ações dos *Five Eyes*, termo que designa o agrupamento das agências de inteligência de Austrália, Canadá, Estados Unidos, Reino Unido e Nova Zelândia. Essas agências são ligadas por um tratado que autoriza o compartilhamento, entre elas, de informações secretas. O acordo original foi firmado em 1946 entre Estados Unidos e Grã-Bretanha, no contexto da Segunda Guerra Mundial. Os primeiros países monitorados foram os da extinta União Soviética. Os outros três países foram agregados ao acordo por uma razão técnica: ampliar o nível de vigilância sobre os demais países. Dada a dispersão geográfica dos cinco países, juntos eles conseguem monitorar todos os satélites estacionários no globo terrestre.

Os *Five Eyes* são capazes de monitorar, por exemplo, chamadas telefônicas, de fax, transmissões de internet (fixa ou móvel) e de rádio em todo o mundo. Lidam, também, com inteligência de comunicações, que permite saber quem se comunica com quem, quando e

como. Fazem, ainda, análise de tráfego (muito utilizada na área militar) que permite observar um volume de fluxo de informações não usual partindo de determinado órgão. A receptação de dados compreende inclusive os cabos submarinos, pois essas Agências dispõem de uma tecnologia que permite a interceptação desses cabos mesmo em alto mar (*interceptation of vessels*). É um fato que surpreende, pois se pensava que isso não mais seria possível com os cabos atuais, feitos de fibra ótica.

Encerrando sua contribuição, o depoente apresentou algumas ações que considera importantes no combate aos atos de espionagem contra o Brasil. São elas:

a) A aprovação do projeto de lei do Marco Civil da Internet, que irá regulamentar o uso da rede sob os aspectos jurídico e civil, bem como os direitos e responsabilidades dos usuários;

b) O desenvolvimento de um sistema de correio eletrônico brasileiro para uso da Administração Pública e, futuramente, da população. A ferramenta pode assegurar a privacidade das comunicações e, acima disso, a liberdade de expressão, essencial para a vida em democracia. O Brasil conta com gente capacitada a desenvolver esse projeto.

c) A criação de um sistema nacional de criptografia de *e-mails*, desejo expresso pela Presidenta Dilma é que já está sendo desenvolvido pelo Serviço Federal de Processamento de Dados (Serpro). Conforme dito pelo presidente do Serviço, o objetivo é livrar o Governo da espionagem estrangeira. As chaves de criptografia devem ser utilizadas para cifrar não somente informação governamental e de empresas, mas também as comunicações pessoais, por meio das quais informações importantes podem ser interceptadas clandestinamente.

d) O investimento em satélites e cabos submarinos de comunicação próprios, conforme aponta a Estratégia Nacional de Defesa. Hoje, 90% do tráfego de informações que sai do Brasil passa pelo território norte-americano, ainda que se destine a outras localidades.

e) A constituição de um comando cibernético único para tratar de questões de segurança da informação. Conforme justificou, as divisões das Forças Armadas têm estratégias, táticas e doutrinas próprias para os domínios terrestre, marítimo e aéreo. De forma similar, a Agência Espacial Brasileira cuida da área de domínio espacial. Mas falta ao Brasil um órgão com expertise em domínio cibernético, que envolve técnicas e conhecimentos próprios. Uma batalha cibernética, diferente das terrestres ou marítimas, ocorre em questão de horas.

f) A aproximação do trabalho dos órgãos governamentais com as pesquisas desenvolvidas nas universidades, o que pode reforçar a capacidade do País em proteger o tráfego de informações.

g) A inclusão da discussão sobre segurança cibernética nos currículos escolares. O surgimento de bons analistas de segurança depende da formação crítica sobre o assunto. O surgimento de mais especialistas nesta área ajudará o ambiente corporativo a aprimorar suas ferramentas de segurança cibernética.

h) O investimento em canais para o recebimento de denúncias de espionagem, aproveitando o reconhecimento do Brasil como um país aberto à permanência dos denunciantes. O próprio jornalista Glenn Greenwald declarou que, no território britânico, não sentiria a mesma liberdade de fazer as revelações que fez no Brasil. Isso pode ser visto de maneira positiva por potenciais denunciantes, que observam atentamente o que acontecerá com Snowden.

Sr. Rafael Henrique Rodrigues Moreira

Inicialmente, o depoente apresentou o Comitê Gestor da Internet (CGI). Criado por decreto presidencial em 2003 e coordenado pelo Ministério da Ciência, Tecnologia e Inovação (MCT), esse Comitê é composto por 21 membros advindos do governo, do terceiro setor, da iniciativa privada e da comunidade acadêmica e científica, constituindo uma visão pluralista que é elogiada em todo o mundo.

Na sequência, apresentou informações sobre o contexto em que se desenvolvem as discussões sobre segurança cibernética.

As novas tecnologias tornaram o uso de recursos de informática e comunicação mais baratos e acessíveis. E o Brasil se beneficia disso. Enquanto a economia brasileira cresce a uma média de 0,9 a 1% ao ano, esse setor, tomado isoladamente, cresce a uma média de 15 a 18% ao ano. Evidência disso é que o Brasil é, hoje, o terceiro maior mercado mundial de tecnologia da informação e de comunicação.

Mundialmente, cria-se, a cada dois anos, a mesma quantidade de dados desenvolvida do início da civilização até 2003. A cada minuto são trocados 168 milhões de e-mails, postados 1500 páginas de blogs e criados 60 novos blogs.

Contudo, à medida que a sociedade se torna mais conectada, cresce a necessidade de discutir e implementar ações nas áreas de segurança da informação, proteção de dados pessoais, direitos civis na internet, propriedade intelectual e direitos autorais.

A segurança de um ambiente digital depende do controle da rede de comunicações e do tráfego de informações. Esse controle, contudo,

passou a ser relativo com o advento da computação em nuvem, que hospeda informações em *data centers* espalhados pelo mundo.

Além disso, a topologia da rede mundial de computadores foi constituída para concentrar o tráfego de dados nos Estados Unidos. Isso se apresenta como uma dificuldade a mais para o tratamento seguro das informações que trafegam pela internet.

Vários exemplos mostram como o alto grau de conectividade pode causar prejuízos sociais e traduzem a responsabilidade governamental em salvaguardar informações estratégicas e as relativas aos cidadãos.

Primeiro, é possível que um *cracker* interrompa uma rede elétrica, pois hoje os relés não são mecânicos, e sim digitais, conectados em rede. O setor energético é, inclusive, um daqueles considerados estratégicos para a espionagem.

Segundo, o Datasus é um banco de dados que reúne informações sobre a saúde de milhões de usuários do Sistema Único de Saúde e que tem muito valor para determinados ramos do mercado.

E, terceiro – tratado em outro momento da exposição –, o Brasil chegou a ser o maior distribuidor de *spams* da América Latina. Dos principais *malwares*, os mais disponibilizados eram do tipo *worms*, que copiam senhas para serem utilizadas em crimes cibernéticos. Atualmente, com o gerenciamento da Porta 25, por onde a maioria dessas ameaças trafegava, esse fato está mudando.

Diante das ameaças a que estão expostos, os cidadãos estão interessados em saber como o governo irá manipular e armazenar dados e informações sensíveis, de forma que eles fiquem protegidos do acesso indevido por lobistas ou agentes de governos estrangeiros. Essa é a importância de definir um marco regulatório que reafirme o investimento

em pesquisa, desenvolvimento e inovação na área de segurança da informação.

Falando especificamente dos atos de espionagem, o depoente esclareceu que os Estados Unidos não são o único país que faz espionagem eletrônica. Porém, dado seu desenvolvimento tecnológico, é ele quem define os padrões e tecnologias que serão utilizados na espionagem. Nesse sentido, o grande volume de informações que hoje circulam pela rede fez com que se desenvolvessem sofisticadas ferramentas de manipulação e análise de dados. Uma vez de posse dos dados – o que ocorre quando eles trafegam em rede ou são armazenados nos *data centers* de empresas americanas – a NSA utiliza essas ferramentas para interpretar e classificar as informações de acordo com seu grau de relevância estratégica. No caso do dado criptografado, esse é levado a servidores que, utilizando-se de computação de alto desempenho, tentam quebrar as chaves que os codificaram.

A mobilidade também favorece a espionagem. O rastreamento de celulares permite, *a priori*, acesso à teia de relações de quem usa o dispositivo. Contudo, caso o dispositivo não conte com criptografia ou caso essa tenha seu chaveamento "quebrado", é possível ter acesso também ao próprio conteúdo das ligações. Já o protocolo 3G dos dispositivos móveis é aberto e facilita o rastreamento de telefones tanto para fins lícitos (como a resolução de crimes), como para fins ilícitos (como espionagem industrial, tecnológica ou de estratégias governamentais).

Adicione a isso o fato de que, por lei, o governo norte-americano pode ter acesso aos dados dos serviços de e-mail e de hospedagem sediados em seu território. Na interpretação brasileira, expressa na abertura da Assembleia-Geral das Nações Unidas, esse poder

deveria dirigir-se somente ao cidadão americano e não poderia ser aplicado a cidadãos estrangeiros.

Por fim, lembrou que o mercado de crimes cibernéticos, conhecido como *darknet*, movimenta muito dinheiro. Há, inclusive, listas de preços para o repasse de informações adquiridas ilegalmente.

Apresentado esse cenário, o expositor defendeu que o Brasil encontra-se diante de uma oportunidade favorável ao investimento, nas universidades, em atividades de pesquisa, desenvolvimento e inovação na área de segurança cibernética, bem como na criação de um complexo industrial voltado especificamente para as "tecnologias de fronteira".

Uma das perspectivas para isso é um programa de defesa e segurança cibernética que está sendo desenvolvido pelos ministérios da Ciência, Tecnologia e Inovação e da Defesa.

A título de exemplo, o Pentágono americano investe em empresas localizadas no Vale do Silício para que eles criem novas tecnologias que serão utilizadas, futuramente, pelo governo americano.

O Brasil não dispõe, ainda, de produtos de criptografia prontos. É isso que levou a Petrobrás a declarar que não havia empresas brasileiras aptas a oferecer soluções de criptografia para a petroleira. Por outro lado, um estudo de mercado revelou a existência de 87 empresas nacionais na área de segurança da informação e criptografia. Com estímulo governamental, essas empresas teriam condições de desenvolver soluções nas áreas de segurança e defesa cibernética.

Paralelamente à questão da criptografia, o País poderá desenvolver um modelo de certificação e homologação de equipamentos de informática, pois não pode continuar a adquirir de multinacionais tecnologias que não sabe ao certo como foram desenvolvidas.

Passando à etapa final de sua exposição, defendeu a aprovação do projeto de lei do Marco Civil da Internet como forma de garantir a proteção de dados pessoais de brasileiros quando colocados em rede, ainda que o armazenamento ocorra no exterior. A União Europeia conta, desde 1995, com uma lei desse tipo. Sobre o projeto do Marco, em tramitação na Câmara dos Deputados, destacou alguns pontos que considera sensíveis:

a) Permanência da neutralidade de rede, fundamental para equilibrar interesses e manter a isonomia entre os detentores da infraestrutura e os geradores ou provedores de aplicações;

b) Armazenamento obrigatório de determinados tipos de dados no País. Na Coreia do Sul, por exemplo, dados financeiros devem obrigatoriamente ser armazenados em *data centers* localizados no país;

c) Regras sobre a guarda de registros de atividades na rede (*logs*), importantes para investigações policiais e forenses;

d) Confinamento de tráfego, que é um assunto delicado e que merece ser mais discutido. Por ele, criam-se regras para que o tráfego de informações entre dois dispositivos que se utilizam de IP brasileiro ocorra via redes brasileiras.

e) Direitos autorais na rede, assunto que, ao seu ver, pode ser tratado com mais propriedade no projeto da reforma da Lei de Direitos Autorais.

Sr. Rodrigo Elia Assad

O depoente – que integra um grupo de trabalho colaborativo focado em criar soluções para empresas de tecnologia de informação, o Assert Lab – apresentou questões relevantes sobre a espionagem americana.

Preliminarmente, lembrou que as grandes empresas americanas oferecem muito dinheiro para a contratação de gente qualificada de outros países, perpetuando seu poder sobre as mais recentes inovações tecnológicas. Assim, o Brasil deve buscar estratégias para preservar as 87 empresas nacionais que lidam com segurança da informação e criptografia.

O primeiro ponto apresentado é que, se antes não se prestava tanta atenção aos dados gerados por governo, empresas e usuários, hoje, diante do crescimento exponencial do volume de dados produzidos anualmente, muito se discute sobre a responsabilidade corporativa sobre essas informações.

Nessa seara, as perguntas que devem ser respondidas são:

a) Que dados são gerenciados?

b) Quais deles são considerados relevantes?

c) Como esses dados são manipulados?

d) Onde eles estão salvos?

Ocorre que, atualmente, a quantidade de dados produzidos é significativamente maior do que a capacidade de armazenamento das organizações em geral. Assim, a oferta de estocagem gratuita de dados tornou-se um negócio extremamente atrativo. Mas isso acaba criando um problema que precede até mesmo a questão da privacidade: de quem acaba sendo a propriedade desses dados?

A segunda questão levantada é que, hoje, computação significa conexão. Os novos aplicativos são desenvolvidos para operarem em conexão, trocando informações. Isso torna desafiante a tarefa de conseguir rastrear, do início ao fim, a circulação das informações.

Afora isso, é preciso definir uma estratégia para identificar precisamente o que se deseja monitorar. Essa tarefa demanda tempo, investimento e pesquisa. No caso americano, a necessidade de defesa fomentou a desenvolvimento tecnológico. O Vale do Silício, por exemplo, foi criado no final da Primeira Guerra Mundial. Da mesma forma, a Intel iniciou suas atividades fabricando radares.

Prosseguindo sua exposição, o Sr. Rodrigo apresentou alguns pontos de reflexão que o episódio da espionagem ao Brasil deixa:

a) A convergência dos pontos de conexão para o território norte-americano partiu de uma decisão estratégica. O Brasil precisa decidir como lidará com a gestão de seus pontos de tráfego de dados. É possível, por exemplo, fazer o monitoramento na base de onde os dados saem ou na extremidade dos pontos de tráfego. Basta criar um centro de processamento de dados no ponto onde se quer analisar as informações. Mas lembrou serem essas mudanças onerosas e difíceis.

b) Existe, hoje, um mercado das vulnerabilidades, por meio do qual governos e empresas compram de *hackers* informações sobre falhas de programação de outras empresas ou instituições não com o intuito de corrigi-las, mas para manter essas informações em segredo e utilizá-las estrategicamente. Conforme os analistas de *malwares*, o setor energético está em evidência nesse mercado.

c) A mobilidade é outro problema a ser enfrentado. A partir da captura do sinal, por antenas, é possível localizar fisicamente um telefone celular. Ocorre que a captura do sinal tem sido feita até mesmo por embaixadas, sob a justificativa de que o sinal é distribuído abertamente por via aérea e, portanto, a interceptação deles não significa violação.

Apresentados contexto e principais problemas a serem enfrentados, o depoente finalizou sua exposição sugerindo a adoção, pelo Brasil, das seguintes providências:

a) Aprovação do Marco Civil da Internet;

b) Utilização de uma plataforma de computação em nuvem nacional, tecnologia já disponível;

c) Desenvolvimento de um comando para monitoramento e rastreamento de informações no Brasil, incluindo um sistema de classificação e armazenamento seguro de informações relevantes;

d) Definição de uma estratégia para o uso de criptografia e de algoritmos nas atividades de Estado. O Brasil deve desenvolver seu próprio sistema para cifrar informações, eliminando o risco de utilizar tecnologias que repassam chaves de segurança a terceiros.

Encerrada a primeira parte da Audiência Pública, a Senadora Vanessa Grazziotin questionou os convidados sobre pontos específicos.

Pergunta 1 (Senadora Vanessa Grazziotin). Solicitou-se a análise da vulnerabilidade dos sistemas de segurança cibernética que o Brasil utiliza, numa escala comparativa, a países com nível de desenvolvimento compatível com o brasileiro.

Resposta do Sr. Paulo Sério Pagliusi: Explicou que só agora o Brasil acordou para esse tipo de problema. O próprio Parlamento Europeu já havia levantado essa questão com relação ao serviço de inteligência norte-americano. Dizia-se que espionagem corporativa era uma teoria da conspiração, mas hoje se sabe que é uma realidade e que seu início remonta à Guerra Fria. Com o fim dela, porém, o esforço de

espionagem foi direcionado para as áreas econômica e industrial. O Brasil precisa levar mais a sério esse assunto. Numa escala de 0 a 10, sendo que 0 representa vulnerabilidade total, o País ganharia nota entre 3 e 4. Para avançar nesta escala, é preciso ter consciência da situação e aprender a combatê-la. Acredita que a sociedade está consciente do problema, pois as pessoas passaram a perceber que, mais do que usuários de redes sociais, fazem parte de um contexto mercadológico. Isso fica evidente nos termos de acordo de quem aceita fazer parte de uma rede social como o Facebook: esses termos dizem que o serviço é o dono da informação e pode excluí-la a qualquer momento.

Sr. Rafael Henrique Rodrigues Moreira: O Brasil é especialmente vulnerável em razão do tamanho de sua economia, maior do que a de países do mesmo nível de desenvolvimento. Há muito o que avançar nesse assunto. Há apenas um ano, o Brasil era o principal distribuidor de *spams* do mundo. Isso porque, para o envio dessas mensagens, os *crackers* utilizavam-se da porta 25, que estava sob gestão das operadoras de telecomunicações. A partir de um trabalho conjunto do CGI, Anatel e dessas operadoras, foi possível melhorar o gerenciamento dessa porta e diminuir o número de *spams* que saem do Brasil. É tempo de que o Brasil pense estrategicamente não só no controle de suas comunicações, como também nas saídas dessa rede. Os órgãos, a exemplo do Exército, precisam estar capacitados para trabalhar suas próprias redes, efetivando o projeto de infovia, sob responsabilidade do Ministério do Planejamento, Orçamento e Gestão (MPOG).

Sr. Rodrigo Elia Assad: No Brasil, há setores que investem em segurança da informação. Os bancos são um exemplo. É preciso olhar

para os segmentos mais estratégicos e promover um trabalho mais efetivo sobre eles.

Pergunta 2 (Senadora Vanessa Grazziotin). Quanto à auditoria e homologação de equipamentos, questionou-se em quanto é aumentada a vulnerabilidade a ataques virtuais devido à falta desses serviços e se haveria, no país, alguma entidade que cuidasse de tais serviços em áreas mais sensíveis, como defesa nacional.

Resposta do Sr. Paulo Sério Pagliusi: O Brasil conta com instituições dedicadas a homologação, a exemplo da Isaca (*Information Systems Audit and Control Association*), instituição com mais de 40 anos, e da *Cloud Security Alliance Brazil*, entidade que o expositor preside. São instituições sem fins lucrativos que cuidam da segurança informacional e da governança da tecnologia da informação. A Isaca, em particular, confere uma certificação chamada Cisa (*Certified Information Systems Auditor*), que é homologada e fomentada pelo próprio Gabinete de Segurança Institucional da Presidência da República. O Departamento de Segurança da Informação e Comunicações da Presidência da República recomenda que todo servidor público que trabalha com segurança da informação detenha esse tipo de certificação.

Sr. Rafael Henrique Rodrigues Moreira: Falando sobre como garantir que o Governo tenha acesso a equipamentos e programas realmente seguros, deu o exemplo dos Estados Unidos e da Austrália. Esses países instituíram um sistema de requisitos de segurança que deve ser seguido por empresas que tem interesse em vender equipamentos ou softwares para o Governo. Da mesma forma, o Governo brasileiro pode estabelecer regras de certificação e homologação para a aquisição de

equipamentos e programas que serão utilizados em áreas estratégicas. Uma proposta nesse sentido já é desenvolvida pelo Ministério da Ciência, Tecnologia e Inovação (MCTI). Por fim, disse que uma rede mais segura e com controle governamental depende de um conjunto de padrões, técnicas e analistas que experiência.

Sr. Rodrigo Elia Assad: Complementou as respostas anteriores dizendo que o Centro Tecnológico do Exército (CTEx), em parceria com o MCTI desenvolve um selo de nacional certificação.

Pergunta 3 (Senadora Vanessa Grazziotin). O Google ofereceu cobertura de internet banda larga a áreas do Brasil que ainda não dispõem dessa facilidade. O serviço será oferecido por meio de balões que emitem o sinal de internet. Assim, perguntou qual seria o risco incorrido pelo Brasil ao autorizar a oferta do provedor.

Sr. Rafael Henrique Rodrigues Moreira: Para que o governo tenha mais controle, é preciso homologar e certificar os equipamentos que serão utilizados pelo Google, opinião com a qual o Sr. Rodrigo Elia Assad concordou.

Pergunta 4 (Senadora Vanessa Grazziotin). Questionou-se qual seria o efetivo grau de controle da rede de que o Brasil dispõe, especialmente para a proteção das áreas governamentais mais sensíveis, e de que forma as antenas instaladas em embaixadas sediadas no Brasil poderiam ser utilizadas para a captura irregular de dados de internet e de telecomunicações.

Resposta do Sr. Paulo Sério Pagliusi: O Brasil ainda não goza de um patamar elevado quanto ao controle de rede. Porém, os

acontecimentos recentes levaram o País a ser mais consciente do problema. A partir de um trabalho de treinamento promovido em Brasília, disse ter constatado que os gestores públicos têm pouco conhecimento sobre segurança cibernética. Ressaltou a importância de promover campanhas de conscientização para criar uma cultura com relação a isso.

Sr. Rodrigo Elia Assad: O controle de redes, além de uma questão de segurança cibernética, é uma estratégia de defesa. O único país que desenvolveu uma estratégia efetiva de defesa cibernética foi a China, que não depende da conexão externa para manter suas redes em funcionamento. O Brasil precisa desenvolver a capacidade de lidar com grandes repositórios de dados (*big datas*), para acessar, com facilidade, informações importantes. Deve-se investir, também, no aspecto educacional para que as pessoas aprendam a ser seletivas sobre o conteúdo que disseminam nas redes.

Pergunta 5 (Senadora Vanessa Grazziotin). Indagou-se sobre a possibilidade de detectar quais são as informações que estão sendo acessadas de forma ilegal.

Sr. Rodrigo Elia Assad: A princípio, todos os dados salvos em grandes provedores internacionais podem ser acessados, porque passam a pertencer a esses serviços. Foi o que motivou o governo francês a não autorizar a venda de um sítio nacional de vídeos para uma empresa americana, considerando o quanto as informações contidas ali – vídeos, fotos, contatos e informações pessoais voluntariamente publicados – são estratégicas. Com relação ao controle de tráfego, disse que há técnicas desenvolvidas que permitem predizer se uma determinada rede está sendo interceptada. Os americanos, por exemplo, conseguiram detectar que uma

marca chinesa estava inserindo *backdoors* nos equipamentos que produziam. Reforçou que o Brasil precisa criar uma indústria nacional que abrigue empresas de classe mundial nas áreas que o País tem interesse em desenvolver, dizendo que o País tem competência para desenvolver suas próprias ferramentas de análise e defesa.

Resposta do Sr. Paulo Sério Pagliusi: Todo crime cibernético deixa evidências, pois acaba gerando registros de atividades. Por meio desse princípio, é possível ter um monitoramento contínuo do ambiente de rede. As corporações, de forma geral, precisam agir proativamente ao utilizar preventivamente técnicas e métodos já desenvolvidos para o monitoramento contínuo da informação e a análise do fluxo de dados na rede. Isso lhes permitirá ter ampla consciência situacional das ameaças cibernéticas a que estão expostas e de como se defender delas. Declarou, ainda, que o grupo colaborativo que integra desenvolveu o primeiro sistema de gerenciamento de segurança da informação nacional, trabalho que já foi apresentado ao CGI.

11ª Reunião, realizada no dia 5/11/2013 (telefonia móvel: TIM, Claro, Vivo e Oi)

Objeto: Audiência Pública com os representantes das Empresas de Telefonia Móvel: TIM, Claro, Vivo e Oi.

No dia 5 de novembro de 2013, a CPI da Espionagem,[78] mediante Requerimento nº 20/2013, de autoria do Senador Ricardo Ferraço, ouviu os Srs. Nelson de Sá, Diretor da TIM; Ivan Campagnolli, Diretor da Claro S.A.; S.A.; Ari Sergio Perri Falarini, Diretor de Operações da Telefônica Vivo; e Marcos Augusto Mesquita Coelho, Diretor de Relações Institucionais da Oi.

O objetivo da audiência pública, conforme anotado no Requerimento, foi discutir e prestar esclarecimentos sobre as denúncias feitas pelo jornalista Glenn Greenwald. O conteúdo das informações ofertadas por Glenn sugere que empresas de telecomunicações, com atuação no Brasil, mantém acordo de envio de dados de comunicações de cidadãos brasileiros para companhia estrangeira sediada nos EUA, a qual, por sua vez, repassa essas informações à Agência de Segurança Nacional americana (NSA).

A Senadora Vanessa Grazziotin, antes de passar a palavra aos convidados, comunicou a resposta dada pela Anatel a requerimento

---

[78] Criada conforme o Requerimento nº 811, de julho de 2013-SF, de autoria da Senadora Vanessa Grazziotin (PCdoB/AM) e outros Senadores, para, no prazo de cento e oitenta dias, investigar "a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal",

formulado pela CPI. O requerimento buscava saber quais embaixadas possuem estações de comunicação a rádio no Brasil e em qual número. A Agência respondeu que quatro embaixadas possuem estações de rádio no País e as quantidades de cada uma são: o Chile possui duas estações portáteis; a França, cinco; a Romênia, vinte; e os EUA, 841 estações de comunicação, dentre fixas e móveis, operando em todo o território nacional. A Presidente da CPI, sem fazer qualquer julgamento prévio, chamou a atenção para o grande número de estações sob poder dos EUA.

Feito o comunicado, os trabalhos expositivos foram abertos pelo Sr. Nelson de Sá, Diretor da TIM. Para ele, esta é uma boa oportunidade para a companhia mostrar os trabalhos que vem sendo desenvolvidos em seu interior, no que diz respeito à segurança de dados de usuários.

Baseada na transparência, a empresa TIM respeita as determinações constitucionais e legais quanto à inviolabilidade de dados. Conforme o palestrante, à Constituição Federal (art. 5, XII) e à Lei de Interceptação (Lei n. 9.296/1995) não cabem interpretações, isto é, devem ser seguidas à risca. Em outras palavras, espionagem é crime, é interceptação não autorizada.

Explicando o papel desempenhado pelas empresas de Telecom, afirmou que elas são provedores de acesso à internet, cuja responsabilidade está na construção das vias de tráfego de dados e de voz na rede. Num outro plano, estão os provedores de aplicação, que são as empresas ofertantes de serviços que utilizam de tais vias construídas pelos provedores de acesso.

Asseverou que a empresa não mantém qualquer tipo de parceria com órgãos estrangeiros para a realização de escuta telefônica e

acesso a dados privados de seus clientes. A TIM preserva e resguarda integralmente as informações e o sigilo de seus usuários, respeitando os casos em que a legislação especifica as circunstâncias de quebra de sigilo.

Prova disso é o armazenamento de todas as informações dos usuários em *datacenters* localizados no Brasil, sobre os quais recaem rígidos controles de segurança. Estando entre os maiores da América Latina, esses *datacenters* corroboram a atitude da companhia em expandir os meios de segurança e proteção de dados. Disse que ampliação dos investimentos no setor foi da ordem de oitenta por cento.

No que diz respeito aos sistemas de operação de suporte, informou que eles possuem acesso restrito, protegido e rastreáveis. Na mesma linha, os sistemas de gestão de dados pessoais, assim como a interceptação legal, são passíveis de auditoria e fiscalização pela Anatel.

Sendo uma companhia de vanguarda tecnológica, a TIM dispõe de um Centro de Segurança Operacional – Security Operation Center – (SOC), situado em São Paulo, que é referência tecnológica para o mercado. Paralelamente, visando ao combate e ao tratamento de incidentes de internet, existe um time próprio de funcionários que garante a segurança, o *Computer Security Incident Response Team* (CSIRT). E há, também, um segundo grupo que faz testes de invasão, que realiza, preventivamente, busca por fragilidades do sistema.

Em síntese, explicou que os dados são protegidos do mundo externo por três plataformas. A primeira é a plataforma de infraestrutura de segurança, a qual controla os acessos à rede, efetuando a proteção primária do complexo. A segunda é a de monitoração, que identifica e rastreia os acessos indevidos à rede. A última é a plataforma evolutiva, que

correlaciona os eventos e analisa os *logs* para contactar incidentes. Se houver algum incidente, este vai para a apuração técnica do CSIRT.

Portanto, a TIM detém os melhores produtos para detecção e combate a ataques, trabalha e investe para ter segurança operacional e submete-se, fielmente, às leis que regulam o tema.

Em seguida, o Sr. Ivan Campagnolli falou em nome da operadora Claro. Disse que a empresa atua no ramo da telefonia móvel, utilizando-se da estrutura de *backbone* (traduzido do inglês, significa "espinha dorsal") da Embratel.

Enfatizou que não há dúvida de como é regulado o assunto de proteção e segurança de dados: há uma legislação clara e aplicável. Mesmo assim, é importante compreender os atores envolvidos e suas características.

Dessa forma, trouxe alguns dados sobre a companhia telefônica que representa. A Claro tem cobertura nacional, ligando todo o território brasileiro por meio de fibra ótica. Há, em alguns lugares – como é o caso da linha que parte de Manaus – interconexão com fibras óticas de outras empresas, a exemplo da que se estabelece com a Oi na cidade amazonense citada. Além da conexão em território brasileiro, existem cabos que vão para a Europa e para os EUA.

Atualmente, a empresa possui um cabo em consórcio com a Embratel, denominado "América 2", e outro cuja propriedade é integralmente sua, o AMX-1, ainda em construção, que está previsto para entregar no primeiro trimestre de 2014. Para suportar a demanda, a Claro tem capacidade comprada em cabos de outras operadoras, com as quais são estabelecidas regras de confidencialidade de dados e de voz.

Diante das necessidades, cada vez mais crescentes, de se garantir a segurança dos dados de clientes, a companhia desenvolveu, e mantém em conjunto com a Embratel, estrutura de segurança que abrange: o controle físico (quem acessa, com qual perfil e o que está autorizado a fazer); a responsabilidade por quem executará as cópias de segurança; quais atualizações de hardware e software devem ser feitas; a proteção contra ataques; a resposta a incidentes de segurança; e a utilização de antivírus. Essas medidas visam garantir que todos os dados sejam invioláveis.

A respeito dos satélites que prestam serviços para a empresa, a cargo da Star One,[79] disse que tanto o controle de sua posição como de seu caminho orbital são feitos no Brasil. Dessa maneira, há absoluta segurança do sigilo de dados.

Ademais, as interconexões necessárias são feitas com operadoras legalmente constituídas, mediante contratos balizados pelo sigilo e pela confidencialidade esperada pelos usuários e pela sociedade em geral.

Confirmando as ideias apresentadas pelos expositores que o antecederam, o Sr. Ari Falarini, representante da Vivo, reiterou o campo sólido em que são celebrados os contratos de conexão e interconexão das empresas. Seja nacionalmente, seja em âmbito internacional, esses acordos fixam-se na responsabilidade do sigilo e da confidencialidade da informação trespassada entre usuários.

---

[79] Empresa da Embratel responsável pela operação e pelo controle das estações de comunicação, abrangendo todo o território nacional e América do Sul nas bandas C, X, Ku e Ka.

À semelhança das concorrentes congêneres, a Vivo, que está presente em 25 países e presta serviços a mais de 300 milhões de clientes, possui capacidade de gerenciamento e segurança de rede de abrangência nacional. Há três centros de operação para a rede móvel, localizados em São Paulo, Brasília e Belo Horizonte. Essa estrutura é responsável por monitorar e acompanhar 76 milhões de telefones móveis (que totaliza mais de dezenove bilhões de minutos falados e seis bilhões de SMS enviados por mês), quatorze mil sites e 29 mil estações móveis.

A Vivo opera a telefonia fixa apenas no Estado de São Paulo, alcançando 42 milhões de habitantes, 1.800 centros de telefonia, onze milhões de terminais telefônicos e quase 4 milhões de acessos a banda larga. Para este ramo de serviço, existem dois centros de gerência e um *datacenter* específico na grande São Paulo.

Para garantir o desenvolvimento da rede, que já conta com 78.480 quilômetros de fibra ótica e 235 mil quilômetros de fios de cobre, a empresa tem investindo maciçamente na área, a partir de previsões quadrienais. No quadriênio 2007-2010, o investimento foi de dezesseis bilhões de reais, enquanto no lapso de 2011-2014, foi de 24 bilhões.

Disse, ainda, que está sendo construído um backbone para uso próprio e outro que pode ser comutado com as demais operadoras. Isso ajudará no aumento da capacidade nacional e internacional. Esta, aliás, é coberta pelo *backbone* nacional, o qual permite fazer o direcionamento e a distribuição do tráfego, de acordo com as necessidades de cada operação.

Informou que, dentre os trinta gigabytes destinados à Europa e aos EUA, 229 deles vão para território americano. Dessa forma, é natural que haja acordos com operadoras europeias e americanas, a fim de dar

conta da execução de tamanha quantidade de serviços. Mas isso não é feito sem a observância dos critérios de segurança já expendidos anteriormente.

Por fim, informou à CPI a respeito da inauguração do *datacenter* da empresa, situado em Tamboré, região metropolitana de São Paulo, que já obteve certificação em três aspectos: quanto ao padrão do projeto; quanto à rigidez de padrões de disponibilidade de segurança; e quanto aos requisitos ecológicos.

Fechando as apresentações iniciais dos convidados, o representante da Oi, Sr. Marcos Mesquita, disse que a empresa é a pioneira na prestação de serviços convergentes no País (serviços de transmissão de voz, local e de longa distância, telefonia móvel, acesso à banda larga e TV por assinatura).

Nessa esteira, a dimensão de seus negócios denota a importância da companhia para o País. Fundada em 1998, a Oi já contabiliza investimentos na escala de 102 bilhões de reais. Está presente em 5.565 Municípios, isto é, faz-se atuante em todo o território nacional; provê 74,3 milhões de acesso aos mais variados serviços; e cria 160 mil empregos diretos. Em resposta a essas iniciativas, 120 bilhões de reais em tributos foram recolhidos pelos cofres públicos, desde sua fundação.

A empresa conta com mais de 178 mil quilômetros de fibra ótica, albergando todo o território nacional, e oferecendo, a mais de 4.800 municípios, serviços de telefonia móvel. Ao lado disso, a Oi detém e disponibiliza a maior rede pública de Wi-Fi no País.

Sobre o tema específico tratado pela CPI nesta audiência, o Sr. Marques salientou, inicialmente, que há uma preocupação crescente com a segurança de dados. Isso se mostra evidente por três razões: 1) aumento das ameaças produzidas virtualmente, seja por dados, seja por voz; 2)

incremento no interesse por fraudes e espionagens; e 3) ampliação das expectativas dos clientes quanto à segurança.

Essas três razões evidenciam que é preciso estar constantemente atento para aspectos de vulnerabilidade, que sempre existirão e sempre terão de ser monitorados – leia-se: é necessário que haja trabalho frequente de prevenção e defesa. Nessa linha de raciocínio, é fundamental que as leis acompanhem as mudanças tecnológicas.

Fez, na sequência, uma breve síntese do conteúdo das denúncias em relação à espionagem conduzida pela agência americana NSA. Elas denotam que: a) as redes de Telecom são vulneráveis; b) os contratos de interconexão possibilitam o acesso a dados e comunicações, com origem no Brasil, por governos ou instituições de segurança estrangeiras; c) há "colaboracionismo" de empresas de Telecom brasileiras com representantes de países estrangeiros.

Para o representante da Oi, essas denúncias são infundadas e não há como comprová-las. Isso por que: a) a rede de transporte de dados da Oi processa pacotes IP[80] e é completamente transparente às camadas superiores, onde estão contidas as informações; b) a rede de transporte de dados da Oi é um meio que encaminha as solicitações de uma determinada origem para um determinado destino, sem que elas sejam armazenadas; c) os equipamentos usados pela rede de transporte de dados possuem rígido sistema de controle e de acesso; d) a Oi não armazena informações de correspondências entre os endereços de IP e seus respectivos usuários.

Assim, a responsabilidade de responder ou não uma determinada requisição de um usuário de origem e/ou criptografar os dados

---

[80] IP, do inglês, *Internet Protocol*, é a identificação de um dispositivo, por exemplo, de um computador.

enviados é dos próprios usuários. A rede, portanto, é um meio de transporte de dados e de voz, conforme o caso. E, por isso, a proteção à inviolabilidade das comunicações dos clientes é o maior ativo da empresa.

No que diz respeito aos contratos de interconexão, asseverou que a companhia tem contratos com quase todas as importantes empresas do mundo. A propósito desse tema, disse que a Anatel, a pedido desta CPI, está finalizando trabalho de auditagem desses contratos, o qual detalhará a estrutura e as cláusulas que os regem, a fim de averiguar sua adequação aos parâmetros internacionais.

Sublinhou que a Oi presta seus serviços com base numa política de segurança de dados, conforme a qual, todo acesso não autorizado é bloqueado, identificado e rastreável. Mas isso é suficiente para nos tranquilizar? Disse que não, mas qualquer tentativa de espionagem será identificada, mesmo que *a posteriori*.

Destacou, também, que, quando começaram os debates acerca da espionagem americana, arguíu-se existir vazio legislativo sobre o tema aqui no Brasil. No entanto, o palestrante demonstrou, numa breve pesquisa, que o assunto é bem delineado pela legislação nacional: o Código Civil prevê que a invasão de privacidade configura ato ilícito, ensejando sua reparação mediante o ressarcimento material; o Código Penal, com a alteração promovida pela Lei 12.737/2012 – Lei dos Crimes Informáticos (Lei Carolina Dieckmann) –, tipificou as condutas criminosas promovidas nessa seara, prevendo, inclusive agravante quando o delito for cometido contra autoridade pública; e, ainda, a Lei de Interceptação Telefônica (Lei 9.296/1996), já citada, também trata do tema em seu art. 10 ("Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de

informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei").

Além desses diplomas legais, a espionagem com interesses econômicos é punida com legislação protetiva da propriedade intelectual, ao passo que a espionagem com interesses políticos e contra a segurança nacional é tratada pela Lei de Segurança Nacional (Lei 7.170/1983).

Se existem leis e há uma imensa gama de ferramentas tecnológicas direcionadas para a segurança, onde está a fragilidade do sistema?

O Sr. Marcos Mesquita respondeu que a maior fragilidade para a segurança de qualquer sistema está na atitude das pessoas que neles atuam. Portanto, é necessário valorizar uma cultura de segurança. Os sistemas não resolverão tudo por nós. Basta lembrar que a NSA, a grande espiã do mundo, foi espionada da forma mais antiga que existe, por um funcionário de terceiro escalão de uma empresa terceirizada: Edward Snowden.

Finalizada a primeira parte, foi passada a palavra ao Relator da CPI para que este iniciasse questionamento aos palestrantes, ao que foi seguido pelos Senadores Eduardo Suplicy, Vanessa Grazziotin e Pedro Taques.

Pergunta 1 (Senador Ricardo Ferraço). Considerando que, em audiência anterior, o Sr. Greenwald disse que as empresas de telecomunicações são parceiras-chave no processo de espionagem, perguntou se as empresas representadas na reunião possuem algum acordo de entrega de dados ou relatórios a algum governo.

Resposta do Sr. Marcos Augusto Coelho: O Sr. Marcos Augusto Coelho negou a existência de qualquer tipo de acordo de repasse de dados.

Resposta do Sr. Ivan Campagnolli: Negou a existência de qualquer tipo de acordo de transferência de dados com entidades nacionais ou internacionais. A única hipótese de repasse de dados é sob determinação judicial.

Resposta do Sr. Ari Sérgio Falarini: Disse não haver nenhum tipo de acordo de entrega de dados para governos ou entidades externas.

Pergunta 2 (Senador Ricardo Ferraço). Questionou como é feito o repasse de dados de usuários, quando solicitado por mecanismo legal.

Resposta do Sr. Marcos Augusto Coelho: O convidado explicou que, nos casos de interceptação legal, não há nenhuma participação da companhia na escuta da operação. A autoridade policial faz a escuta e, terminada a investigação, o *link* é cortado, sem que haja qualquer envolvimento da empresa com o conteúdo das comunicações.

Pergunta 3 (Senador Ricardo Ferraço). Indagou onde e como poderia haver interceptação de dados nas redes das companhias, bem como se seria possível ocorrer interceptação sem que nenhum funcionário tenha conhecimento. Se sim, quando a operação poderia ser percebida e quais seriam as providências tomadas.

Resposta do Sr. Marcos Augusto Coelho: O Sr. Marcos Augusto Coelho disse que toda experiência de vazamento de dados de

clientes acabou gerando uma melhora na capacidade de evitar esse tipo de falha. Destacou que o ponto fraco geralmente é o ser humano, a pessoa que comete o crime. Citou um caso em que um funcionário, apesar de ter passado por um processo seletivo rigoroso, recebeu um apelo externo para repassar dados dos clientes. No entanto, o procedimento foi rastreado em seu equipamento e ele acabou sendo preso. Assim, ressaltou que o fundamental é que o sistema se previna contra esse tipo de interferência. Caso isso não seja possível, que o ponto de fragilidade seja rastreável. Segundo ele, imediatamente após a identificação do ponto frágil, é feito um trabalho de revisão de procedimentos e aumento da capacidade de segurança.

Resposta do Sr. Ivan Campagnolli: Inicialmente, enfatizou que o crime de interceptação acompanha a evolução tecnológica, muda com o tempo e de maneira individualizada, buscando falhas no sistema, na manutenção no momento específico do crime. Quando identificado, o procedimento normal é a abertura de um boletim de ocorrência para apurar se alguém, de posse de informações confidenciais, agiu de maneira criminosa. Reforçou que a empresa possui todo um procedimento e cuidado com a rede para evitar que isso ocorra, pela responsabilidade que tem na proteção de seus ativos. Ademais, defendeu que todo acordo de conexão com uma operadora legalmente estabelecida seja redigido por um contrato que contenha cláusulas que garantam a preservação da integridade dos dados.

Resposta do Sr. Nelson de Sá: O Sr. Nelson de Sá reforçou que o elo de fragilidade no sistema é a pessoa que comete o crime. Segundo informou, a TIM realiza auditorias praticamente de hora em hora para verificar tudo o que foi solicitado legalmente. É feita a varredura de todas

as centrais e, se houver alguma programação que não esteja atrelada a um ofício, o processo é desfeito e é aberta uma investigação. Se houvesse um vazamento de dados – o que nunca ocorreu na empresa – o fato seria comunicado oficialmente aos órgãos competentes.

Resposta do Sr. Ari Sérgio Falarini: Lembrou que qualquer frequência liberada para uso no Brasil passa por um controle feito pela Anatel, que também a fiscaliza. Ademais, qualquer intervenção na rede é rapidamente sinalizada pelos sistemas de alarme das operadoras. As ações necessárias são tomadas de imediato, até mesmo para não haver nenhuma perda de tráfego. No caso da fibra ótica, disse ser praticamente impossível utilizar um aparato que, em um curto espaço de tempo, consiga mapear volume de informações transmitidas.

Pergunta 4 (Senador Eduardo Suplicy). Perguntou se as empresas possuem algum mecanismo para garantir a privacidade dos usuários de seus sistemas, tanto nas comunicações por telefone quanto por internet.

Resposta do Sr. Ivan Campagnolli: Disse que existe uma série de mecanismos, proteções codificadas de senha, quem tem acesso, com que perfil e para qual atividade. O processo é auditado e os mecanismos protegem a rede contra ataques externos ininterruptamente. Afirmou com convicção que a rede da empresa é segura.

Resposta do Sr. Nelson de Sá: Explicou que os mecanismos para garantir a comunicação privada são implementados pelo próprio protocolo GSM, mas que, atualmente, já existem mecanismos que utilizam aparelhos de criptografia. No caso da internet, salientou que se trata de uma rede aberta, passível de diversos mecanismos de quebra de sigilo. Assim,

muitas vezes, por desconhecimento, ao aceitar um contrato de adesão referente ao uso de um programa, a pessoa abre mão de sua liberdade.

Resposta do Sr. Ari Sérgio Falarini: Ratificou a importância de o usuário ficar atento no momento de aceitar os termos e condições de uso de um aplicativo ou ferramenta adquirido, para ter a consciência do uso que pode ser feito daquilo.

Pergunta 5 (Senador Ricardo Ferraço). Questionou quais são os aspectos enfocados nas auditorias realizadas periodicamente pela Agência Nacional de Telecomunicações (Anatel), se os aspectos segurança de rede e sigilo das informações são considerados.

Resposta do Sr. Marcos Augusto Coelho: O representante da Oi disse não saber os pontos de checagem da Anatel nas auditorias, pois não atende a fiscalização. Contudo, disse acreditar que a Anatel tenha programas de auditagem que cubram todos os aspectos da operação de telecomunicações. Acrescentou que, por ser cotada em bolsas internacionais, a Oi é obrigada a obedecer a padrões internacionais em boa parte de seus processos. Por isso, é auditada por entidades externas constantemente, para garantir que sejam mantidos certos padrões de gerenciamento, tanto em aspectos operacionais quanto financeiros e de segurança.

Resposta do Sr. Ivan Campagnolli: Informou que a Anatel considera diversos fatores nas auditorias. Disse não se lembrar de nenhuma auditoria específica de segurança, mas que nem todos os casos passam pelo Comitê Executivo. Em sua opinião, após os eventos recentes, a agência certamente tratará de forma mais específica do tema.

Resposta do Sr. Nelson de Sá: Explicou que as fiscalizações da Anatel possuem variados modelos e formas, além de ocorrerem periodicamente. Segundo relatou, recentemente foram questionados e testados os padrões de controle da empresa. Destacou que a TIM também é uma empresa cotada nas bolsas internacionais, passando, portanto, constantemente por auditorias de *Sarbanes-Oxley*, que incluem a verificação dos níveis de controle de segurança.

Resposta do Sr. Ari Sérgio Falarini: Informou que são realizadas regularmente auditorias da Anatel, tanto para SLAs técnicos operacionais quanto para verificação dos dispositivos de segurança na rede. No procedimento, são informados os funcionários que tiveram acesso à rede, o horário em que a acessaram, bem como o tipo de atuação realizada. Há ainda a auditoria interna, que verifica se as programações estão corretas. Caso não estejam, o problema é rapidamente identificado e corrigido.

Pergunta 6 (Senadora Vanessa Grazziotin). Considerando que o Sr. Nelson de Sá declarou que a TIM possui um *data center* instalado no Brasil e que todos os *data centers* de internet estão localizados nos Estados Unidos, perguntou que tipo de informações as empresas armazenam em seus centros. Além disso, solicitou que os palestrantes opinassem se a obrigatoriedade de as empresas de internet manterem *data centers* no Brasil aumentaria a segurança dos brasileiros.

Resposta do Sr. Marcos Augusto Coelho: Ponderou que, se tratasse do tema de forma superficial, responderia que a Oi é favorável à manutenção de *data centers* de internet no Brasil, que essa medida aumentaria a clientela da empresa. Contudo, lembrou que esse debate, incluído na discussão do marco civil da internet, deriva da ideia de que se o

Brasil possuir dados armazenados em seu território, sob sua jurisdição, poderá requisitá-los para efeito de investigação. No entanto, pontuou que o grande problema nessa questão reside no fato de o usuário, para utilizar um serviço, concordar com termos de uso de uma empresa estrangeira. Assim, acaba aceitando que qualquer demanda sobre aquele serviço deva ser feita em um foro no exterior, abrindo mão da proteção da legislação brasileira, o que dificulta imensamente o procedimento, caso necessário. Dessa forma, sublinhou que o foco da discussão deve ser a jurisdição dos dados, e não a guarda propriamente dita, pois o problema permanecerá se os dados forem guardados em território nacional, mas mantida a jurisdição do país de origem. O local onde os dados são armazenados não afeta em nada a questão da privacidade propriamente dita, já que estarão submetidos às mesmas regras internacionais de qualidade e operacionalidade. Informou ainda que há um projeto de lei na Câmara dos Deputados que trata de forma eficiente sobre o tema.

Resposta do Sr. Ivan Campagnolli: Afirmou que a Claro é favorável à manutenção de *data centers* no Brasil.

Resposta do Sr. Nelson de Sá: Esclareceu que são armazenados nos *data centers* os metadados de uma ligação ou de início de uma comunicação de dados, mas nunca o conteúdo. Quanto à obrigatoriedade de *data centers* de internet no País, ponderou que a medida em si não resolveria o problema, uma vez que muitas empresas manteriam os dados no Brasil, mas não os forneceriam dada a matriz ser estrangeira. Apesar disso, defendeu que haja incentivos e investimentos para que esses dados tenham polos tecnológicos de armazenamento no País, já que com o uso da nuvem será cada vez mais difícil saber a localização dessas informações no mundo.

Resposta do Sr. Ari Sérgio Falarini: Disse que a Vivo defende a existência de *data centers* locais.

Pergunta 7 (Senadora Vanessa Grazziotin). Relembrando que até mesmo a Presidenta Dilma teve suas comunicações interceptadas – inclusive telefônicas – perguntou o que os palestrantes sabem sobre o caso, além do divulgado pela imprensa. Tomando esse caso como exemplo, perguntou o que garante a segurança das comunicações.

Resposta do Sr. Marcos Augusto Coelho: Informou que não sabia que tinha havido interceptação de conteúdo das comunicações da Presidenta. Reafirmou que, mesmo nos casos de interceptação legal, não há nenhuma participação da empresa na escuta da operação.

Resposta do Sr. Ivan Campagnolli: Disse não saber mais detalhes do ocorrido, mas que a preocupação com o assunto existe, tanto que há equipamentos celulares criptografados.

Resposta do Sr. Nelson de Sá: Sobre a segurança das comunicações, afirmou que ela é garantida por protocolos, mas que, infelizmente, não há limites tecnológicos para a prática de crimes.

Pergunta 8 (Senador Ricardo Ferraço). Questionou se, quando as empresas de telecomunicações nacionais fazem alianças com empresas estrangeiras, a legislação permite que estas tenham acesso ou possam ter acesso, caso demandem, às comunicações realizadas.

Resposta do Sr. Marcos Augusto Coelho: O representante da Oi disse que não há nenhum tipo de acordo de repasse de dados. Há apenas questões relacionadas a faturamento, que permitem que o titular de uma rede externa possa cobrar do cliente da Oi quando este utilizar sua rede,

como ocorre em ligações de longa distância. Nesse caso, a empresa precisa saber quem ligou, quando e o tempo da ligação para fazer a tarifação, mas nada relacionado ao conteúdo da comunicação.

Resposta do Sr. Ivan Campagnolli: Ratificou que a aliança com outras empresas é segura, é uma relação comercial estabelecida por um contrato válido, juridicamente perfeito e que preserva, por obrigação, todos os dados dos clientes. Não há entrega de metadados para nenhuma operadora e acredita que os acordos sejam respeitados.

Resposta do Sr. Nelson de Sá: Informou que a TIM mantém alianças apenas comerciais, que não há nenhum acordo de troca de dados.

Resposta do Sr. Ari Sérgio Falarini: Afirmou que a Vivo não inclui nenhuma cláusula que permita a abertura de informações dos clientes em seus contratos comerciais. Os contratos prezam por um padrão de qualidade, de disponibilidade e de preservação do conteúdo da informação do cliente.

Pergunta 9 (Senador Pedro Taques). Solicitou que os palestrantes comentassem sobre os processos, instrumentos e mecanismos necessários para a interceptação das comunicações telefônicas da Presidenta Dilma fora do sistema de rede das empresas. Perguntou se os palestrantes têm conhecimento se é possível fazer no Brasil interceptação sem a participação das companhias, por meio de malas, *notebooks, tablets* e outros apetrechos, dado que a literatura informa que, em alguns países podem-se adquirir esses equipamentos.

Resposta do Sr. Marcos Augusto Coelho: O palestrante sublinhou que a rede não armazena nada, mas que existe a rede doméstica do cliente, que está fora do gerenciamento da Oi. Assim, a empresa não

consegue certificar sua segurança. Salientou que tudo que precisa utilizar a rede da companhia é detectável, identificável e rastreável. Segundo o Sr. Marcos Augusto Coelho, o primeiro ponto de fragilidade na comunicação a ser analisado é a estrutura interna do cliente. A rede é a última coisa a ser olhada.

Resposta do Sr. Nelson de Sá: Confirmou a existência de maletas que capturam a informação, que na última feira de segurança havia um estande expondo essas ferramentas. Em sua opinião, a interceptação da Presidenta Dilma pode ter ocorrido de forma mais próxima do que se imagina, inclusive utilizando essas maletas.

Resposta do Sr. Ari Sérgio Falarini: Afirmou ter a convicção de que a interceptação das comunicações da Presidenta Dilma ocorreu de uma maneira mais próxima do que se imagina.

Pergunta 10 (Senador Pedro Taques). Considerando a hipótese de a agência americana estar acessando o conteúdo das comunicações da Presidenta Dilma dos Estados Unidos, questionou se as redes das companhias nacionais constatariam essa invasão. Ademais, perguntou se existem protocolos internacionais que tratem disso. Por fim, indagou se é possível fazer essa interceptação remotamente, por um método não invasivo na rede, mas por meio de ondas de rádio.

Resposta do Sr. Leandro Henz (gestor de rede da Oi, representando o Sr. Marcos Augusto Coelho): De acordo com o Sr. Leandro Henz, seria inviável, do ponto de vista prático, fazer uma interceptação nos cabos submarinos (que transportam grandes quantidades de dados entre as operadoras) para se obter dados, por serem extremamente pesados, com um alta voltagem e comportarem um tráfego de 500 *gigabits*

por segundo. Portanto, se ocorresse uma interceptação, seria indetectável. No caso da comunicação por celular, por sua vez, há relatos na literatura de que existem equipamentos que, se colocados próximos ao usuário conseguem, com certo tempo, captar esses dados móveis. Outra maneira de fazer uma interceptação seria por meio do próprio aparelho celular. Como os *smartphones* são pequenos computadores, ao aceitar a instalação de um aplicativo, o usuário pode, equivocadamente, autorizar um *spyware* ou um *malware* que vai enviar toda a informação contida no dispositivo para determinado lugar.

Resposta do Sr. Ivan Campagnolli: O Sr. Ivan Campagnolli informou que é muito mais difícil ter o mecanismo para detectar uma interceptação por ondas de rádio. Por outro lado, se realizada por meio da conexão de fio, dependeria de uma informação sigilosa – que, se repassada, configuraria crime – e poderia ser descoberta por um processo normal de recuperação. Segundo ele, até mesmo uma improvável interceptação nos cabos submarinos seria detectada.

Resposta do Sr. Ari Sérgio Falarini: Retomando o que foi dito pelos demais convidados, ratificou que as empresas trabalham para prover segurança ao usuário, mas que existem artifícios comercializados – como as maletas já citadas – que podem ser utilizados de maneira maliciosa. Sobre a vulnerabilidade das redes, reforçou que os cabos submarinos são de difícil manuseio, pois requerem equipamentos e veículos extremamente especializados, sofisticados e custosos para tanto. Lembrou que as intervenções na rede são rapidamente sinalizadas pelos sistemas de alarme das operadoras. No caso da fibra ótica, disse ser praticamente impossível utilizar um aparato que, em um curto espaço de tempo, consiga mapear volume de informações transmitidas.

12ª Reunião, realizada no dia 12/11/2013 (Serpro e Prodasen)

Objeto: Audiência Pública com os representantes do Serviço Federal de Processamento de Dados (Serpro) e da Secretaria Especial de Informática do Senado Federal (Prodasen).

No dia 12 de novembro de 2013, a CPI da Espionagem, com base em entendimento firmado pelos membros da Comissão, promoveu uma audiência pública para ouvir os Srs. Marcos Vinícius Ferreira Mazoni, Diretor-Presidente do Serviço Federal de Processamento de Dados (Serpro) e Victor Guimarães Vieira, Diretor da Secretaria Especial de Informática do Senado Federal (Prodasen). O objetivo desta audiência pública foi conhecer as preocupações desses órgãos – referenciados como algumas das melhores empresas de processamento do País – com relação à segurança da informação e as soluções que eles adotam quanto a isso. A reunião foi presidida pela Senadora Vanessa Grazziotin, estando presente o Senador Eduardo Suplicy. Participou da rodada de questionamentos, também, o Sr. André Luiz Bandeira Molina, coordenador da área de Infraestrutura de Tecnologia da Informação do Prodasen.

Marcos Vinícius Ferreira Mazoni

O Diretor-Presidente do Serpro concentrou-se em apresentar as vulnerabilidades de segurança e privacidade a que as informações governamentais estão expostas e o que entende como soluções a esses problemas.

Inicialmente, esclareceu a relação do Serpro com o tema da segurança da informação. Embora a empresa pública não seja a responsável direta pela segurança cibernética do Governo, lida com sistemas

estratégicos para o funcionamento do País, o que exigiu o desenvolvimento, ao longo do tempo, de soluções com foco na segurança da informação. Entre esses sistemas estratégicos, citou os que permitem gerenciar serviços de importação e exportação, transferências de recursos do Governo Federal para outros entes federativos, arrecadação e despesas do Governo. Uma interrupção nos serviços da empresa implicaria prejuízos ao País e acarretaria uma paralisação do próprio Estado.

Para a apresentação à CPI, o convidado apresentou vulnerabilidades e soluções em seis áreas: rede mundial de computadores; rede de governo; nuvens de governo; centros de dados de governo; aplicações de governo; e correio eletrônico utilizado pelo governo.

Rede mundial de computadores

As principais vulnerabilidades da rede mundial de computadores são:

a) A concentração da governança da internet nos Estados Unidos. O Brasil tem um modelo de gestão de governança da internet que deveria servir como modelo internacional, pois conta com a participação da sociedade, de órgãos governamentais e de entidades privadas;

b) Quanto à rede física da internet, muitos dos cabos e satélites utilizados pelo Brasil não são controlados pelo País, mas por empresas privadas. Noticia-se, atualmente, a existência de submarinos dedicados à coleta de dados diretamente dos cabos que cruzam os mares;

c) Já a rede lógica da internet (incluindo as rotas, os servidores centrais da internet e o sistema de nomes de domínios – DNS) concentra-se principalmente nos Estados Unidos, o que sujeita os dados que transitam por esses grandes centros de roteamento à legislação daquele país;

d) Por fim, liga-se a isso o fato de que grande parte dos dados é armazenada em centrais norte-americanas, o que permite que essas informações sejam acessadas pelo Departamento de Defesa dos Estados Unidos.

As soluções apresentadas a essas vulnerabilidades da rede mundial são, conforme o expositor:

a) Governança mundialmente democratizada da internet, uma das ideias defendidas pela presidenta Dilma na abertura da 68ª Assembleia-Geral das Nações Unidas;

b) Distribuição geográfica e política dos servidores centrais da internet, fazendo com que a tráfego de informações comece a ocorrer também fora dos Estados Unidos;

c) Instalação de um maior número de cabos de conexão de redes no continente sul-americano, o permitiria um controle mais efetivo da rede física;

d) Desenvolvimento de satélites, o que faz parte da política aeroespacial brasileira;

e) Fortalecimento do Comitê Gestor de Internet (CGI), responsável pela governança da internet no Brasil e que é modelo de participação de diferentes atores.

Rede de Governo

O segundo rol de vulnerabilidades e soluções refere-se à rede de Governo. Hoje, toda a infraestrutura física da "infovia" que atende aos órgãos governamentais é operada pelo Serpro. Mas isso não garante proteção total a essa rede, que está exposta às seguintes vulnerabilidades:

a) Predominância de redes de operadoras de telecomunicações, o que representa um problema na medida em que, para reduzir custos, a

troca de tráfego entre operadoras normalmente ocorre fora do Brasil, principalmente em Miami (EUA);

b) Costuma-se trabalhar com dados não criptografados.

c) Fragilidades de segurança contidas nos *softwares*, como *backdoors*. Isso porque esses produtos obedecem à legislação norte-americana, que dá ao Departamento de Segurança dos Estados Unidos o direito de acesso aos dados manipulados por esses programas. Classificou alguns destes como "caixas pretas", pois eles não permitem saber ao certo que informações enviam pela rede.

d) A exposição de roteadores de borda, que traz vulnerabilidade à informação sempre que a parte da rede sobre a qual há controle se liga a outras redes.

e) Por último, apontou que o domínio da infraestrutura (equipamentos de rede) e das aplicações utilizadas (sistemas operacionais e bancos de dados) pertence a empresas privadas, especialmente norte-americanas. Assim, mesmo que o ambiente seja gerido com a máxima segurança, o aparato por trás dele carece de controle.

Sobre as vulnerabilidades apontadas nesta segunda etapa, ofereceu como possíveis soluções:

a) Uso de uma infraestrutura pública de comunicação. Explicou que fibras óticas estão ligando as capitais do País e que a "infovia" de Brasília está em expansão. Isso garantirá que o País tenha um maior controle das informações que saem da rede. Muita ênfase foi dada ao reconhecimento de qualquer tentativa de entrada não autorizada no ambiente controlado pelo Serpro. Mas o movimento inverso também é necessário, pois ainda não se tem um controle efetivo das informações que saem pelas *backdoors* de equipamentos e *softwares*.

b) Liga-se a esse objetivo a meta de ampliar a capacidade governamental de gestão, monitoramento e auditoria de equipamentos. Conforme detalhou, o Instituto Nacional de Tecnologia da Informação (ITI) contrata o Centro de Pesquisa da Universidade de São Paulo (USP) para auditar todos os equipamentos utilizados pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). É o mesmo Instituto que audita os equipamentos utilizados pelo sistema bancário brasileiro. Isso não torna o sistema bancário livre de tentativas de ataque. Contudo, quanto mais protegido o sistema, maior a capacidade de processamento necessária para quebrar suas chaves, o que consome muita energia e torna o processo extremamente oneroso.

c) Outra meta é o investimento em protocolos de segurança da informação que sejam seguros e livres. Ao contrário do que se pensa, os *softwares* livres não são menos seguros. Por terem código aberto, eles podem ser auditados e podem ser alterados para ampliar o nível de segurança, diferentemente de um *software* proprietário.

d) Relacionou também o investimento em *hardware* nacional de rede. O meio universitário brasileiro já detém capacidade de desenvolver roteadores com taxa de transferência (*throughput*) compatível com os internacionais. Já há, também, roteadores comerciais desenvolvidos no Brasil com capacidade próxima aos internacionais. Até 2015, os equipamentos centrais do projeto Infovia Brasil deverão ser de origem nacional. Ainda sobre esse assunto, o expositor explicou que o mundo acadêmico desenvolve um método para subtrair a inteligência de roteamento (camada três) dos equipamentos e construí-la novamente por meio de programação, o que torna o equipamento mais seguro. Em breve, essa tecnologia será aplicada aos equipamentos nacionais.

e) Outra solução apontada é o uso de criptografia, que deve ser associada com o desenvolvimento nacional de *hardware*, deixando os ambientes virtuais mais protegidos contra ataques cibernéticos. Porém, esse conhecimento de criptografia deve ser associado com o desenvolvimento nacional de *hardware*, deixando os ambientes virtuais mais protegidos contra ataques cibernéticos. A criptografia do ICP-Brasil e do Serpro é desenvolvida em parceria com universidades brasileiras. Já o *hardware* é nacional, desenvolvido em conjunto com a Universidade Federal de Santa Cataria (UFSC) e com a Universidade de Campinas (Unicamp) e produzido por uma empresa no Centro de Tecnologia da Unicamp.

f) Finalizando, citou a necessidade de ampliar investimento na indústria nacional de defesa cibernética. À medida que essas empresas avançarem, elas serão capazes de oferecer equipamentos competitivos e desenvolver proteção contra ameaças externas.

Criptografia

Nesse tocante, o expositor explicou que o recurso de criptografia, quando utilizado, destina-se ao chaveamento do caminho das mensagens, mas não do conteúdo delas. Soma-se a isso o fato de que os algoritmos de criptografia e os equipamentos criptográficos são criados ou controlados por países estrangeiros. Além do mais, é preciso cuidado com a construção de chaves criptográficas fracas, a depender dos algoritmos empregados nelas.

A solução a esses problemas passa pelo investimento em projetos de formação e pesquisa em criptografia. O Serpro, por exemplo, desenvolve, em parceria com a USP e a UFSC, um projeto de formação de técnicos nessa área. É preciso que os órgãos governamentais façam amplo uso do recurso de criptografia e das chaves públicas fornecidas pelo ICP-

Brasil. A parceria com outros países aprimora esse processo, já que a cooperação permite que se construa uma rede cada vez mais segura para todos. Por fim, é preciso auditar os equipamentos e programas em uso para a descoberta de falhas e vulnerabilidades.

Nuvem de Governo

Passando a tratar de computação em nuvem para o Governo, o palestrante considerou de extremo risco a contratação de serviços privados nessa área. Segundo ele, embora nove das dez maiores nuvens no mundo sejam feitas a partir de *software* livre, o acesso do contratante ao conjunto de dados alocados é dificultado, o que não resolveria o problema de salvaguardá-los. Há ainda a ressalva de que muitos serviços obedecem às leis americanas, que facilitam o acesso do Governo dos EUA aos dados. Outro problema apontado é a falta integração entre diferentes nuvens, pois de nada adianta haver uma nuvem governamental que não consiga se relacionar com outras.

Explicando possíveis saídas a essas questões, disse que o Serpro desenvolve, desde 2012, um projeto nacional para criar a nuvem de Governo, feita a partir de *software* livre, o que oferecerá à nuvem um nível de segurança que o *software* proprietário não alcançaria. Além disso, a empresa busca construir uma ferramenta de comunicação entre diferentes nuvens, também feita com código aberto. Para isso, conta com equipes especializadas nos seus onze polos de desenvolvimento, trabalhando com diferentes tipos de tecnologias. Ainda utilizando *software* livre, o Serviço desenvolve redes sociais que se conectam com as redes mais comuns, como Facebook e Twitter, mas não alocam dados nelas. A rede Participatório, da Presidência da República, é um exemplo.

Centros de dados de governo

O próximo tópico discutido foi o tratamento dado os centros de dados (*data centers*) governamentais. As principais vulnerabilidades, nesse caso, são:

a) A possibilidade de acesso indevido a dados e aplicações, pois os programas utilizados neles são dependentes de sistemas operacionais fechados;

b) A contratação de centros de dados privados, seja dentro ou fora do Brasil, também implica certo risco, uma vez que esses, buscando renovar de contratos, muitas vezes aprisionam dados como forma de pressionar o governo, como se essas informações fossem propriedades deles.

A isso, o palestrante apresentou como soluções:

a) Ações de gestão e classificação de documentos e dados, o que evita a superproteção de informações que não são sigilosas e, que, devem, inclusive, ser de conhecimento público.

b) Gerenciamento de identidades, que busca tratar as fragilidades internas. Na construção do programa para declaração do imposto de renda anual, por exemplo, são alocados mais de quatrocentos profissionais. Deve haver registro de todas as ações feitas, e de sua autoria. Mas os ambientes externos também devem ser monitorados e geridos, permitindo reconhecer qualquer tentativa de acesso indevido a dados.

c) Uso de protocolos de segurança abertos e livres, evitando programas de código fechado, que podem passar informações aos seus fabricantes.

d) Análise de licenciamento de *softwares*, de forma que eles passem a respeitar a legislação brasileira e eliminem quaisquer formas de *backdoor*.

e) Uso progressivo de *softwares* livres, o que por si só já elimina o problema de *backdoors*. No Serpro, 70% dos programas utilizados são em *software* livre. O programa para declaração do imposto de renda disponibilizado em 2012, por exemplo, é todo desenvolvido em *software* livre, o que atende também à necessidade de portabilidade. Assim, o programa passou a ser aberto em qualquer ambiente operacional, e não somente no da Microsoft.

f) Por fim, auditoria dos equipamentos e programas em uso, o que, no caso do Serpro, é feito em parceria com universidades.

Aplicações de Governo

Prosseguindo a exposição, o Sr. Marcos falou das principais vulnerabilidades das aplicações de governo, que se referem a programas com *backdoors*, sem possibilidade de auditoria (pois não são feitos em código livre) e com licenças sujeitas à legislação estrangeira, especialmente a norte-americana. Citou também, o despreparo dos gestores públicos responsáveis pelas contratações quanto ao tema de segurança. Nesse sentido, muitos juristas apontam que o Brasil pode estipular a obrigação de atendimento à lei nacional nos editais para a compra de produtos ou contratação de serviços. Mas esse recurso, não raro, é ignorado, porque a segurança da informação ainda não é vista como preocupação relevante.

As soluções para isso, apontou o expositor, passam por:

a) Uso de *software* livre, o que o Serpro busca desde 2007. Esses programas permitem alterações sem que se dependa do fabricante, o que aumenta o padrão de segurança;

b) Uso de *softwares* públicos, que são replicáveis. Por meio deles, as boas experiências e soluções podem ser compartilhadas.

c) Análise de licença de *software* nas aquisições governamentais, de forma que os termos dessas licenças obedeçam à legislação brasileira.

d) Promoção de capacitação em normas de segurança.

e) Por último, o aumento do número de profissionais com formação sólida em segurança da informação e a criação de centros de excelência nessa área.

Correio eletrônico

Por último, o expositor fez considerações quanto ao uso de correio eletrônico. O uso de programas sujeitos à legislação estrangeira facilita a interceptação de mensagens e o monitoramento de comunicações por outros países. Segundo narrou, a existência de *backdoors* nos programas Outlook e BlackBerry já foi identificada. Ainda falta conscientização dos usuários sobre o problema. Muitos utilizam emails particulares em serviço, outro problema apontado.

Apresentando soluções e esses problemas, o expositor destacou que o Serpro desenvolve o programa de correio eletrônico Expresso que, por determinação da Presidência, será utilizado por toda a gestão pública Federal. O Expresso é desenvolvido em *software* livre e já tem reconhecimento internacional. Os dados das mensagens trocadas serão todos hospedados nos servidores do Serpro. Preocupada com a gestão segura de arquivos, a nova versão do programa criptografará não só o caminho da mensagem, como todo o conteúdo dela. Além de oferecer o Expresso, o Serpro, em parceria com universidades, analisa a segurança de outros programas de correio eletrônico.

Sr. Victor Guimarães Vieira

Em sua apresentação, o Sr. **Victor Guimarães Vieira** trouxe informações acerca das atividades do Prodasen, órgão de gestão de informação do Senado Federal.

Atribuições: gerir a informação, implementar a estratégia de tecnologia da informação, prover serviços, soluções, suporte e infraestrutura tecnológica da informação àquela Casa Legislativa, além de gerir os riscos operacionais com origem em tecnologia da informação.

Produtos e serviços: a) soluções tecnológicas aos processos finalísticos da Casa – atividade legislativa, gabinetes de Senadores e orçamento; b) soluções tecnológicas aos processos administrativos, financeiros e de recursos humanos do Senado; e c) padronização dos sistemas desenvolvidos, em código aberto, pelo próprio Prodasen.

Controles de segurança adotados: a) legais, com políticas e normas de segurança no âmbito do Senado Federal e fiscalização externa realizada pelo Tribunal de Contas da União (TCU); b) de gestão corporativa de segurança da informação, com análises e avaliação de riscos; c) técnicos, com a utilização de *firewalls* de rede e de aplicação, IPS, proxy e proxy reverso, criptografia, antivírus, *antispam* e outros produtos complementares para o funcionamento e a preservação do Datacenter; e d) administrativos, com a segregação de funções, segurança perimetral, capacitação de usuários, auditorias e processos de trabalho, podendo envolver outros setores da Casa, como a Polícia do Senado e a Telefonia.

Dados relevantes sobre as atividades de controle de segurança na rede do Senado: a) 35 milhões de mensagens maliciosas bloqueadas de janeiro a outubro de 2013, correspondendo aproximadamente a 30% das

mensagens externas recebidas; b) cerca de 3 milhões tentativas bloqueadas de ataques à rede somente no mês de outubro de 2013.

Melhores práticas adotadas em segurança da informação: recomendações do TCU e orientações do *Control Objectives for Information and related Technology* (COBIT) e da *Information Technology Infrastructure Library* (ITIL).

Indicadores de segurança utilizados: análises de segurança, relatórios de segurança e comunicados de usuários e da comunidade.

Normativos de segurança da informação no Senado Federal: a) Política de Gestão de Riscos Organizacionais do Senado Federal – Ato da Comissão Diretora nº 16/2013; b) acesso e uso da Internet e das redes sociais por meio da Rede do Senado Federal – Ato do Primeiro-Secretário nº 14/2011; c) uso e administração do sistema de correio eletrônico do Senado Federal – Ato do Primeiro-Secretário nº 6/2010; d) uso e administração dos recursos computacionais e da rede do Senado Federal: Ato do Primeiro-Secretário nº 54/2009; e) uso e administração do serviço de acesso à rede sem fio nas dependências do Senado Federal – Ato do Primeiro-Secretário nº 7/2008; f) uso e administração do serviço de acesso remoto da rede local do Senado Federal – Ato do Primeiro-Secretário nº 25/2003; e g) Regulamento Administrativo do Senado Federal que dispõe sobre áreas e uso de tecnologia da informação no Senado Federal.

Encerrada esta primeira parte, os convidados foram questionados pelos parlamentares. A sequência foi iniciada pelo Sr. Eduardo Suplicy.

Pergunta 1 (Senador Eduardo Suplicy). Pediu a definição de *software*, *hardware*, nuvem e e-mail seguro.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: esclareceu que *hardware* é a máquina, a parte física. Já o *software* é o programa.

Nuvem é um conceito atual e complexo. Trata-se de uma tecnologia nova de armazenamento de dados, realizado em múltiplos ambientes, possibilitando maior disponibilidade de acesso.

Um sistema de e-mail é seguro quando se tem o controle de sua programação, conhecendo a cada um dos seus elementos, e se tem o controle sobre o ambiente de proteção. Assim, por exemplo, é o caso do Expresso V3 desenvolvido pelo Serpro a ser adotado no Governo Federal brasileiro, uma vez que foi feito em plataforma de *software* livre e está no ambiente de proteção do próprio Serpro. Ainda quanto ao Expresso V3, disse ser resultado da cópia das melhores funções oferecidas nos *softwares* de mercado, como o Gmail, Exchange e Lotus Notes e que possui alto grau de segurança por ter somente uma porta de acesso a todos os seus componentes, podendo o Serpro alterar o grau de proteção de acordo com as necessidades apresentadas.

Pergunta 2 (Senador Eduardo Suplicy). Pediu o levantamento de quantos e-mails cada senador recebe e envia, para verificar grau de comunicação com a população brasileira. Contou sobre a importância de se acessar os dados pela *internet*, principalmente para controle de gastos públicos.

Resposta do Sr. Victor Guimarães Vieira: afirmou que irá fazer o levantamento do número de e-mails recebidos e enviados pelos senadores e enviará para o gabinete do senador Suplicy.

Pergunta 3 (Senadora Vanessa Grazzioti). Questionou se o Serpro teria condições de promover auditagem nas máquinas da administração direta e indireta.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: sobre auditagem, o convidado afirmou que, atualmente, toda rede bancária se comunica de forma exclusiva com o Sistema Integrado de Administração Financeira da União (Siafi), através do sistema SOTN, desenvolvido pelo Serpro. Assim, o sistema de mensageria é direto para todos os pagamentos feitos para e pela União, controlado pelo Serpro, portanto, auditáveis.

Há, ainda, produtos como o Portal dos Convênios, com auditabilidade em prefeituras, ONGs ou hospitais, com necessidade de pacote de serviços para virtualização de ambientes. Citou a comunicação com os DETRANs do País.

Explicou que o *software* de gestão de segurança utilizado pelo Serpro é o Zabbix, que, apesar de ser aberto e livre internacionalmente, é controlado por aquela empresa pública, possibilitando toda a auditabilidade.

Pergunta 4 (Senadora Vanessa Grazzioti). Perguntou se o Serpro e o Prodasen terceirizam serviços. Em caso afirmativo, indagou quais serviços seriam terceirizados. Se a manutenção das redes e do equipamento no Serpro e no Prodasen é realizada por terceirizados e quais são as medidas de proteção em relação às informações que estão contidas.

Resposta do Sr. André Luiz Bandeira Molina: afirmou que existem vários contratos com terceirizados, mas que há requisitos de segurança, como o termo de confidencialidade. A maioria dos contratos é de cunho operacional, como a central de atendimentos, que realiza

atendimento e monitoramento de chamados. Ademais, quando as prestações de serviço são de manutenção e intervenção no sistema, há o acompanhamento do trabalho. Mas ressaltou que a gestão dos equipamentos e dos *softwares* é realizada pelos servidores do Senado Federal.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: todos os serviços de suporte são realizados pelo Serpro, não terceirizam desenvolvimento e operações de sua rede. Os fornecedores são chamados, apenas eventualmente, quando a equipe técnica não consegue solucionar o problema. Entretanto, o trabalho é realizado em conjunto.

Pergunta 5 (Senadora Vanessa Grazzioti). Perguntou qual o percentual de tecnologia nacional presente nos equipamentos e *softwares* de segurança que são utilizados pelo Serpro e pelo Prodasen. Se existe iniciativa no sentido de se alcançar a autonomia brasileira nessa tecnologia. Se há algum comitê público brasileiro de desenvolvimento de tecnologia da informação ou de segurança da informação.

Resposta do Sr. Victor Guimarães Vieira: afirmou que não sabe precisar exatamente o percentual de tecnologia nacional utilizado pelo Prodasen, mas o índice de importação de tecnologia na questão de *hardware* é bem alto. Entretanto, o mesmo não se dá com os *softwares*, pois o sistema utilizado na área finalística do Senado Federal é desenvolvido internamente.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: esclareceu que existe maior dependência de tecnologia internacional na questão do *software*, mas também é expressiva no *hardware*. O investimento deve ser feito nos dois aspectos.

Pergunta 6 (Senadora Vanessa Grazzioti). Fez referência ao Expresso V3, que é o e-mail público utilizado pelo Governo Federal de utilização exclusiva do Governo. Indagou se há possibilidade de ser desenvolvido um e-mail similar para a população em geral, quem caberia desenvolvê-lo e qual a viabilidade financeira desse projeto.

Resposta do Sr. Victor Guimarães Vieira: afirmou que o desenvolvimento de um correio eletrônico nacional, capaz de atender a população, encontra óbices na concorrência e no elevado custo. Afirmou que o Serpro teria como dimensionar o custo com mais precisão. Para que o projeto seja realizado, o convidado acredita que o incentivo deva ser muito grande.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: informou que a Anatel, empresa pública de telecomunicações do Uruguai, está contratando o Serpro para desenvolver e-mail público e disponibilizar para a população.

Se fosse implantado em um país com as dimensões continentais do Brasil, seria necessária uma infraestrutura mais robusta. Em sua opinião, a Telebrás seria a responsável pelo projeto. Mas sugeriu que as operadoras de telecomunicações ofereçam o serviço aos seus clientes. Frisou que o esforço é universalizar o Expresso V3, apesar do foco do Serpro ser o atendimento à Administração Pública Direta Federal.

Pergunta 7 (Senadora Vanessa Grazzioti). Pediu a opinião dos convidados sobre a criação de uma agência nacional de segurança da informação.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: defendeu a criação de uma agência nacional de segurança da informação, para que se discuta o tema. Elogiou o trabalho que o Exército Brasileiro realiza com a segurança cibernética no País, entretanto frisou que o foco é mais o patrimônio físico do que o cibernético.

Pergunta 8 (Senadora Vanessa Grazzioti). Pediu a opinião dos convidados sobre *data centers* e neutralidade da rede, questões polêmicas do projeto do marco civil da *internet*.

Resposta do Sr. André Luiz Bandeira Molina: o convidado acredita ser importante ter *data centers* nacionais. Entretanto, irá aumentar o custo na prestação do serviço, sendo importante se observar se a informação é crítica ou não.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: disse que neutralidade da rede é fundamental. Segundo ele, significa a obrigação das operadoras em não abrir o pacote de dados dos clientes, como estes utilizam a capacidade de internet contratada.

Defendeu a criação de *data centers* como parte de uma política de desenvolvimento do País, mas não como solução de segurança. A solução tem a ver com respeitar a legislação brasileira.

Pergunta 9 (Senadora Vanessa Grazzioti). Diante da afirmação dos convidados de que todos os equipamentos, inclusive os nossos telefones, possuem *backdoor*, indagou o que garante a segurança no tráfego e no armazenamento das informações, visto que a maior parte dos aparelhos é importada dos Estados Unidos.

Resposta do Sr. Victor Guimarães Vieira: disse que o que garante a segurança é a criptografia.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: a respeito de *backdoor*, o Serpro acredita ser importante trabalhar com auditabilidade, criptografia e *software* livre. Deve-se realizar controle sobre códigos e sistemas estratégicos para o País. Toda importação e exportação passa pelo sistema computacional do Serpro, através da Marinha Mercante, Anvisa, Receita Federal e Polícia Federal – o sistema "Porto sem Papel" foi desenvolvido todo no *software* livre Demoiselle do Serpro.

Assim, o investimento nacional deve ser em criptografia, em *hardware* nacional e *software* livre, para melhor controle dos ambientes da rede.

Pergunta 10 (Senadora Vanessa Grazzioti). Diante da informação que o Governo Federal, em Brasília, utiliza a rede de fibra ótica e questionamento o uso fora da cidade, perguntou o que acontece quando sai da rede governamental e entra em uma rede privada. Afirmou que há vulnerabilidade, pois o Estado brasileiro não dispõe de cabeamento e nem de satélite. O satélite que o País possuía no passado foi vendido junto com a Embratel. E quem forneceu a consultoria para o Governo brasileiro, na época da privatização das comunicações, foi formalmente, a empresa Booz Allen, que trabalha e presta serviços diretamente à NSA. Assim, questionou sobre a necessidade de expandir o cabeamento público.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: afirmou que o Serpro utiliza redes fora de seu ambiente. Os grandes *backbones* são contratados de operadoras, pois a rede pública não tem capacidade de atender, via Telebrás, a necessidade do Serpro. Assim, contratam circuitos

no nível 2, que chegam aos seus centros de dados e, a partir desse momento, os *switches* são administrados pelo Serpro. Há uma diminuição da vulnerabilidade, mas não sua eliminação, visto que há nos *switches* equipamentos importados.

Ainda, comentou a venda do Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD), juntamente com a Embratel. O Brasil era um dos únicos países que produzia emenda de fibra ótica. O Estado desenvolvia a tecnologia e colocava para a indústria, se comprometendo com a demanda. Porém, com a perda do CPqD, o País também perdeu tal tecnologia de central telefônica.

Pergunta 11 (Senadora Vanessa Grazzioti). Perguntou como os órgãos têm alcançado a capacidade tecnológica. É realizado apenas com pessoal próprio, ou conta com o apoio das universidades e convênios? Seria o caso de se criar um comitê de desenvolvimento de tecnologia da informação?

Resposta do Sr. Victor Guimarães Vieira: Existe, no Governo Federal, a TI Controle, que são órgãos do Governo que se mobilizam mensalmente para explicitar as melhores práticas e trocar informações; as próprias contratações. São reuniões mensais para discutir as melhores práticas no Governo Federal. Entretanto, não há um órgão específico para tratar de tecnologia e desenvolvimento entre as universidades e pesquisadores.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: discorreu sobre o projeto brasileiro na área de segurança realizado pela Universidade de São Paulo. Trata-se de um laboratório de pesquisa de alta tecnologia, com destaque para o projeto de desenvolvimento de *hardware*.

Prestam consultoria para o ITI e várias empresas em todo o mundo. Em parceria com o Serpro, pretendem, até o ano de 2014, produzir *hardware* nacional robusto, com criptografia nacional. Elencou outras universidades que possuem projetos na área de segurança: Universidade de Santa Catarina e Universidade de Pernambuco.

Ademais, afirmou que não existe um comitê público de segurança. Visando troca de informações, existe, na esfera federal, o Gabinete de Segurança Institucional (GSI); nas empresas estaduais, a Associação Brasileira de Entidades Públicas de Tecnologia de Informação (ABEP); nas empresas municipais, a Associação Brasileira das Entidades Municipais de Informática (ASBEMI). Entretanto, dizem respeito mais a troca de experiência das melhores práticas do que segurança em si. Destacou a importância de serem criados comitês e trocas de experiências, na lógica do *software* livre.

Por fim, informou que o Serpro possui um centro de pesquisa, com investimentos em tecnologia. Desenvolveram ferramentas, nuvem, Expresso e rede social. Possuem vários projetos com as Universidades dos Estados de São Paulo, Santa Catarina, Rio Grande do Sul, Paraná, Minas Gerais, Pernambuco e Amazonas.

ANEXO III

I. Sugestões apresentadas pela presidente da CPI, senadora Vanessa Grazziotin, acolhidas pelo relator.

Considerações e recomendações a serem incluídas no relatório final da CPI.

Prezados senhores

Cumprimento o trabalho de nosso relator, que ao longo dos últimos sete meses pode compilar e reunir um retrato minucioso de nossas falhas na área de segurança cibernética.

Para corroborar com este relatório, sugiro a inclusão das seguintes recomendações que foram fruto de um encontro muito frutífero que tive em SP com empresas do setor:

AÇÃO 1 – "Compras Educativas" – Criação de um Comitê Gestor no Governo, com alocação de R$50 milhões/ano para compras educativas no setor cibernético. A compra Educativa serve para que a indústria mantenha o seu pessoal do núcleo duro (talentos chave) em atividade e desenvolvendo projetos de menor porte, com o objetivo de se obter ou manter domínio tecnológico em áreas estratégicas.

AÇÃO 2: "Inovação Direcionada" - Criação de edital de subvenção FINEP especifico para o setor cibernético com valor da ordem de 100 milhões. Idealmente, tal edital deve ser coordenado com compras garantidas pelo Governo, tal qual preconizado pela medida MP.6 do Anexo I deste documento.

Adicionalmente, esta ação pode estar coordenada com a AÇÃO 1, acima, e com as medidas 1.2, 4.1 e 4.2 do Anexo I.

Nesta seção são apresentadas medidas viabilizadoras para o setor cibernético no país. Tais proposições se apoiam em parte na publicação "Medidas Viabilizadoras ABIMDE", de Dezembro de 2013.

MEDIDA VIABILIZADORA 1.1 – "Compre Brasil" – Elaboração de legislação objetiva que instrua, oriente e motive os responsáveis pelas aquisições de sistemas e produtos de defesa a priorizar sua compra na BID brasileira. A Constituição Federal estabelece, em seu Artigo 219, que o mercado interno integra o patrimônio nacional e que sua exploração deve visar o desenvolvimento, o bem-estar da população e a autonomia tecnológica do País.

MEDIDA VIABILIZADORA 1.2 – "Programas e Projetos Estratégicos" – Definição e divulgação, com a necessária antecedência, dos principais projetos estratégicos do Ministério da Defesa. A visibilidade antecipada do escopo, do cronograma e do orçamento desses projetos permitirá que a BID brasileira se prepare adequadamente (tanto em termos

de capacitação tecnológica e industrial, quanto de recursos humanos e financeiros) para atender às necessidades.

MEDIDA VIABILIZADORA C.1.5 – "Segurança, Defesa e Infraestruturas Críticas" – Extensão, aos setores de segurança pública e Infraestruturas Críticas, da legislação e dos conceitos aplicados aos produtos e às empresas do setor de defesa.

MEDIDA PONTUAL MP.1 – "Aplicação da Lei 12.598/2012" – Estímulo e, se preservadas condições de concorrência, obrigatoriedade no setor público no uso da Lei 12.598/2012.

MEDIDA PONTUAL MP.2 – "Maior Alcance da Lei 12.598/2012" – Ampliação do escopo da Lei 12.598/2012 para atender compras não só pelas Forças Armadas, mas também sistemas aplicados infraestruturas críticas de Estado, alinhando-se ainda mais com a END.

MEDIDA PONTUAL MP.3 – "Ampliação do escopo do Decreto nº 8.186/2014 de 17 de Janeiro de 2014 (CERTICS)" – Ampliação do referido Decreto para abarcar, além de software, o projeto e o desenvolvimento de hardware e semicondutores, atendendo assim a todo o segmento de TIC. Provê-se, assim, benefícios de concorrência para os sistemas projetados e desenvolvidos no país (maior valor agregado) e não somente para os aqui fabricados.

MEDIDA PONTUAL MP.4 – "Compliance" – Estabelecimento e monitoramento de requisitos de segurança cibernética mínimos a serem observados por provedores de serviços públicos e operadores de

infraestruturas críticas no país, como por exemplo, controle de tráfego, telecomunicações, serviços financeiros, e distribuidores de energia.

MEDIDA VIABILIZADORA 2.1 – "Promoção da Exportação" – Criação de mecanismos, regras e normas governamentais que promovam a exportação de produtos de defesa e segurança e orientem os servidores públicos a participar e contribuir na conquista de clientela estrangeira para os produtos nacionais. A assinatura de acordos bilaterais incentivará as vendas de governo a governo, atendendo àqueles países desejosos de comprar produtos de defesa do Brasil, e permitirá oferecer "garantias de Estado", por meio de um sistema facilitador do tipo, por exemplo, do FMS (Foreign Military Sales) norte-americano.

MEDIDA VIABILIZADORA 3.2 – "Desoneração da Folha de Pagamento" – Desoneração da folha de pagamento das empresas de defesa e segurança, visando dar maior proteção e competitividade ao setor que depende extraordinariamente de mão-de-obra especializada, aplicada em produtos com longos ciclos de desenvolvimentos, e que, em geral, não conta com encomendas regulares.

MEDIDA VIABILIZADORA 4.1 – "Orçamento Público" – Aperfeiçoamento da legislação orçamentaria (LRF – Lei de Responsabilidade Fiscal, PPA – Orçamento Plurianual de Investimentos, LDO – Lei de Diretrizes Orçamentarias e LOA – Lei Orçamentaria Anual) para permitir o comprometimento de recursos orçamentários de longa duração, plurianuais e em volumes compatíveis com as necessidades nacionais de investimento em programas de defesa e segurança. Migração

dos programas de investimento do Ministério da Defesa para os programas prioritários de Governo (como o PAC) garantindo, de imediato, o planejamento de longo prazo e a continuidade dos orçamentos.

MEDIDA VIABILIZADORA 4.2 – "Contra-Garantias" – Criação de mecanismos legais para o reconhecimento do acervo tecnológico das empresas de defesa e segurança como um bem a ser preservado e que possa ser oferecido em contra-garantia às operações financeiras ligadas ao Governo. A indústria de defesa e segurança é, acima de tudo, uma indústria do conhecimento, e o maior patrimônio das empresas é o conhecimento por elas acumulado.

Observação: tais garantias devem servir ao aparato público de financiamento, independente do cliente e do mercado final.

MEDIDA VIABILIZADORA 4.5 – "Continuidade dos Programas" – Criação de mecanismos legais garantidores da execução, financeira e física, e da continuidade dos programas de segurança e defesa, em níveis que garantam o atendimento das necessidades estratégicas nacionais e o fortalecimento da BID.

MEDIDA VIABILIZADORA 4.7 – "Crédito Especial para Ciência, Tecnologia e Inovação" – Criação de arcabouço legal e de mecanismos para a agilização do fornecimento de crédito para o financiamento de programas de interesse estratégico de defesa e segurança, com prazo alongado para sua utilização.

MEDIDA VIABILIZADORA C.5.1 – "Nível Superior – Formação e Aperfeiçoamento" – Ampliação dos esforços de formação, treinamento, especialização e reciclagem de recursos humanos para a área cibernética. Criação de estágios e cursos de nível superior e de pós-graduação, no País e no exterior, nas diversas especialidades necessárias ao projeto, pesquisa, desenvolvimento, inovação, produção e manutenção de produtos de defesa e segurança cibernéticas, aproveitando oportunidades como as oferecidas pelo Programa Ciência sem Fronteiras.

MEDIDAS PONTUAIS MP.5 - "Escola de Cibernética e Spin-Offs" - Criação de Escola Nacional de Cibernética, envolvendo a Academia (Universidades Federais, Estaduais), Empresas, Centros de Pesquisa e a Administração de forma a reunir competências teóricas, técnicas, operacionais e aplicadas. O currículo deve ser amplo em termos de tecnologias e áreas de conhecimento, focando a formação no desenvolvimento e na operação de soluções na área cibernética. Tal escola deverá incentivar, de forma coordenada com os instrumentos de fomento existentes e a serem criados, "spin-offs" (na forma de "start-ups") na área cibernética.

MEDIDA VIABILIZADORA 6.1 – "Projeto, Pesquisa e Desenvolvimento" – Atualização da Política de Ciência, Tecnologia e Inovação para a Defesa Nacional, sua aprovação pelo Legislativo Federal, e edição dos instrumentos normativos decorrentes. Investimentos em capacitação para defesa, por imposição dos países desenvolvidos, não estão sujeitos às regras restritivas da Organização Mundial do Comércio (OMC)

e, usados corretamente, podem se tornar importantes e eficazes instrumentos de política industrial.

MEDIDAS PONTUAIS MP.6 - "Garantias de Compras" – Criação de mecanismos que garantam a coordenação entre recursos de fomento e aquisições mínimas por parte do poder público, no modelo do FINEP INOVA Medicamentos. Garantias adicionais deverão ser providas para à micro e pequena empresa inovadora.

MEDIDA VIABILIZADORA MV.1 – "Monitoramento e Responsabilização na Cadeia Produtiva de Cibernética" – Criação de arcabouço legal, coordenado com um sistema de certificações e homologações, que estabeleça mecanismos de monitoramento dos atores envolvidos na cadeia produtiva de produtos sensíveis da área cibernética, incidindo essa responsabilização nas pessoas naturais, nas pessoas jurídicas envolvidas e na solidariedade entre elas.

MEDIDA VIABILIZADORA C.9.2 – "Homologação e Certificação" – Fortalecimento do sistema nacional de certificação e metrologia (SINMETRO), com a consequente redução dos períodos e dos custos para a homologação de produtos de defesa e segurança e para a certificação internacional dos produtos brasileiros. Concretização de acordos com outras nações para reconhecimento mútuo de tais certificações (por exemplo, a ISO/EIC 15.408 – "Common Criteria"), abrindo o mercado externo para produtos brasileiros.

MEDIDA VIABILIZADORA MV.2 – "Coordenador para a Área Cibernética" – Elevação ou criação de ente executivo para a área cibernética nos escopos civil e militar, com capacidade e autoridade para coordenar os esforços e programas na área.

Este é apenas o início de um longo trabalho de construção de uma segurança cibernética à altura de nossa importância geopolítica.

Senadora Vanessa Grazziotin (PCdoB-AM)

II. Manifestação do Ministro de Estado da Defesa, Celso Amorim, em audiência pública na Comissão de Relações Exteriores e Defesa Nacional, em 27 de março de 2014

"....

Bem, mas além de todas essas funções ligadas à defesa da Pátria e esses projetos e essa permanente luta para ter os recursos necessários, ainda que sempre compreendendo que o País tem também outras necessidades, nós temos que lidar com situações, de certa forma – não diria – imprevistas, mas cuja dimensão não era prevista. Uma delas é a questão da espionagem. O Senador conhece isso hoje em dia melhor do que todos nós, porque esteve muito envolvido na comissão sobre este tema, e

isso nos levou a buscar reforçar ainda mais o que já estava na estratégia nacional de defesa e que já vinha sendo implementado, que é a parte de defesa cibernética. Nós temos um centro de defesa cibernética que está a cargo do Exército, mas é claro que cada força também tem as suas ações nessa área e elas estão sendo coordenadas. E eu determinei, em função dessas questões de espionagem, que fosse feito um grupo de trabalho, que nos dessem recomendações mais imediatas. Na realidade, essas recomendações estão ainda sendo objeto de exame de como implementar. Há várias, mas eu vou salientar duas: uma é uma escola de defesa cibernética, que pode servir, inclusive, para outros órgãos da administração – aliás, queremos trabalhar com eles –, porque a questão de recursos humanos é absolutamente fundamental nesse campo, pois não adianta você ter o equipamento perfeito e ter que depender de uma empresa estrangeira para fazer a revisão, por exemplo. Então, é absolutamente fundamental entre parênteses entre os programas que nós temos apoiado, seja diretamente, seja em conjunto com o MCTI, num programa de nova defesa, tem estado sempre presente a questão de software adequado à defesa. Este é um aspecto: a escola. O outro aspecto – e já é uma coisa dentro do Exército, ainda sendo estudado, mas é importante que se saiba como passar de um centro para um comando de defesa cibernética.

....."

III. Malware da NSA encontrado – documento encaminhado à senadora Vanessa Grazziotin em 8 de abril de 2014

VirusImmune

http://twitter.com/virusimmune
contato@inlovirus.com.br

Malware da NSA encontrado

A empresa de segurança de dados VirusImmune (www.virusimmune.com.br) anuncia a descoberta de três exemplares de malware da NSA (National Security Agency), direcionados exclusivamente ao governo brasileiro e empresas do Brasil:

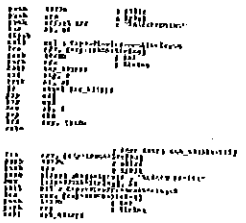
O funcionamento entre eles é muito semelhante e grande parte do código é comum, o que comprova que foram criados pela mesma pessoa ou grupo.

A seguir alguns detalhes:

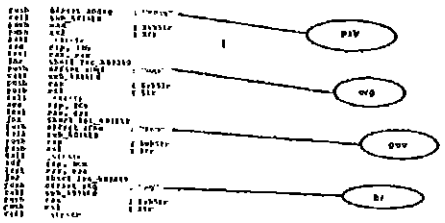
Informações	Exemplar 1	Exemplar 2	Exemplar 3
MD5	(Disponível para parceiros)	(Disponível para parceiros)	(Disponível para parceiros)
Tamanho do arquivo (em bytes)	102.400	172.032	45.056
Inicialização automática?	Não	Não	Não
Ícone	Não	Não	Não
Possui resources?	Não	Não	Não
Assinatura digital?	Não	Não	Não
Compactado?	Não	Não	Não
Strings criptografadas?	Sim	Sim	Sim
Data de compilação	09/05/2012	10/07/2012	01/08/2012
Leitura do Domínio/Workgroup	petr, org, gov, br	petr, org, gov, br	petr, ong, org, gov, br
Arquivos que captura	'.doc', '.ppt', '.xls', 'pass'.*, 'senha'.*	'.doc', '.ppt', '.xls', 'pass'.*, 'senha'.*	-
Método de envio dos arquivos	e-mail para NIASC@nsa.gov via porta 587 (email autenticado) Senha do email: ******** (Disponível para parceiros)	POST para um site na Ásia	Grava dados em um arquivo criptografado: %WINDIR%\windowsupdatareport.log
Keylogger	Não	Não	Sim

Funcionamento:

- Ao iniciar, o malware tenta ler o conteúdo das variáveis do ambiente: USERDOMAIN e LOGONSERVER, para tentar obter o nome do domínio e/ou workgroup:

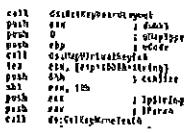


- Em seguida é feita uma checagem por um dos seguintes textos: "petr", "org", "gov" ou "br" (Exemplares 1 e 2) e também por "ong" (Exemplar 3):



- Caso NÃO encontre nenhum dos textos, ele simplesmente sai do malware (isso dificulta a análise por analisadores automáticos de malware, pois os mesmos teriam que ler os nomes de domínio/workgroup com algum dos textos anteriores).

- Keylogger (Exemplar 3):



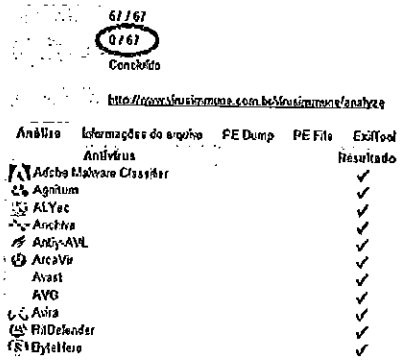
- O keylogger, grava tudo o que é digitado pelo usuário no arquivo %WINDIR%\windowsupdatereport.log em modo criptografado (Exemplar 3):

```
mov     edi, offset aUindowsupdater ; "UindowsUpdateReport.log"
or      ecx, 0FFFFFFFFh
xor     eax, eax
```

- Como o keylogger (exemplar 3) não possui qualquer tipo de método de envio do arquivo, existe a possibilidade de algum outro módulo ler este arquivo e envia-lo para um site, FTP ou email.

- Após todas as unidades serem checadas, ele encerra o malware.

De acordo com a análise feita pelo site www.virusinmune.com.br, nenhum dos 67 antivirus disponíveis na época detectaram qualquer tipo de infecção no arquivo:



Conclusões:

- Pelas características dos exemplares e pela falta de código de inicialização automática, acreditamos que existam módulos específicos que façam a execução dos mesmos. Possivelmente um módulo central que execute os mesmos através de comandos, controle a segurança, faça o controle dos mesmos contra firewalls e etc;
- Os exemplares foram desenvolvidos com intenção de ataque específico e direcionado, como pode ser determinado pelos textos encontrados: petr, gov, org, br;
- A dificuldade em ler o domínio/workgroup com os textos específicos, reduz a chance de um analisador automático de malware identificar os exemplares, necessitando fazer análise manual;
- Após a identificação dos três exemplares pelas empresas de antivirus, possivelmente serão encontrados outros com padrões semelhantes.
- Os três exemplares foram enviados para o site www.virusinmune.com.br em dias diferentes, mas pela mesma fonte, um IP localizado em Nova York (EUA) - (Disponível para parceiros);
- As redes do Governo e das empresas estatais precisam urgentemente de uma checagem minuciosa para identificar outros possíveis problemas/exemplares que devem existir;
- Lembramos que não basta ter uma solução de antivirus instalada, pois nenhum identificou os exemplares. A solução do problema requer conhecimento profundo de arquivos e análise de malware para que seja feita uma pesquisa avançada.

Sala das Sessões,

Senador **RICARDO FERRAÇO**

Resposta do Sr. Glenn: asseverou que não é possível acreditar numa afirmação como essa. Seria muita ingenuidade crer que o Ministério de Minas e Energia foi apenas alvo de um exercício para que o serviço secreto canadense testasse suas habilidades espionárias.

Pergunta 10 (Senador Ricardo Ferraço). O Sr. Glenn sabe como as informações brasileiras são capturadas pelo sistema de espionagem estrangeiro? Elas são interceptadas nas saídas internacionais ou são colhidas onde os cabos brasileiros aportam?

Resposta do Sr. Glenn: afirmou que há documento publicado que relata como os cabos são invadidos pela NSA. Porém, não é detalhado qual cabo a NSA invade exatamente.

Pergunta 11 (Senador Ricardo Ferraço). Existem evidências de espionagem tradicional por meio de interceptações telefônicas realizadas diretamente nas redes de Telecom? Qual o nível de envolvimento das empresas brasileiras de telecomunicações?

Resposta do Sr. Glenn: redarguiu que não é possível afirmar, neste instante, algo sobre isso. É necessário averiguar se nos documentos que possui há alguma informação acerca das empresas brasileiras de telecomunicações e espionagem estrangeira.

Pergunta 12 (Senador Ricardo Ferraço). Há evidências de participação de empresas internacionais, que atuam no Brasil, no esquema de espionagem estrangeiro, a exemplo da AT&T?

Resposta do Sr. Glenn: afirmou que há matérias publicadas que explicam o sistema usado pela NSA contra outros países. Em síntese, a

NSA desenvolve um programa de cooperação com uma grande empresa de telecomunicação. Esta, por sua vez, faz acordos com empresas estrangeiras, permitindo o acesso a dados de cidadãos e de empresas estrangeiras. Disse que uma dessas empresas que participaram do programa com a NSA foi a AT&T. Assentou que várias empresas brasileiras possuem contrato com a AT&T, mas ele não pode afirmar que é a AT&T a empresa que coleta os dados e repassa para a NSA. Aliás, é esta a informação mais protegida da NSA: quais as empresas fazem parte do programa de cooperação.

Pergunta 13 (Senador Ricardo Ferraço). Há indícios de outros países, além dos integrantes do grupo "Five Eyes", estarem usando a inteligência de comunicações para fins de espionagem?

Resposta do Sr. Glenn: informou que existem três grupos que se relacionam com a NSA. O primeiro é o "Five Eyes", que exerce a função de espionagem e, ao que parece, não é espionado. Este grupo compreende os EUA, o Canadá, a Inglaterra, a Austrália e a Nova Zelândia. O segundo, é composto por alvos da NSA, mas que, às vezes, trabalham em conjunto com ela. É o caso, por exemplo, de Alemanha, França, Espanha e Itália. Um terceiro conjunto, e aqui se situa o Brasil, é preenchido apenas pelos alvos da NSA. Todavia, ele não sabe dizer se há outros países espionando o Brasil, além do Canadá, dos EUA e da Inglaterra.

Pergunta 14 (Senador Ricardo Ferraço). Há algum indício de quebra de dados criptografados durante as investidas recentes de espionagem?

Resposta do Sr. Glenn: asseverou que há indícios sobre essa ruptura de informações criptografadas, mas que elas não se referem ao

Brasil especificamente. Salientou, todavia, que ao se quebrar determinada informação secreta da internet, isso fragiliza o sistema, o que pode impactar futuramente o Brasil.

Pergunta 15 (Senador Ricardo Ferraço). V. Sa. ainda mantém contato com o Sr. Snowden?

Resposta do Sr. Glenn: afirmo que mantém contato com o Sr. Snowden, quase diariamente.

Pergunta 16 (Senador Ricardo Ferraço). É possível o Sr. Snowden contribuir para esta CPI, de forma mais objetiva, já que ele é a fonte primária das informações?

Resposta do Sr. Glenn: embora não possa falar pelo Sr. Snowden, o Sr. Glenn acredita que ele saiba mais detalhes sobre as espionagens desenvolvidas pelos EUA e aliados. Repisou, todavia, a necessidade de ele estar protegido para poder divulgar tais informações. Caso interesse à CPI, o Sr. Snowden pode ser contactado por meio de seu advogado, cujo endereço eletrônico é público e está disponível na internet.

Tendo em vista esta informação, o Senador Ricardo Ferraço manifestou a necessidade de serem formalizados dois requerimentos: um para o advogado do Sr. Snowden, para que consulte-o sobre a possibilidade de teleconferência com esta CPI; e outro para a missão diplomática da Rússia, país em que está asilado Snowden, com o fito de solicitar autorização do embaixador para esta interlocução.

Pergunta 17 (Senadora Vanessa Grazziotin). Em relação ao "Five Eyes", existe um acordo de cooperação entre os países componentes ou eles agem de maneira individual/

Resposta do Sr. Glenn: disse que há tanto colaboração entre os países do "Five Eyes" como atuação individual em tópicos específicos. Informou que este grupo se reúne com frequência para compartilhar informações capturadas mediante espionagem.

Pergunta 18 (Senador Ricardo Ferraço). Há cooperação de pessoa física ou jurídica com a espionagem dos EUA, isto é, empresas como Google, Facebook ou Skype têm relação com a NSA?

Resposta do Sr. Glenn: afirmou que um artigo publicado por ele já tratou desse tema. Reconheceu que muitas dessas empresas negaram ter relação ampla com a NSA. Mas ponderou que essa negativa se referiu ao fato de que a NSA não tem acesso ilimitado aos seus bancos de dados. O acesso é permitido apenas na dimensão em que a lei autoriza. Sucede que a lei dos EUA possui limites claros para cidadãos americanos, e quase não os têm para estrangeiros. Em verdade, para a espionagem estrangeira ser autorizada, basta que a NSA vá ao Tribunal Secreto e apresente seu programa de investigação que a ordem será concedida. Na prática, não há filtro algum.

Pergunta 19 (Senador Ricardo Ferraço). Qual a capacidade do Brasil em termos de contrainteligência e de proteção cibernética?

Resposta do Sr. Glenn: embora não seja perito, afirmou que existem várias propostas interessantes sendo desenvolvidas, não só no Brasil, mas também na Europa, para construir servidores independentes dos

EUA. Hoje, a raiz do problema é a internet depender, em grande parte, de servidores norte-americanos.

Pergunta 20 (Senadora Vanessa Grazziotin). V. Sa. já foi vítima de ameaças ou de algum tipo de intimidação?

Resposta do Sr. Glenn: reafirmou que, por trabalhar com jornalismo de alto risco, já sofreu várias ameaças, sobretudo do governo britânico. Este, aliás, informou que está em andamento uma investigação criminal contra ele, tendo por base as matérias lançadas nos últimos dias.

Pergunta 21 (Senadora Vanessa Grazziotin). Recentemente, o escritor búlgaro-germânico, Ilija Trojanow, foi detido em Miami pela companhia aérea American Airlines. V. Sa. tem informações sobre este caso?

Resposta do Sr. Glenn: disse que conhece o Sr. Ilija Trojanow e que ele é muito respeitado no meio jornalístico. Esclareceu que sua detenção se deu em razão da agressividade com que denunciou o sistema de espionagem da NSA contra a Alemanha.

Encerradas as perguntas, a Senadora Vanessa Grazziotin pediu que fosse elaborado um requerimento solicitando ao Itamaraty informações mais detalhadas sobre o incidente de detenção do Sr. David Miranda.

Após a aprovação de requerimentos, a Presidente da CPI da Espionagem, Senadora Vanessa Grazziotin, encerrou a audiência pública.

8ª Reunião, realizada no dia 15/10/2013 (Polícia Federal e Anatel)

Objeto: Audiência pública com a presença dos senhores José Alberto de Freitas Iegas, Diretor de Inteligência da Polícia Federal, e João Batista de Rezende, Presidente da Anatel.

No dia 15 de outubro de 2013, sob a Presidência da Senadora Vanessa Grazziotin, a CPI da Espionagem ouviu o Sr. José Alberto de Freitas Iegas, Diretor de Inteligência da Polícia Federal, e o Sr. João Batista de Rezende, Presidente da Anatel.

Após a abertura dos trabalhos, a Presidente da Comissão, Senadora Vanessa Grazziotin, apresentou breve síntese dos resultados obtidos pela CPI até o momento, no que tange às audiências públicas. Dentre as propostas ouvidas, destacou: que seja dada particular atenção ao marco civil da internet, em especial as questões da neutralidade, dos direitos do usuário e da governança; a criação da Agência de Segurança Cibernética, voltada para a proteção dos dados de defesa estratégica do Brasil; a utilização obrigatória de *softwares open source* no governo central, empresas estratégicas e estrutura de defesa; a obrigação da Anatel homologar somente o uso de roteadores sem *backdoor* pelas empresas de telecomunicações; a criação e estímulo à rede segura para tráfego de dados; e a proibição de participação em licitações de empresas que descumprirem legislação de proteção de dados pessoais. Destacou que estas propostas estão alinhadas com relatório aprovado pela União Europeia, bem como com as propostas apresentadas pela Presidenta Dilma Rousseff em seu discurso proferido na ONU.

O primeiro convidado a fazer uso da palavra foi o **Sr. José Alberto de Freitas Iegas**. Informou que, no âmbito da Polícia Federal, foi instaurado inquérito policial para investigar a possível quebra do sigilo das comunicações brasileiras e, a pedido do Diretor-Geral, Dr. Leandro Coimbra, entregou cópia integral do inquérito à CPI.

Com base nas denúncias em investigação, constatou a necessidade de aprimoramento do sistema de comunicação do Governo Federal, bem como da legislação da área de inteligência, especialmente no que tange às atividades relacionadas ao antiterrorismo.

No que diz respeito à atuação das empresas de tecnologia, afirmou que a maioria colabora com as investigações da Polícia Federal e cumpre integralmente as ordens judiciais recebidas. No entanto, algumas, em especial a Google, impõem obstáculos, alegando que, como a matriz está nos Estados Unidos, seria necessária a obtenção de ordem emanada de autoridade judiciária americana.

Como conclusão de sua exposição, destacou que há vulnerabilidades na área de informação, considerando o fator humano o mais importante, devendo ser objeto de investimento contínuo e especial atenção.

Em seguida, a CPI passou a palavra ao **Sr. João Batista de Rezende**, Presidente da Anatel, que tratou da confidencialidade no uso de redes de telecomunicações no Brasil e das ações realizadas pela Anatel em relação às notícias divulgadas pela imprensa após as revelações feitas por Edward Snowden.

O ponto de partida de sua explanação foi o direito à inviolabilidade da intimidade das pessoas, assim como a inviolabilidade do

sigilo das comunicações telefônicas e de dados, tendo como única exceção o cumprimento de ordem judicial, para fins de investigação criminal ou instrução processual penal. Neste sentido, frisou que a Anatel não armazena nem realiza interceptação de dados de ligações telefônicas, dados pessoais ou troca de informações na forma de e-mail ou mensagens.

A seguir, tratou das dimensões estratégicas da Internet e das telecomunicações, com foco na governança da Internet. Informou que há várias questões importantes relacionadas ao tema, que devem ser abordadas no marco civil, destacando as seguintes: comércio eletrônico, tributação e direitos do consumidor; direito à privacidade e à intimidade dos cidadãos; liberdade de expressão e direito à informação; inovação, novos modelos de negócios e defesa da concorrência; inclusão digital e massificação dos serviços; e segurança cibernética. Em sua opinião, o marco civil é uma oportunidade para analisar questões referentes à defesa das informações estratégicas do Estado.

No que diz respeito à mecânica das comunicações globais, explicou que para que usuários possam realizar chamadas internacionais ou utilizar seus terminais em *roaming*, são necessários acordos de interconexão internacional entre empresas brasileiras de telecomunicações e empresas em outros países. No momento da interconexão, há troca de informações de sinalização entre as operadoras, incluindo: número de origem, número de destino, duração e horário da chamada. Estes dados saem do país por canais como cabos submarinos ou satélites. Tendo em vista que as principais empresas da Internet são dos Estados Unidos, há concentração de tráfego e das receitas do setor naquele país. Em sua visão, o desequilíbrio do tráfego aumenta a vulnerabilidade das comunicações de brasileiros.

Após esta visão geral do mercado, passou a explanar sobre a atuação da Anatel em relação aos fatos divulgados pela imprensa. Neste sentido, informou que a agência iniciou procedimento de fiscalização, enviando uma série de perguntas para as principais empresas de telecomunicações para que fosse possível analisar as fragilidades nas redes, tendo por fundamento o fato de que as prestadoras são responsáveis pela inviolabilidade do sigilo das comunicações em toda a sua rede, bem como pela confidencialidade dos dados e informações. Destacou que este trabalho está sendo realizado em conjunto com a Polícia Federal.

Os principais temas abordados nos questionamentos foram os seguintes: 1) Política de controle de acesso a informações; 2) Controles de acesso (físico e remoto); 3) Política de proteção contra códigos maliciosos e vírus; 4) Procedimentos de *backup* e recuperação de dados e informações; 5) Contratos internacionais de *Roaming* e Interconexão; 6) Procedimentos e registros quanto a incidentes de segurança, Centros de Operações de Segurança (SOC) e coordenação com outros centros; e 7) Ações específicas em resposta à divulgação das notícias sobre a suposta espionagem feita pela *National Security Agency* (NSA).

Da análise das respostas recebidas, constatou-se que:

a) Todas as empresas consultadas afirmam possuir controle de acesso, embora nem todas sigam normas internas ou padrões e normas de órgãos certificadores;

b) Nem todas mantém controle de acesso por meios de autenticação (senhas e *logins*);

c) Todas afirmaram que utilizam *software* específico de proteção e segurança tanto nas estações quanto nos servidores, e possuem

equipamentos programados para atuar em períodos pré-determinados de periodicidade para a varredura;

d) Todas as empresas afirmaram possuir rotinas de *backups*, embora nem sempre o local de armazenamento dos dados esteja no Brasil;

e) Algumas operadoras brasileiras mantêm contratos que normatizam os procedimentos de completamento de chamadas internacionais em território brasileiro e em território estrangeiro (interconexão e *roaming*); esses acordos são cobertos por cláusulas específicas de segurança e confidencialidade, não incluindo qualquer aspecto de cooperação por parte das prestadoras brasileiras no que diz respeito à coleta de informações de chamadas ou de usuários brasileiros.

f) Praticamente todas as empresas informaram que não existiram ocorrências ou suspeitas de violação dos sistemas ou redes de telecomunicações nos últimos três anos que colocassem em risco dados críticos. Nas tentativas de invasão detectadas, todas foram devidamente bloqueadas pelos sistemas de segurança implantados e tratavam de dados institucionais ou servidores utilizados para testes.

g) Quanto às ações específicas sobre a suposta espionagem da NSA, as prestadoras responderam, por meio do Sinditelebrasil, que "nenhuma prestadora de serviços de telecomunicações associada provê ou facilita informações que possam quebrar o sigilo de seus usuários, salvo mediante ordem judicial na forma da lei brasileira". Além disso, em função das denúncias, apenas uma prestadora informou ter realizado procedimentos de auditorias extraordinárias, nas quais não foram detectadas qualquer anormalidade ou atividade suspeita.

Por ocasião da apresentação na CPI, a documentação recebida encontrava-se em análise pelos técnicos da Anatel. Também haviam sido

encaminhadas para a Polícia Federal e para a Agência Brasileira de Inteligência, atendendo a solicitações recebidas.

Algumas medidas preventivas e reativas foram citadas, com destaque para o projeto de Segurança de Infraestruturas Críticas de Telecomunicações (SIEC), com foco inicial nos grandes eventos internacionais. Outras medidas citadas foram: a) Desenvolvimento de Regulamentação para Mitigação de Desastres, que inclui o Gerenciamento de Riscos em Redes de Telecomunicações; b) Implantação da Gerência da Porta 25, com impacto na redução de *spams*; c) Regulamentos de Qualidade para redes de banda larga fixa e móveis, com monitoramento da disponibilidade operacional e de parâmetros técnicos por uma entidade externa independente; e d) atuação, em cooperação, com diversos organismos internacionais.

Como conclusão de sua apresentação, destacou a necessidade de investimentos para se mitigar riscos de espionagem no Brasil. Citou números relacionados ao Serviço de Inteligência dos EUA, que possui 107 mil funcionários e um orçamento de US$ 52,6 bilhões. Por fim, indicou cinco dimensões a serem abordadas em relação à segurança cibernética: 1) Medidas legais, relacionadas ao aprimoramento da legislação, tendo em conta as atividades ilícitas cometidas nas redes de TIC em âmbito nacional e internacional; 2) Medidas técnicas e processuais, voltadas para a promoção da segurança e gestão de riscos, incluindo esquemas de certificação, protocolos e normas; 3) Estruturas institucionais, destacando-se proposta de criação de uma agência cibernética, que pudesse abranger vários setores, uma vez que, na visão do expositor, trata-se da segurança do Estado brasileiro; 4) Capacitação, incluindo estratégias e mecanismos de formação de pessoal; e 5) Cooperação internacional.

Encerrada esta primeira parte, os convidados foram questionados pelos parlamentares. A sequência foi iniciada pelo Relator da CPI, Senador Ricardo Ferraço, que indagou ao Sr. José Alberto de Freitas Iegas, da Polícia Federal, nos seguintes termos:

Pergunta 1 (Senador Ricardo Ferraço). O Departamento de Inteligência da Polícia Federal foi surpreendido com as denúncias trazidas a público pelo Sr. Snowden ou existiam evidências de que isso poderia estar acontecendo?

Resposta do Sr. José Alberto de Freitas Iegas: afirmou que foram, sim, surpreendidos. No entanto, esclareceu que espionagem e contraespionagem não é atribuição finalista da Polícia Federal.

Pergunta 2 (Senador Ricardo Ferraço). – A Polícia Federal dispõe de informação e conhecimento de que existam bases da Agência de Segurança Nacional dos Estados Unidos funcionando na Capital, Brasília, ou em outras cidades, como foi denunciado há algum tempo por alguns veículos de comunicação?

Resposta do Sr. José Alberto de Freitas Iegas: asseverou não ser verdadeira a notícia de que há bases americanas instaladas em Brasília, como foi veiculado pela imprensa. Afirmou, ainda, que não existe nenhuma base dos Estados Unidos trabalhando em conjunto com a Polícia Federal, da forma como foi divulgado.

Pergunta 3 (Senador Ricardo Ferraço). Existe algum tipo de parceria entre o Departamento de Polícia Federal e a Agência de Segurança Nacional do governo norte-americano?

Resposta do Sr. José Alberto de Freitas Iegas: informou não haver e nunca ter existido parceria entre a Polícia Federal e a NSA. Há cooperação com a Embaixada dos Estados Unidos, assim como existe com vários outros países, no aspecto de troca de informações, cooperação e capacitação, sempre relacionadas à área criminal e à área de antiterrorismo.

Pergunta 4 (Senador Ricardo Ferraço). Como se dá a interação do Departamento de Polícia Federal e outros órgãos que lidam com crimes e segurança cibernética de nações com as quais o nosso País mantém relações amistosas? Há alguma estrutura semelhante nos países vizinhos?

Resposta do Sr. José Alberto de Freitas Iegas: informou que a Polícia Federal possui um núcleo especializado em crimes cibernéticos. Acrescentou que há em torno de 17 ou 18 adidâncias no exterior – na América do Sul, México, Estados Unidos e Europa – que atuam na troca de informações e na interação com outros países e organismos internacionais, em função de vários acordos e tratados firmados pelo Governo brasileiro, com transparência, jamais com ações voltadas à espionagem ou contraespionagem, mas com foco na apuração de crimes.

Pergunta 5 (Senador Ricardo Ferraço). É possível afirmar que temos um nível significativo de segurança para fazer frente às ameaças cibernéticas? O que seria necessário para melhorar nossa capacidade de proteção?

Resposta do Sr. José Alberto de Freitas Iegas: considerando os altos investimentos realizados pelos Estados Unidos na área de tecnologia da informação, desde a criação da Internet, o convidado opinou pela necessidade do Brasil realizar investimentos constantes, capacitação e aprimoramento permanente na área de tecnologia e segurança. Acredita haver redes relativamente seguras, tendo citado, no âmbito da Polícia Federal, a existência de algumas redes criptografadas, que fazem com o fluxo de informações seja seguro. Mas considera não ser possível afirmar que as redes estejam protegidas, de forma absoluta.

Pergunta 6 (Senador Ricardo Ferraço). No inquérito que V. Sª coordena, foi ouvido o correspondente do *The Guardian*, o Sr. Glenn Greenwald?

Resposta do Sr. José Alberto de Freitas Iegas: afirmou que ele foi ouvido, tendo, inclusive, sido entregue cópia do depoimento à CPI. No entanto, esclareceu que o Sr. Glenn Greenwald apenas apresentou informações genéricas, que não foram contundentes na elucidação dos fatos. Acrescentou que o foco das investigações é descobrir se ocorreu quebra ilegal do sigilo das comunicações, sendo esta a questão criminal a ser apurada.

Pergunta 7 (Senador Ricardo Ferraço). V. Sª considerou que as denúncias ou os detalhamentos das denúncias são superficiais ou mesmo fantasiosas?

Resposta do Sr. José Alberto de Freitas Iegas: sem desqualificar as informações prestadas pelo jornalista, que considera importantes para alertar quanto às vulnerabilidades de nossos sistemas,

esclareceu que, para fins de investigação criminal, que é o foco da Polícia Federal, as informações prestadas não foram contundentes, mas um pouco superficiais.

Pergunta 8 (Senador Ricardo Ferraço). Após considerar que o correspondente do *The Guardian*, de certa forma, é uma fonte secundária de informações, sendo a fonte primária o Sr. Snowden, questionou se a Polícia Federal dispõe de adido militar na Embaixada do Brasil na Rússia e se o inquérito em curso está considerando a hipótese de ouvir o Sr. Snowden.

Resposta do Sr. José Alberto de Freitas Iegas: informou que a Polícia Federal não dispõe de adido militar na Embaixada do Brasil na Rússia, mas que, por meio de cooperação internacional, a Polícia Federal está tentando realizar a oitiva do Sr. Snowden. Acrescentou que esta oitiva é uma das prioridades do inquérito.

Pergunta 9 (Senador Ricardo Ferraço). Que tipo de providência concreta foi realizada pelo Departamento de Polícia Federal para que o Governo brasileiro possa, através de suas estruturas, ouvir o Snowden?

Resposta do Sr. José Alberto de Freitas Iegas: esclareceu que a tentativa de realizar a oitiva do Sr. Snowden está sendo feita por intermédio do Ministério da Justiça e do Ministério das Relações Exteriores, através de acordos e tratados internacionais, utilizando-se de meios diplomáticos.

Pergunta 10 (Senador Ricardo Ferraço). Questionou se a oitiva do Sr. Snowden poderia ser considerada uma diligência definitiva para que o inquérito possa ser concluído, perguntando, também se há data para sua conclusão.

Resposta do Sr. José Alberto de Freitas Iegas: informou que não há data para conclusão do inquérito. Há questões técnicas que precisam ser esclarecidas e diligências que a Anatel tem realizado. Apesar de não considerar que estejam reféns da oitiva do Sr. Snowden, considera que ele certamente tenha conhecimento de detalhes técnicos importantes, que facilitariam as investigações e trariam novos elementos ao inquérito policial.

Pergunta 11 (Senador Ricardo Ferraço). Indagou se, ainda que o inquérito não seja dependente da oitiva do Sr. Snowden, ela se constituiria em um fato determinante para a se apurar as denúncias com maior profundidade.

Resposta do Sr. José Alberto de Freitas Iegas: confirmou que a oitiva do Sr. Snowden é um fato determinante e uma providência importantíssima para o prosseguimento do inquérito.

Pergunta 12 (Senador Ricardo Ferraço). Não há prazo para conclusão do inquérito? O inquérito, quando é constituído, não possui prazo definido?

Resposta do Sr. José Alberto de Freitas Iegas: esclareceu que há um prazo inicial de 30 dias, mas que já houve pedido de prorrogação por mais 30 dias. Acrescentou que, diante da necessidade de realização de novas diligências, a Polícia Federal tem solicitado

prorrogação de prazo ao Ministério Público e à Justiça, que têm concedido. Asseverou, no entanto, que tem a intenção de concluir o inquérito o mais breve possível, mesmo que com ressalvas, se houver impedimento e não possa ser realizada a oitiva do Sr. Snowden.

Comentários do Relator, Senador Ricardo Ferraço. Ao concluir os questionamentos formulados ao Sr. José Alberto de Freitas Iegas, externou sua impressão de que há coincidência de interesses entre o inquérito conduzido pela Polícia Federal e as informações almejadas pela CPI. Reconheceu que as denúncias feitas pelo Sr. Glenn Greenwald são contundentes, importantes; no entanto, avaliou que não trouxeram à Comissão elementos suficientes para responder questões importantes, tais como: houve violação das comunicações da Presidente Dilma? Houve quebra das comunicações da Petrobras? De que maneira foi violado? Como foi violado?

Resposta do Sr. José Alberto de Freitas Iegas: Anuiu plenamente com as ponderações do Relator, acrescentando, por sua vez, que faltam dados e informações que possam confirmar as denúncias, sendo elas superficiais.

A seguir, o Relator formulou perguntas ao **Sr. João Batista de Rezende**, Presidente da Anatel, nos seguintes termos:

Pergunta 13 (Senador Ricardo Ferraço). Em sua primeira pergunta dirigida ao Presidente da Anatel, o Relator tratou do marco civil da Internet. Em suas palavras: "De que maneira o novo marco civil poderá contribuir objetivamente para a construção de redes que possibilitem maior

segurança para o nosso País? Na avaliação de V. Sª e da Anatel, isso é uma questão de legislação ou de investimento em torno de estruturas que possam dar ao nosso País a condição de melhorar a sua capacidade de proteção e de reação, considerando a vida real como ela é, considerando que vamos continuar convivendo com esse tipo de violação? Como o novo marco civil poderá contribuir objetivamente para inibir a espionagem ou a violação?"

Resposta do Sr. João Batista de Rezende: afirmou que, em sua visão, o sistema de proteção de dados e informações estratégicas do Estado concretiza-se muito mais do ponto de vista operacional do que em função do marco civil. No entanto, considera que as relações entre pessoas no Brasil e as empresas transnacionais, especificamente Google e Facebook, podem ser melhor regulamentadas, com aprimoramento do entendimento de responsabilidades e deveres desses grupos em nosso país.

Pergunta 14 (Senador Ricardo Ferraço). O Relator perguntou se os questionamentos que foram conduzidos pela Anatel às nossas companhias Telecom até o momento seriam satisfatórios. Contextualizou sua pergunta, comentando ter sido dito à CPI, pelo Sr. Glenn Greenwald, que uma das possibilidades de informações terem sido violadas ou vazadas seria como decorrência da existência de parcerias ou alianças entre empresas de telecomunicações no Brasil e companhias de outros países, sobretudo norte-americanas. Indagou se há algum indicativo neste sentido.

Resposta do Sr. João Batista de Rezende: informou que, até o momento, não há nenhum tipo de indício que leve a concluir que há colaboração ou envio de informações para organismos de espionagem.

Acrescentou que, em sua opinião, não haverá em documento algum, formal, a declaração de que alguém estaria colaborando com espionagens. Lembrou que os documentos coletados foram enviados para a Polícia Federal, que poderá aprofundar nas apurações. Novamente interpelado pelo Relator sobre o assunto, reiterou a resposta dada.

Pergunta 15 (Senador Ricardo Ferraço). Dirigindo-se aos dois convidados, concluiu seus questionamentos, solicitando que externassem suas avaliações sobre o estado da arte e o atual nível de desenvolvimento da segurança cibernética em nosso País, com informações sobre o que está sendo realizado e o que deveria ser feito, tendo em conta as ações no mesmo sentido de outros países, que, como o Brasil, buscam protagonismo internacional.

Resposta do Sr. João Batista de Rezende: opinou ser necessário investir mais em rede de tecnologia e em *softwares*. Além disso, acredita ser importante a criação de um organismo que coordene as várias entidades que trabalham com segurança cibernética: o Ministério da Defesa, o Gabinete de Segurança Institucional da Presidência, o Ministério de Ciência e Tecnologia, bem como as agências que atuam na área. Citou o exemplo dos Estados Unidos, onde ocorreu, após o atentado terrorista de 11 de setembro, a criação de uma agência para coordenar as demais agências, atuando em diversas frentes, tais como as áreas diplomática e operacional. Indagado pelo Relator se essa integração no Estado brasileiro hoje não existe, respondeu que, em sua opinião, a reflexão sobre estas questões estão, agora, iniciando.

Resposta do Sr. José Alberto de Freitas Iegas: corroborou a afirmação do Presidente da Anatel no que tange à necessidade de grandes

investimentos em tecnologia, incluindo satélites próprios, e investimentos constantes em capacitação. Vislumbra a criação de uma agência que possa coordenar outras organizações, nos moldes da ANS americana, como uma possibilidade para assessorar diretamente a Presidência da República.

Concluídos os questionamentos por parte do Relator, Senador Ricardo Ferraço, a Srª. Presidente, Senadora Vanessa Grazziotin, formulou suas perguntas, nos seguintes termos:

Pergunta 16 (Senadora Vanessa Grazziotin). Dirigindo-se ao Presidente da Anatel, perguntou, em relação aos questionamentos encaminhados às empresas, se todas responderam.

Resposta do Sr. João Batista de Rezende: informou que enviaram os questionamentos para as maiores empresas, que são aquelas com contratos e conexões de *roaming*. Comentou que há várias prestadoras de serviços muito pequenas, e julgaram que não seria interessante incluí-las. Em relação às empresas para as quais os questionamentos foram enviados, informou que todas responderam.

Pergunta 17 (Senadora Vanessa Grazziotin). Dirigindo-se ao Sr. João Batista de Rezende, questionou como se dá a fiscalização da Anatel nas empresas que trabalham com Internet, instaladas no Brasil, e se há fiscalização como a que ocorre com as empresas de telecomunicações.

Resposta do Sr. João Batista de Rezende: informou que, em relação à Internet, o trabalho de fiscalização refere-se a requisitos de qualidade, que é o serviço de comunicação multimídia. Não há fiscalização de conteúdo. Por fim, esclareceu que a fiscalização das empresas que

trabalham com Internet é diferente da que ocorre com as empresas de telecomunicações.

Pergunta 18 (Senadora Vanessa Grazziotin). O processo de homologação dos equipamentos de telecomunicações regulamentado pela Anatel poderia ser aperfeiçoado para contemplar a verificação e detecção das vulnerabilidades propositadamente inseridas pelo fabricante?

Resposta do Sr. João Batista de Rezende: informou que seriam necessários investimentos em tecnologia e que a Anatel se instrumentalizasse com esta finalidade, para ser possível detectar fragilidades nos *softwares*.

Pergunta 19 (Senadora Vanessa Grazziotin). Questionou se na regulamentação da Anatel está previsto que as empresas destaquem ou registrem as possíveis vulnerabilidades em seus equipamentos.

Resposta do Sr. João Batista de Rezende: em atenção à presente pergunta, e complementando a resposta anterior, esclareceu que, nas homologações, a Anatel busca verificar questões de vulnerabilidade. No entanto, como a espionagem é um processo ilegal, considera evidente que não se possa detectar facilmente vulnerabilidades propositadamente inseridas pelos fabricantes. No que tange à regulamentação, informou que não há previsão de que a própria empresa explicite eventuais vulnerabilidades de seus equipamentos, pelo fato de se partir do suposto que os *softwares* não podem trazer prejuízos à prestação dos serviços.

Pergunta 20 (Senadora Vanessa Grazziotin). Há possibilidade de a Anatel adotar um sistema de auditagem regular quanto à segurança das operadoras de comunicação?

Resposta do Sr. João Batista de Rezende: afirmou que acompanham a segurança das redes implantadas no Brasil, destacando que atuam buscando a melhor qualidade na prestação de serviços para o usuário, mas não com o objetivo de impedir processos de espionagem.

Pergunta 21 (Senadora Vanessa Grazziotin). Considerando a lei americana chamada "Ato Patriótico", que exige autorização judicial para que empresas ofereçam dados de cidadãos americanos, mas não estabelece tal requisito para estrangeiros, questiona se haveria outra forma, tecnológica ou não, de detectar o repasse de informações por parte de empresas instaladas no Brasil, seja de Internet ou de telecomunicações, para a NSA.

Resposta do Sr. João Batista de Rezende: informou que, nos procedimentos formais, não. Somente como atividade de contraespionagem, que não é objeto da Agência.

Pergunta 22 (Senadora Vanessa Grazziotin). Destacando ser este um ponto essencial, questionou ao Presidente da Anatel quais as iniciativas de contraespionagem adotadas pelo Brasil, seja pela própria Agência, seja por outro órgão.

Resposta do Sr. João Batista de Rezende: esclareceu que a Agência Nacional de Telecomunicações regula o setor. Não realiza nenhuma atividade de espionagem, nem de contraespionagem. Em relação

a eventuais atividades de proteção, busca atuação em cooperação com a Abin e a Polícia Federal.

Pergunta 23 (Senadora Vanessa Grazziotin). Partindo da indagação se é comum embaixadas pedirem instalação de antenas, a Presidente da CPI solicitou informações sobre a embaixada americana.

Resposta do Sr. João Batista de Rezende: informou ser comum que embaixadas realizem pedidos relacionados à instalação de antenas. No que tange à embaixada americana, disse que ela tem uma outorga de serviço limitado privado, com 821 estações espalhadas no Brasil. Há unidades fixas e outras móveis. Funcionam regularmente. A Anatel possui a localização e demais dados registrados. Quanto à fiscalização, informou que se dá sob o aspecto técnico, não em relação à utilização, ao conteúdo das comunicações.

Comentário da Senadora Vanessa Grazziotin: considerando as respostas, a Presidente da CPI solicitou ao Presidente da Anatel o envio dos dados referentes às instalações de antenas da embaixada americana.

Pergunta 24 (Senadora Vanessa Grazziotin). Dirigindo-se ao Sr. José Alberto de Freitas Iegas, indagou como se dá a interação entre o Departamento da Polícia Federal e outros órgãos que lidam com crimes de segurança cibernética.

Resposta do Sr. José Alberto de Freitas Iegas: informou que, em relação aos organismos nacionais, essa troca de informações é permanente. Dependendo da necessidade, há reuniões periódicas pelo Sistema Brasileiro de Inteligência, presidido pela Abin. Quando há necessidade de informação ou diligência formal fora do país para instrução

de investigações, isso ocorre por meio de cooperação com organismos internacionais de vários países que têm representação diplomática no Brasil.

Pergunta 25 (Senadora Vanessa Grazziotin). Indagou se há algum mecanismo tecnológico que seja capaz de detectar quando uma informação está sendo interceptada ou quando dados estão sendo repassados.

Resposta do Sr. José Alberto de Freitas Iegas: informou que obter esse tipo de informação é muito difícil, pois se ocorre espionagem, isso se dá de maneira clandestina.

Comentário da Senadora Vanessa Grazziotin. Considerando matéria do dia, que trata da coleta e armazenamento de listas de *e-mails* pessoais pela agência NSA, dos Estados Unidos, ponderou que, segundo o noticiário, tais ações dependem de acordos com empresas de telecomunicações instaladas ao redor do mundo e que, segundo a matéria, seriam acordos secretos.

Pergunta 26 (Senadora Vanessa Grazziotin). Indagou ao Sr. José Alberto de Freitas Iegas qual é a criptografia utilizada pela Polícia Federal e quem a desenvolveu.

Resposta do Sr. José Alberto de Freitas Iegas: afirmou desconhecer estas informações, comprometendo-se a levantá-las e repassar posteriormente para a Senadora.

Pergunta 27 (Senadora Vanessa Grazziotin). Indagou se há acordo de cooperação entre a Polícia Federal e o FBI.

Resposta do Sr. José Alberto de Freitas Iegas: afirmou não haver acordo com o FBI, mas com a embaixada americana, principalmente na área de capacitação. Indagado, asseverou que não há colaboração da Polícia Federal com eventual atuação de servidores americanos em território nacional. Comentou que, se o fazem, isso ocorre de maneira clandestina.

Pergunta 28 (Senadora Vanessa Grazziotin). O Departamento de Polícia Federal se ressente de eventual falta de coordenação de áreas de inteligência dos diferentes órgãos da administração pública federal exatamente nesse campo da contrainteligência que nós estamos abordando?

Resposta do Sr. José Alberto de Freitas Iegas: esclareceu que há um fluxo de informações e uma integração muito grande, principalmente com a Abin e com os demais órgãos de inteligência das Forças Armadas. Em sua visão, não há falta de troca de informações: pelo contrário, as trocas de informações ocorrem de modo muito adequado.

Pergunta 29 (Senadora Vanessa Grazziotin). Dirigindo-se aos dois convidados, indagou qual o percentual de tecnologia nacional nos equipamentos de segurança cibernética e inteligência de sinais utilizados hoje pela Polícia Federal, e quais informações a este respeito a Anatel possui.

Resposta do Sr. José Alberto de Freitas Iegas: Informou desconhecer o valor percentual, mas informou que, dentre as tecnologias utilizadas pela Polícia Federal, várias são nacionais.

Resposta do Sr. João Batista de Rezende: Afirmou que, no setor de telecomunicações, a maior parte dos equipamentos é estrangeiro, embora existam algumas empresas nacionais. Citou, em relação aos roteadores de Internet, que há apenas quatro ou cinco empresas no mundo que os produzem. Indagado, estimou, de forma geral, em oitenta por cento a predominância de tecnologia não nacional.

Pergunta 30 (Senadora Vanessa Grazziotin). Considerando que, no passado, o Brasil tinha uma presença forte no setor de telecomunicações, mas que, com as privatizações, a situação alterou-se radicalmente, indagou se este quadro torna nosso país mais vulnerável.

Resposta do Sr. João Batista de Rezende: esclareceu que a arquitetura da internet é que propicia as vulnerabilidades, não o fato das empresas serem de capital nacional ou estrangeiro.

Pergunta 31 (Senador Eduardo Suplicy). Após tecer considerações sobre a segurança dos novos sistemas de comunicações em presídios, notícias de ameaça de morte feita ao Governador Geraldo Alckmin e notícias de possíveis ameaças à Copa de 2014, aos jogos e às eleições, indagou se a área de inteligência da Polícia Federal está hoje cooperando com os órgãos de segurança pública do Estado de São Paulo, do Rio de Janeiro e outros.

Resposta do Sr. José Alberto de Freitas Iegas: assegurou que há cooperação entre a área de inteligência da Polícia Federal e as polícias estaduais. Explicou que, como a atividade de inteligência é uma atividade não ostensiva, muitas vezes o resultado de seu trabalho surge como uma prisão ou uma apreensão, realizada normalmente pela polícia

estadual, sendo que o trabalho de inteligência não é divulgado – e, em sua opinião, realmente não deve ser.

Durante a fase das perguntas, o Relator, **Senador Ricardo Ferraço**, deu notícia de confirmação de audiência, na Embaixada da Rússia, para que representantes da CPI, em conjunto com o embaixador, avaliem a possibilidade de teleconferência com o Sr. Snowden. Em relação à notícia, a Senadora Vanessa Grazziotin sugeriu que a oitiva do Sr. Snowden, via teleconferência, fosse feita em conjunto com a Polícia Federal, uma vez que os objetivos da CPI e do inquérito em andamento são os mesmos; e também com a Comissão de Relações Exteriores da Câmara dos Deputados, que possui pedido neste sentido.

Como palavras finais, o **Sr. João Batista de Rezende** frisou que, com o objetivo de aumentar a proteção dos dados estratégicos do Estado brasileiro, é preciso investir em tecnologia. Por outro lado, lembrou que, como atualmente todo o tráfico mundial passa pelas redes e os dados circulam pelo mundo inteiro, um sistema de espionagem eficiente, que não deixe vestígios, não requer a participação de qualquer empresa local. Em relação às investigações em andamento, a Anatel está avançando nas questões técnicas, juntamente com a Polícia Federal. Caso haja nova informação relevante, encaminhará à CPI.

Por sua vez, o Sr. **José Alberto de Freitas Iegas**, em suas palavras finais, ponderou que a principal dificuldade em se apurar se houve um ataque ou uma retirada de informações é exatamente o acesso aos provedores, o acesso aos sistemas centrais das empresas que, em regra, estão nos Estados Unidos. Em sua opinião, se os peritos da Polícia Federal

tivessem acesso às centrais dessas empresas, talvez fosse possível constatar a violação aos sistemas.

Encerrada a fase de perguntas, feitas as colocações finais dos expositores, após agradecer aos convidados, a Presidente da CPI da Espionagem, Senadora Vanessa Grazziotin, encerrou a audiência pública.

9ª Reunião, realizada no dia 22/10/2013 (segurança cibernética)

Objeto: Audiência Pública com os representantes da Cloud Security Alliance Brasil (CSA Brasil), do Comitê Gestor da Internet (CGI) e da Universidade Federal de Pernambuco (UFPE), para discutir o tema segurança cibernética.

No dia 22 de outubro de 2013, a CPI da Espionagem, com base na aprovação do Requerimento nº 19/2013, de autoria do Senador Ricardo Ferraço e conforme entendimento firmado pelos membros da Comissão, promoveu uma audiência pública para ouvir os Srs. Paulo Sérgio Pagliusi, Presidente da Cloud Security Alliance Brasil (CSA Brasil); Rafael Henrique Rodrigues Moreira, Conselheiro do Comitê Gestor da Internet (CGI); e Rodrigo Elia Assad, Professor da Universidade Federal de Pernambuco (UFPE). O objetivo desta audiência pública, conforme expôs a presidente da reunião Senadora Vanessa Grazziotin, foi debater formas de limitar a transferência de dados do Brasil para outros países e a possibilidade de sujeitar empresas estrangeiras à lei brasileira quanto ao acesso de dados de organizações e cidadãos brasileiros.

Sr. Paulo Sérgio Pagliusi

O depoente destacou pontos sobre os atos de espionagem norte-americanos a partir de uma análise técnica de cerca de seis horas de entrevistas concedidas pelo jornalista Edward Snowden. Na sequência, listou ações que considera úteis no combate ao problema.

Os recentes episódios da espionagem americana sobre Brasil e França ganharam projeção internacional e evidenciaram a existência de uma guerra por informação. Esse cenário impõe uma reflexão sobre as estratégicas dos países, pois vai além da discussão técnica de como se faz ou como se protege da espionagem.

Nesse contexto, um dos fatos que ganhou destaque foi a revelação que alguns equipamentos de computação montados nos Estados Unidos já sairiam de fábrica com dispositivos de espionagem instalados. Contudo, estratégias como essa não são inéditas. Em 1992, por exemplo, o sequestro de um representante comercial da empresa de segurança da informação suíça Crypto-AG pelo serviço de contra-inteligência militar iraniano trouxe à tona evidências de que a tecnologia de criptografia vendida pela empresa transmitia, clandestinamente, as chaves criptográficas utilizadas junto com as mensagens cifradas. Na época, dezenas de países faziam uso desse recurso, inclusive as Forças Armadas e o Ministério das Relações Exteriores brasileiros. O fato incentivou a Marinha brasileira a desenvolver seus próprios recursos de criptografia.

Outra revelação que chamou atenção é a de que as ações de espionagem alcançam algoritmos criptográficos que, até bem pouco tempo, eram considerados efetivamente seguros, em particular os protocolos TLS e o SSL. Hoje, já há programas de computador dedicados a quebrar esses tipos de protocolo. Isso leva à reflexão de que a decisão de criptografar deve ser analisada com cuidado. Como, de regra, só se codificam informações consideradas sensíveis, a criptografia acaba servindo como um chamariz a agentes mal intencionados. Uma das formas de reagir a isso é cifrar todos os dados (relevantes ou não), de forma a dificultar o trabalho

dos que tentam quebrar esses códigos. Mas é preciso utilizar chaves mais "fortes" na proteção das informações relevantes.

Prosseguindo sua análise, disse que ainda não se sabe o exato alcance do poderio da Agência de Segurança Nacional (*National Security Agency* – NSA) americana. Sabe-se apenas que eles estão à frente nas pesquisas sobre criptografia e que lidam com supercomputadores pelo menos dez anos mais avançados do que as tecnologias hoje conhecidas. As instalações da NSA na cidade de Utah contam com um *data center* avaliado em US$ 2 bilhões. Ele é capaz de armazenar um iotabyte, medida que comporta toda a informação produzida pelo ser humano nos últimos 500 anos.

Mas o cenário de espionagem mundial não é protagonizado somente pela NSA. O monitoramento da rede é uma das ações dos *Five Eyes*, termo que designa o agrupamento das agências de inteligência de Austrália, Canadá, Estados Unidos, Reino Unido e Nova Zelândia. Essas agências são ligadas por um tratado que autoriza o compartilhamento, entre elas, de informações secretas. O acordo original foi firmado em 1946 entre Estados Unidos e Grã-Bretanha, no contexto da Segunda Guerra Mundial. Os primeiros países monitorados foram os da extinta União Soviética. Os outros três países foram agregados ao acordo por uma razão técnica: ampliar o nível de vigilância sobre os demais países. Dada a dispersão geográfica dos cinco países, juntos eles conseguem monitorar todos os satélites estacionários no globo terrestre.

Os *Five Eyes* são capazes de monitorar, por exemplo, chamadas telefônicas, de fax, transmissões de internet (fixa ou móvel) e de rádio em todo o mundo. Lidam, também, com inteligência de comunicações, que permite saber quem se comunica com quem, quando e

como. Fazem, ainda, análise de tráfego (muito utilizada na área militar) que permite observar um volume de fluxo de informações não usual partindo de determinado órgão. A receptação de dados compreende inclusive os cabos submarinos, pois essas Agências dispõem de uma tecnologia que permite a interceptação desses cabos mesmo em alto mar (*interceptation of vessels*). É um fato que surpreende, pois se pensava que isso não mais seria possível com os cabos atuais, feitos de fibra ótica.

Encerrando sua contribuição, o depoente apresentou algumas ações que considera importantes no combate aos atos de espionagem contra o Brasil. São elas:

a) A aprovação do projeto de lei do Marco Civil da Internet, que irá regulamentar o uso da rede sob os aspectos jurídico e civil, bem como os direitos e responsabilidades dos usuários;

b) O desenvolvimento de um sistema de correio eletrônico brasileiro para uso da Administração Pública e, futuramente, da população. A ferramenta pode assegurar a privacidade das comunicações e, acima disso, a liberdade de expressão, essencial para a vida em democracia. O Brasil conta com gente capacitada a desenvolver esse projeto.

c) A criação de um sistema nacional de criptografia de *e-mails*, desejo expresso pela Presidenta Dilma é que já está sendo desenvolvido pelo Serviço Federal de Processamento de Dados (Serpro). Conforme dito pelo presidente do Serviço, o objetivo é livrar o Governo da espionagem estrangeira. As chaves de criptografia devem ser utilizadas para cifrar não somente informação governamental e de empresas, mas também as comunicações pessoais, por meio das quais informações importantes podem ser interceptadas clandestinamente.

d) O investimento em satélites e cabos submarinos de comunicação próprios, conforme aponta a Estratégia Nacional de Defesa. Hoje, 90% do tráfego de informações que sai do Brasil passa pelo território norte-americano, ainda que se destine a outras localidades.

e) A constituição de um comando cibernético único para tratar de questões de segurança da informação. Conforme justificou, as divisões das Forças Armadas têm estratégias, táticas e doutrinas próprias para os domínios terrestre, marítimo e aéreo. De forma similar, a Agência Espacial Brasileira cuida da área de domínio espacial. Mas falta ao Brasil um órgão com expertise em domínio cibernético, que envolve técnicas e conhecimentos próprios. Uma batalha cibernética, diferente das terrestres ou marítimas, ocorre em questão de horas.

f) A aproximação do trabalho dos órgãos governamentais com as pesquisas desenvolvidas nas universidades, o que pode reforçar a capacidade do País em proteger o tráfego de informações.

g) A inclusão da discussão sobre segurança cibernética nos currículos escolares. O surgimento de bons analistas de segurança depende da formação crítica sobre o assunto. O surgimento de mais especialistas nesta área ajudará o ambiente corporativo a aprimorar suas ferramentas de segurança cibernética.

h) O investimento em canais para o recebimento de denúncias de espionagem, aproveitando o reconhecimento do Brasil como um país aberto à permanência dos denunciantes. O próprio jornalista Glenn Greenwald declarou que, no território britânico, não sentiria a mesma liberdade de fazer as revelações que fez no Brasil. Isso pode ser visto de maneira positiva por potenciais denunciantes, que observam atentamente o que acontecerá com Snowden.

Sr. Rafael Henrique Rodrigues Moreira

Inicialmente, o depoente apresentou o Comitê Gestor da Internet (CGI). Criado por decreto presidencial em 2003 e coordenado pelo Ministério da Ciência, Tecnologia e Inovação (MCT), esse Comitê é composto por 21 membros advindos do governo, do terceiro setor, da iniciativa privada e da comunidade acadêmica e científica, constituindo uma visão pluralista que é elogiada em todo o mundo.

Na sequência, apresentou informações sobre o contexto em que se desenvolvem as discussões sobre segurança cibernética.

As novas tecnologias tornaram o uso de recursos de informática e comunicação mais baratos e acessíveis. E o Brasil se beneficia disso. Enquanto a economia brasileira cresce a uma média de 0,9 a 1% ao ano, esse setor, tomado isoladamente, cresce a uma média de 15 a 18% ao ano. Evidência disso é que o Brasil é, hoje, o terceiro maior mercado mundial de tecnologia da informação e de comunicação.

Mundialmente, cria-se, a cada dois anos, a mesma quantidade de dados desenvolvida do início da civilização até 2003. A cada minuto são trocados 168 milhões de e-mails, postados 1500 páginas de blogs e criados 60 novos blogs.

Contudo, à medida que a sociedade se torna mais conectada, cresce a necessidade de discutir e implementar ações nas áreas de segurança da informação, proteção de dados pessoais, direitos civis na internet, propriedade intelectual e direitos autorais.

A segurança de um ambiente digital depende do controle da rede de comunicações e do tráfego de informações. Esse controle, contudo,

passou a ser relativo com o advento da computação em nuvem, que hospeda informações em *data centers* espalhados pelo mundo.

Além disso, a topologia da rede mundial de computadores foi constituída para concentrar o tráfego de dados nos Estados Unidos. Isso se apresenta como uma dificuldade a mais para o tratamento seguro das informações que trafegam pela internet.

Vários exemplos mostram como o alto grau de conectividade pode causar prejuízos sociais e traduzem a responsabilidade governamental em salvaguardar informações estratégicas e as relativas aos cidadãos.

Primeiro, é possível que um *cracker* interrompa uma rede elétrica, pois hoje os relés não são mecânicos, e sim digitais, conectados em rede. O setor energético é, inclusive, um daqueles considerados estratégicos para a espionagem.

Segundo, o Datasus é um banco de dados que reúne informações sobre a saúde de milhões de usuários do Sistema Único de Saúde e que tem muito valor para determinados ramos do mercado.

E, terceiro – tratado em outro momento da exposição –, o Brasil chegou a ser o maior distribuidor de *spams* da América Latina. Dos principais *malwares*, os mais disponibilizados eram do tipo *worms*, que copiam senhas para serem utilizadas em crimes cibernéticos. Atualmente, com o gerenciamento da Porta 25, por onde a maioria dessas ameaças trafegava, esse fato está mudando.

Diante das ameaças a que estão expostos, os cidadãos estão interessados em saber como o governo irá manipular e armazenar dados e informações sensíveis, de forma que eles fiquem protegidos do acesso indevido por lobistas ou agentes de governos estrangeiros. Essa é a importância de definir um marco regulatório que reafirme o investimento

em pesquisa, desenvolvimento e inovação na área de segurança da informação.

Falando especificamente dos atos de espionagem, o depoente esclareceu que os Estados Unidos não são o único país que faz espionagem eletrônica. Porém, dado seu desenvolvimento tecnológico, é ele quem define os padrões e tecnologias que serão utilizados na espionagem. Nesse sentido, o grande volume de informações que hoje circulam pela rede fez com que se desenvolvessem sofisticadas ferramentas de manipulação e análise de dados. Uma vez de posse dos dados – o que ocorre quando eles trafegam em rede ou são armazenados nos *data centers* de empresas americanas – a NSA utiliza essas ferramentas para interpretar e classificar as informações de acordo com seu grau de relevância estratégica. No caso do dado criptografado, esse é levado a servidores que, utilizando-se de computação de alto desempenho, tentam quebrar as chaves que os codificaram.

A mobilidade também favorece a espionagem. O rastreamento de celulares permite, *a priori*, acesso à teia de relações de quem usa o dispositivo. Contudo, caso o dispositivo não conte com criptografia ou caso essa tenha seu chaveamento "quebrado", é possível ter acesso também ao próprio conteúdo das ligações. Já o protocolo 3G dos dispositivos móveis é aberto e facilita o rastreamento de telefones tanto para fins lícitos (como a resolução de crimes), como para fins ilícitos (como espionagem industrial, tecnológica ou de estratégias governamentais).

Adicione a isso o fato de que, por lei, o governo norte-americano pode ter acesso aos dados dos serviços de e-mail e de hospedagem sediados em seu território. Na interpretação brasileira, expressa na abertura da Assembleia-Geral das Nações Unidas, esse poder

deveria dirigir-se somente ao cidadão americano e não poderia ser aplicado a cidadãos estrangeiros.

Por fim, lembrou que o mercado de crimes cibernéticos, conhecido como *darknet*, movimenta muito dinheiro. Há, inclusive, listas de preços para o repasse de informações adquiridas ilegalmente.

Apresentado esse cenário, o expositor defendeu que o Brasil encontra-se diante de uma oportunidade favorável ao investimento, nas universidades, em atividades de pesquisa, desenvolvimento e inovação na área de segurança cibernética, bem como na criação de um complexo industrial voltado especificamente para as "tecnologias de fronteira".

Uma das perspectivas para isso é um programa de defesa e segurança cibernética que está sendo desenvolvido pelos ministérios da Ciência, Tecnologia e Inovação e da Defesa.

A título de exemplo, o Pentágono americano investe em empresas localizadas no Vale do Silício para que eles criem novas tecnologias que serão utilizadas, futuramente, pelo governo americano.

O Brasil não dispõe, ainda, de produtos de criptografia prontos. É isso que levou a Petrobrás a declarar que não havia empresas brasileiras aptas a oferecer soluções de criptografia para a petroleira. Por outro lado, um estudo de mercado revelou a existência de 87 empresas nacionais na área de segurança da informação e criptografia. Com estímulo governamental, essas empresas teriam condições de desenvolver soluções nas áreas de segurança e defesa cibernética.

Paralelamente à questão da criptografia, o País poderá desenvolver um modelo de certificação e homologação de equipamentos de informática, pois não pode continuar a adquirir de multinacionais tecnologias que não sabe ao certo como foram desenvolvidas.

Passando à etapa final de sua exposição, defendeu a aprovação do projeto de lei do Marco Civil da Internet como forma de garantir a proteção de dados pessoais de brasileiros quando colocados em rede, ainda que o armazenamento ocorra no exterior. A União Europeia conta, desde 1995, com uma lei desse tipo. Sobre o projeto do Marco, em tramitação na Câmara dos Deputados, destacou alguns pontos que considera sensíveis:

a) Permanência da neutralidade de rede, fundamental para equilibrar interesses e manter a isonomia entre os detentores da infraestrutura e os geradores ou provedores de aplicações;

b) Armazenamento obrigatório de determinados tipos de dados no País. Na Coreia do Sul, por exemplo, dados financeiros devem obrigatoriamente ser armazenados em *data centers* localizados no país;

c) Regras sobre a guarda de registros de atividades na rede (*logs*), importantes para investigações policiais e forenses;

d) Confinamento de tráfego, que é um assunto delicado e que merece ser mais discutido. Por ele, criam-se regras para que o tráfego de informações entre dois dispositivos que se utilizam de IP brasileiro ocorra via redes brasileiras.

e) Direitos autorais na rede, assunto que, ao seu ver, pode ser tratado com mais propriedade no projeto da reforma da Lei de Direitos Autorais.

Sr. Rodrigo Elia Assad

O depoente – que integra um grupo de trabalho colaborativo focado em criar soluções para empresas de tecnologia de informação, o Assert Lab – apresentou questões relevantes sobre a espionagem americana.

Preliminarmente, lembrou que as grandes empresas americanas oferecem muito dinheiro para a contratação de gente qualificada de outros países, perpetuando seu poder sobre as mais recentes inovações tecnológicas. Assim, o Brasil deve buscar estratégias para preservar as 87 empresas nacionais que lidam com segurança da informação e criptografia.

O primeiro ponto apresentado é que, se antes não se prestava tanta atenção aos dados gerados por governo, empresas e usuários, hoje, diante do crescimento exponencial do volume de dados produzidos anualmente, muito se discute sobre a responsabilidade corporativa sobre essas informações.

Nessa seara, as perguntas que devem ser respondidas são:

a) Que dados são gerenciados?

b) Quais deles são considerados relevantes?

c) Como esses dados são manipulados?

d) Onde eles estão salvos?

Ocorre que, atualmente, a quantidade de dados produzidos é significativamente maior do que a capacidade de armazenamento das organizações em geral. Assim, a oferta de estocagem gratuita de dados tornou-se um negócio extremamente atrativo. Mas isso acaba criando um problema que precede até mesmo a questão da privacidade: de quem acaba sendo a propriedade desses dados?

A segunda questão levantada é que, hoje, computação significa conexão. Os novos aplicativos são desenvolvidos para operarem em conexão, trocando informações. Isso torna desafiante a tarefa de conseguir rastrear, do início ao fim, a circulação das informações.

Afora isso, é preciso definir uma estratégia para identificar precisamente o que se deseja monitorar. Essa tarefa demanda tempo, investimento e pesquisa. No caso americano, a necessidade de defesa fomentou a desenvolvimento tecnológico. O Vale do Silício, por exemplo, foi criado no final da Primeira Guerra Mundial. Da mesma forma, a Intel iniciou suas atividades fabricando radares.

Prosseguindo sua exposição, o Sr. Rodrigo apresentou alguns pontos de reflexão que o episódio da espionagem ao Brasil deixa:

a) A convergência dos pontos de conexão para o território norte-americano partiu de uma decisão estratégica. O Brasil precisa decidir como lidará com a gestão de seus pontos de tráfego de dados. É possível, por exemplo, fazer o monitoramento na base de onde os dados saem ou na extremidade dos pontos de tráfego. Basta criar um centro de processamento de dados no ponto onde se quer analisar as informações. Mas lembrou serem essas mudanças onerosas e difíceis.

b) Existe, hoje, um mercado das vulnerabilidades, por meio do qual governos e empresas compram de *hackers* informações sobre falhas de programação de outras empresas ou instituições não com o intuito de corrigi-las, mas para manter essas informações em segredo e utilizá-las estrategicamente. Conforme os analistas de *malwares*, o setor energético está em evidência nesse mercado.

c) A mobilidade é outro problema a ser enfrentado. A partir da captura do sinal, por antenas, é possível localizar fisicamente um telefone celular. Ocorre que a captura do sinal tem sido feita até mesmo por embaixadas, sob a justificativa de que o sinal é distribuído abertamente por via aérea e, portanto, a interceptação deles não significa violação.

Apresentados contexto e principais problemas a serem enfrentados, o depoente finalizou sua exposição sugerindo a adoção, pelo Brasil, das seguintes providências:

a) Aprovação do Marco Civil da Internet;

b) Utilização de uma plataforma de computação em nuvem nacional, tecnologia já disponível;

c) Desenvolvimento de um comando para monitoramento e rastreamento de informações no Brasil, incluindo um sistema de classificação e armazenamento seguro de informações relevantes;

d) Definição de uma estratégia para o uso de criptografia e de algoritmos nas atividades de Estado. O Brasil deve desenvolver seu próprio sistema para cifrar informações, eliminando o risco de utilizar tecnologias que repassam chaves de segurança a terceiros.

Encerrada a primeira parte da Audiência Pública, a Senadora Vanessa Grazziotin questionou os convidados sobre pontos específicos.

Pergunta 1 (Senadora Vanessa Grazziotin). Solicitou-se a análise da vulnerabilidade dos sistemas de segurança cibernética que o Brasil utiliza, numa escala comparativa, a países com nível de desenvolvimento compatível com o brasileiro.

Resposta do Sr. Paulo Sério Pagliusi: Explicou que só agora o Brasil acordou para esse tipo de problema. O próprio Parlamento Europeu já havia levantado essa questão com relação ao serviço de inteligência norte-americano. Dizia-se que espionagem corporativa era uma teoria da conspiração, mas hoje se sabe que é uma realidade e que seu início remonta à Guerra Fria. Com o fim dela, porém, o esforço de

espionagem foi direcionado para as áreas econômica e industrial. O Brasil precisa levar mais a sério esse assunto. Numa escala de 0 a 10, sendo que 0 representa vulnerabilidade total, o País ganharia nota entre 3 e 4. Para avançar nesta escala, é preciso ter consciência da situação e aprender a combatê-la. Acredita que a sociedade está consciente do problema, pois as pessoas passaram a perceber que, mais do que usuários de redes sociais, fazem parte de um contexto mercadológico. Isso fica evidente nos termos de acordo de quem aceita fazer parte de uma rede social como o Facebook: esses termos dizem que o serviço é o dono da informação e pode excluí-la a qualquer momento.

Sr. Rafael Henrique Rodrigues Moreira: O Brasil é especialmente vulnerável em razão do tamanho de sua economia, maior do que a de países do mesmo nível de desenvolvimento. Há muito o que avançar nesse assunto. Há apenas um ano, o Brasil era o principal distribuidor de *spams* do mundo. Isso porque, para o envio dessas mensagens, os *crackers* utilizavam-se da porta 25, que estava sob gestão das operadoras de telecomunicações. A partir de um trabalho conjunto do CGI, Anatel e dessas operadoras, foi possível melhorar o gerenciamento dessa porta e diminuir o número de *spams* que saem do Brasil. É tempo de que o Brasil pense estrategicamente não só no controle de suas comunicações, como também nas saídas dessa rede. Os órgãos, a exemplo do Exército, precisam estar capacitados para trabalhar suas próprias redes, efetivando o projeto de infovia, sob responsabilidade do Ministério do Planejamento, Orçamento e Gestão (MPOG).

Sr. Rodrigo Elia Assad: No Brasil, há setores que investem em segurança da informação. Os bancos são um exemplo. É preciso olhar

para os segmentos mais estratégicos e promover um trabalho mais efetivo sobre eles.

Pergunta 2 (Senadora Vanessa Grazziotin). Quanto à auditoria e homologação de equipamentos, questionou-se em quanto é aumentada a vulnerabilidade a ataques virtuais devido à falta desses serviços e se haveria, no país, alguma entidade que cuidasse de tais serviços em áreas mais sensíveis, como defesa nacional.

Resposta do Sr. Paulo Sério Pagliusi: O Brasil conta com instituições dedicadas a homologação, a exemplo da Isaca (*Information Systems Audit and Control Association*), instituição com mais de 40 anos, e da *Cloud Security Alliance Brazil*, entidade que o expositor preside. São instituições sem fins lucrativos que cuidam da segurança informacional e da governança da tecnologia da informação. A Isaca, em particular, confere uma certificação chamada Cisa (*Certified Information Systems Auditor*), que é homologada e fomentada pelo próprio Gabinete de Segurança Institucional da Presidência da República. O Departamento de Segurança da Informação e Comunicações da Presidência da República recomenda que todo servidor público que trabalha com segurança da informação detenha esse tipo de certificação.

Sr. Rafael Henrique Rodrigues Moreira: Falando sobre como garantir que o Governo tenha acesso a equipamentos e programas realmente seguros, deu o exemplo dos Estados Unidos e da Austrália. Esses países instituíram um sistema de requisitos de segurança que deve ser seguido por empresas que tem interesse em vender equipamentos ou softwares para o Governo. Da mesma forma, o Governo brasileiro pode estabelecer regras de certificação e homologação para a aquisição de

equipamentos e programas que serão utilizados em áreas estratégicas. Uma proposta nesse sentido já é desenvolvida pelo Ministério da Ciência, Tecnologia e Inovação (MCTI). Por fim, disse que uma rede mais segura e com controle governamental depende de um conjunto de padrões, técnicas e analistas que experiência.

Sr. Rodrigo Elia Assad: Complementou as respostas anteriores dizendo que o Centro Tecnológico do Exército (CTEx), em parceria com o MCTI desenvolve um selo de nacional certificação.

Pergunta 3 (Senadora Vanessa Grazziotin). O Google ofereceu cobertura de internet banda larga a áreas do Brasil que ainda não dispõem dessa facilidade. O serviço será oferecido por meio de balões que emitem o sinal de internet. Assim, perguntou qual seria o risco incorrido pelo Brasil ao autorizar a oferta do provedor.

Sr. Rafael Henrique Rodrigues Moreira: Para que o governo tenha mais controle, é preciso homologar e certificar os equipamentos que serão utilizados pelo Google, opinião com a qual o Sr. Rodrigo Elia Assad concordou.

Pergunta 4 (Senadora Vanessa Grazziotin). Questionou-se qual seria o efetivo grau de controle da rede de que o Brasil dispõe, especialmente para a proteção das áreas governamentais mais sensíveis, e de que forma as antenas instaladas em embaixadas sediadas no Brasil poderiam ser utilizadas para a captura irregular de dados de internet e de telecomunicações.

Resposta do Sr. Paulo Sério Pagliusi: O Brasil ainda não goza de um patamar elevado quanto ao controle de rede. Porém, os

acontecimentos recentes levaram o País a ser mais consciente do problema. A partir de um trabalho de treinamento promovido em Brasília, disse ter constatado que os gestores públicos têm pouco conhecimento sobre segurança cibernética. Ressaltou a importância de promover campanhas de conscientização para criar uma cultura com relação a isso.

Sr. Rodrigo Elia Assad: O controle de redes, além de uma questão de segurança cibernética, é uma estratégia de defesa. O único país que desenvolveu uma estratégia efetiva de defesa cibernética foi a China, que não depende da conexão externa para manter suas redes em funcionamento. O Brasil precisa desenvolver a capacidade de lidar com grandes repositórios de dados (*big datas*), para acessar, com facilidade, informações importantes. Deve-se investir, também, no aspecto educacional para que as pessoas aprendam a ser seletivas sobre o conteúdo que disseminam nas redes.

Pergunta 5 (Senadora Vanessa Grazziotin). Indagou-se sobre a possibilidade de detectar quais são as informações que estão sendo acessadas de forma ilegal.

Sr. Rodrigo Elia Assad: A princípio, todos os dados salvos em grandes provedores internacionais podem ser acessados, porque passam a pertencer a esses serviços. Foi o que motivou o governo francês a não autorizar a venda de um sítio nacional de vídeos para uma empresa americana, considerando o quanto as informações contidas ali – vídeos, fotos, contatos e informações pessoais voluntariamente publicados – são estratégicas. Com relação ao controle de tráfego, disse que há técnicas desenvolvidas que permitem predizer se uma determinada rede está sendo interceptada. Os americanos, por exemplo, conseguiram detectar que uma

marca chinesa estava inserindo *backdoors* nos equipamentos que produziam. Reforçou que o Brasil precisa criar uma indústria nacional que abrigue empresas de classe mundial nas áreas que o País tem interesse em desenvolver, dizendo que o País tem competência para desenvolver suas próprias ferramentas de análise e defesa.

Resposta do Sr. Paulo Sério Pagliusi: Todo crime cibernético deixa evidências, pois acaba gerando registros de atividades. Por meio desse princípio, é possível ter um monitoramento contínuo do ambiente de rede. As corporações, de forma geral, precisam agir proativamente ao utilizar preventivamente técnicas e métodos já desenvolvidos para o monitoramento contínuo da informação e a análise do fluxo de dados na rede. Isso lhes permitirá ter ampla consciência situacional das ameaças cibernéticas a que estão expostas e de como se defender delas. Declarou, ainda, que o grupo colaborativo que integra desenvolveu o primeiro sistema de gerenciamento de segurança da informação nacional, trabalho que já foi apresentado ao CGI.

11ª Reunião, realizada no dia 5/11/2013 (telefonia móvel: TIM, Claro, Vivo e Oi)

Objeto: Audiência Pública com os representantes das Empresas de Telefonia Móvel: TIM, Claro, Vivo e Oi.

No dia 5 de novembro de 2013, a CPI da Espionagem,[78] mediante Requerimento nº 20/2013, de autoria do Senador Ricardo Ferraço, ouviu os Srs. Nelson de Sá, Diretor da TIM; Ivan Campagnolli, Diretor da Claro S.A.; S.A.; Ari Sergio Perri Falarini, Diretor de Operações da Telefônica Vivo; e Marcos Augusto Mesquita Coelho, Diretor de Relações Institucionais da Oi.

O objetivo da audiência pública, conforme anotado no Requerimento, foi discutir e prestar esclarecimentos sobre as denúncias feitas pelo jornalista Glenn Greenwald. O conteúdo das informações ofertadas por Glenn sugere que empresas de telecomunicações, com atuação no Brasil, mantém acordo de envio de dados de comunicações de cidadãos brasileiros para companhia estrangeira sediada nos EUA, a qual, por sua vez, repassa essas informações à Agência de Segurança Nacional americana (NSA).

A Senadora Vanessa Grazziotin, antes de passar a palavra aos convidados, comunicou a resposta dada pela Anatel a requerimento

---

[78] Criada conforme o Requerimento nº 811, de julho de 2013-SF, de autoria da Senadora Vanessa Grazziotin (PCdoB/AM) e outros Senadores, para, no prazo de cento e oitenta dias, investigar "a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal",

formulado pela CPI. O requerimento buscava saber quais embaixadas possuem estações de comunicação a rádio no Brasil e em qual número. A Agência respondeu que quatro embaixadas possuem estações de rádio no País e as quantidades de cada uma são: o Chile possui duas estações portáteis; a França, cinco; a Romênia, vinte; e os EUA, 841 estações de comunicação, dentre fixas e móveis, operando em todo o território nacional. A Presidente da CPI, sem fazer qualquer julgamento prévio, chamou a atenção para o grande número de estações sob poder dos EUA.

Feito o comunicado, os trabalhos expositivos foram abertos pelo Sr. Nelson de Sá, Diretor da TIM. Para ele, esta é uma boa oportunidade para a companhia mostrar os trabalhos que vem sendo desenvolvidos em seu interior, no que diz respeito à segurança de dados de usuários.

Baseada na transparência, a empresa TIM respeita as determinações constitucionais e legais quanto à inviolabilidade de dados. Conforme o palestrante, à Constituição Federal (art. 5, XII) e à Lei de Interceptação (Lei n. 9.296/1995) não cabem interpretações, isto é, devem ser seguidas à risca. Em outras palavras, espionagem é crime, é interceptação não autorizada.

Explicando o papel desempenhado pelas empresas de Telecom, afirmou que elas são provedores de acesso à internet, cuja responsabilidade está na construção das vias de tráfego de dados e de voz na rede. Num outro plano, estão os provedores de aplicação, que são as empresas ofertantes de serviços que utilizam de tais vias construídas pelos provedores de acesso.

Asseverou que a empresa não mantém qualquer tipo de parceria com órgãos estrangeiros para a realização de escuta telefônica e

acesso a dados privados de seus clientes. A TIM preserva e resguarda integralmente as informações e o sigilo de seus usuários, respeitando os casos em que a legislação especifica as circunstâncias de quebra de sigilo.

Prova disso é o armazenamento de todas as informações dos usuários em *datacenters* localizados no Brasil, sobre os quais recaem rígidos controles de segurança. Estando entre os maiores da América Latina, esses *datacenters* corroboram a atitude da companhia em expandir os meios de segurança e proteção de dados. Disse que ampliação dos investimentos no setor foi da ordem de oitenta por cento.

No que diz respeito aos sistemas de operação de suporte, informou que eles possuem acesso restrito, protegido e rastreáveis. Na mesma linha, os sistemas de gestão de dados pessoais, assim como a interceptação legal, são passíveis de auditoria e fiscalização pela Anatel.

Sendo uma companhia de vanguarda tecnológica, a TIM dispõe de um Centro de Segurança Operacional – Security Operation Center – (SOC), situado em São Paulo, que é referência tecnológica para o mercado. Paralelamente, visando ao combate e ao tratamento de incidentes de internet, existe um time próprio de funcionários que garante a segurança, o *Computer Security Incident Response Team* (CSIRT). E há, também, um segundo grupo que faz testes de invasão, que realiza, preventivamente, busca por fragilidades do sistema.

Em síntese, explicou que os dados são protegidos do mundo externo por três plataformas. A primeira é a plataforma de infraestrutura de segurança, a qual controla os acessos à rede, efetuando a proteção primária do complexo. A segunda é a de monitoração, que identifica e rastreia os acessos indevidos à rede. A última é a plataforma evolutiva, que

correlaciona os eventos e analisa os *logs* para contactar incidentes. Se houver algum incidente, este vai para a apuração técnica do CSIRT.

Portanto, a TIM detém os melhores produtos para detecção e combate a ataques, trabalha e investe para ter segurança operacional e submete-se, fielmente, às leis que regulam o tema.

Em seguida, o Sr. Ivan Campagnolli falou em nome da operadora Claro. Disse que a empresa atua no ramo da telefonia móvel, utilizando-se da estrutura de *backbone* (traduzido do inglês, significa "espinha dorsal") da Embratel.

Enfatizou que não há dúvida de como é regulado o assunto de proteção e segurança de dados: há uma legislação clara e aplicável. Mesmo assim, é importante compreender os atores envolvidos e suas características.

Dessa forma, trouxe alguns dados sobre a companhia telefônica que representa. A Claro tem cobertura nacional, ligando todo o território brasileiro por meio de fibra ótica. Há, em alguns lugares – como é o caso da linha que parte de Manaus – interconexão com fibras óticas de outras empresas, a exemplo da que se estabelece com a Oi na cidade amazonense citada. Além da conexão em território brasileiro, existem cabos que vão para a Europa e para os EUA.

Atualmente, a empresa possui um cabo em consórcio com a Embratel, denominado "América 2", e outro cuja propriedade é integralmente sua, o AMX-1, ainda em construção, que está previsto para entregar no primeiro trimestre de 2014. Para suportar a demanda, a Claro tem capacidade comprada em cabos de outras operadoras, com as quais são estabelecidas regras de confidencialidade de dados e de voz.

Diante das necessidades, cada vez mais crescentes, de se garantir a segurança dos dados de clientes, a companhia desenvolveu, e mantém em conjunto com a Embratel, estrutura de segurança que abrange: o controle físico (quem acessa, com qual perfil e o que está autorizado a fazer); a responsabilidade por quem executará as cópias de segurança; quais atualizações de hardware e software devem ser feitas; a proteção contra ataques; a resposta a incidentes de segurança; e a utilização de antivírus. Essas medidas visam garantir que todos os dados sejam invioláveis.

A respeito dos satélites que prestam serviços para a empresa, a cargo da Star One,[79] disse que tanto o controle de sua posição como de seu caminho orbital são feitos no Brasil. Dessa maneira, há absoluta segurança do sigilo de dados.

Ademais, as interconexões necessárias são feitas com operadoras legalmente constituídas, mediante contratos balizados pelo sigilo e pela confidencialidade esperada pelos usuários e pela sociedade em geral.

Confirmando as ideias apresentadas pelos expositores que o antecederam, o Sr. Ari Falarini, representante da Vivo, reiterou o campo sólido em que são celebrados os contratos de conexão e interconexão das empresas. Seja nacionalmente, seja em âmbito internacional, esses acordos fixam-se na responsabilidade do sigilo e da confidencialidade da informação trespassada entre usuários.

---

[79] Empresa da Embratel responsável pela operação e pelo controle das estações de comunicação, abrangendo todo o território nacional e América do Sul nas bandas C, X, Ku e Ka.

À semelhança das concorrentes congêneres, a Vivo, que está presente em 25 países e presta serviços a mais de 300 milhões de clientes, possui capacidade de gerenciamento e segurança de rede de abrangência nacional. Há três centros de operação para a rede móvel, localizados em São Paulo, Brasília e Belo Horizonte. Essa estrutura é responsável por monitorar e acompanhar 76 milhões de telefones móveis (que totaliza mais de dezenove bilhões de minutos falados e seis bilhões de SMS enviados por mês), quatorze mil sites e 29 mil estações móveis.

A Vivo opera a telefonia fixa apenas no Estado de São Paulo, alcançando 42 milhões de habitantes, 1.800 centros de telefonia, onze milhões de terminais telefônicos e quase 4 milhões de acessos a banda larga. Para este ramo de serviço, existem dois centros de gerência e um *datacenter* específico na grande São Paulo.

Para garantir o desenvolvimento da rede, que já conta com 78.480 quilômetros de fibra ótica e 235 mil quilômetros de fios de cobre, a empresa tem investindo maciçamente na área, a partir de previsões quadrienais. No quadriênio 2007-2010, o investimento foi de dezesseis bilhões de reais, enquanto no lapso de 2011-2014, foi de 24 bilhões.

Disse, ainda, que está sendo construído um backbone para uso próprio e outro que pode ser comutado com as demais operadoras. Isso ajudará no aumento da capacidade nacional e internacional. Esta, aliás, é coberta pelo *backbone* nacional, o qual permite fazer o direcionamento e a distribuição do tráfego, de acordo com as necessidades de cada operação.

Informou que, dentre os trinta gigabytes destinados à Europa e aos EUA, 229 deles vão para território americano. Dessa forma, é natural que haja acordos com operadoras europeias e americanas, a fim de dar

conta da execução de tamanha quantidade de serviços. Mas isso não é feito sem a observância dos critérios de segurança já expendidos anteriormente.

Por fim, informou à CPI a respeito da inauguração do *datacenter* da empresa, situado em Tamboré, região metropolitana de São Paulo, que já obteve certificação em três aspectos: quanto ao padrão do projeto; quanto à rigidez de padrões de disponibilidade de segurança; e quanto aos requisitos ecológicos.

Fechando as apresentações iniciais dos convidados, o representante da Oi, Sr. Marcos Mesquita, disse que a empresa é a pioneira na prestação de serviços convergentes no País (serviços de transmissão de voz, local e de longa distância, telefonia móvel, acesso à banda larga e TV por assinatura).

Nessa esteira, a dimensão de seus negócios denota a importância da companhia para o País. Fundada em 1998, a Oi já contabiliza investimentos na escala de 102 bilhões de reais. Está presente em 5.565 Municípios, isto é, faz-se atuante em todo o território nacional; provê 74,3 milhões de acesso aos mais variados serviços; e cria 160 mil empregos diretos. Em resposta a essas iniciativas, 120 bilhões de reais em tributos foram recolhidos pelos cofres públicos, desde sua fundação.

A empresa conta com mais de 178 mil quilômetros de fibra ótica, albergando todo o território nacional, e oferecendo, a mais de 4.800 municípios, serviços de telefonia móvel. Ao lado disso, a Oi detém e disponibiliza a maior rede pública de Wi-Fi no País.

Sobre o tema específico tratado pela CPI nesta audiência, o Sr. Marques salientou, inicialmente, que há uma preocupação crescente com a segurança de dados. Isso se mostra evidente por três razões: 1) aumento das ameaças produzidas virtualmente, seja por dados, seja por voz; 2)

incremento no interesse por fraudes e espionagens; e 3) ampliação das expectativas dos clientes quanto à segurança.

Essas três razões evidenciam que é preciso estar constantemente atento para aspectos de vulnerabilidade, que sempre existirão e sempre terão de ser monitorados – leia-se: é necessário que haja trabalho frequente de prevenção e defesa. Nessa linha de raciocínio, é fundamental que as leis acompanhem as mudanças tecnológicas.

Fez, na sequência, uma breve síntese do conteúdo das denúncias em relação à espionagem conduzida pela agência americana NSA. Elas denotam que: a) as redes de Telecom são vulneráveis; b) os contratos de interconexão possibilitam o acesso a dados e comunicações, com origem no Brasil, por governos ou instituições de segurança estrangeiras; c) há "colaboracionismo" de empresas de Telecom brasileiras com representantes de países estrangeiros.

Para o representante da Oi, essas denúncias são infundadas e não há como comprová-las. Isso por que: a) a rede de transporte de dados da Oi processa pacotes IP[80] e é completamente transparente às camadas superiores, onde estão contidas as informações; b) a rede de transporte de dados da Oi é um meio que encaminha as solicitações de uma determinada origem para um determinado destino, sem que elas sejam armazenadas; c) os equipamentos usados pela rede de transporte de dados possuem rígido sistema de controle e de acesso; d) a Oi não armazena informações de correspondências entre os endereços de IP e seus respectivos usuários.

Assim, a responsabilidade de responder ou não uma determinada requisição de um usuário de origem e/ou criptografar os dados

---

[80] IP, do inglês, *Internet Protocol*, é a identificação de um dispositivo, por exemplo, de um computador.

enviados é dos próprios usuários. A rede, portanto, é um meio de transporte de dados e de voz, conforme o caso. E, por isso, a proteção à inviolabilidade das comunicações dos clientes é o maior ativo da empresa.

No que diz respeito aos contratos de interconexão, asseverou que a companhia tem contratos com quase todas as importantes empresas do mundo. A propósito desse tema, disse que a Anatel, a pedido desta CPI, está finalizando trabalho de auditagem desses contratos, o qual detalhará a estrutura e as cláusulas que os regem, a fim de averiguar sua adequação aos parâmetros internacionais.

Sublinhou que a Oi presta seus serviços com base numa política de segurança de dados, conforme a qual, todo acesso não autorizado é bloqueado, identificado e rastreável. Mas isso é suficiente para nos tranquilizar? Disse que não, mas qualquer tentativa de espionagem será identificada, mesmo que *a posteriori*.

Destacou, também, que, quando começaram os debates acerca da espionagem americana, arguíu-se existir vazio legislativo sobre o tema aqui no Brasil. No entanto, o palestrante demonstrou, numa breve pesquisa, que o assunto é bem delineado pela legislação nacional: o Código Civil prevê que a invasão de privacidade configura ato ilícito, ensejando sua reparação mediante o ressarcimento material; o Código Penal, com a alteração promovida pela Lei 12.737/2012 – Lei dos Crimes Informáticos (Lei Carolina Dieckmann) –, tipificou as condutas criminosas promovidas nessa seara, prevendo, inclusive agravante quando o delito for cometido contra autoridade pública; e, ainda, a Lei de Interceptação Telefônica (Lei 9.296/1996), já citada, também trata do tema em seu art. 10 ("Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de

informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei").

Além desses diplomas legais, a espionagem com interesses econômicos é punida com legislação protetiva da propriedade intelectual, ao passo que a espionagem com interesses políticos e contra a segurança nacional é tratada pela Lei de Segurança Nacional (Lei 7.170/1983).

Se existem leis e há uma imensa gama de ferramentas tecnológicas direcionadas para a segurança, onde está a fragilidade do sistema?

O Sr. Marcos Mesquita respondeu que a maior fragilidade para a segurança de qualquer sistema está na atitude das pessoas que neles atuam. Portanto, é necessário valorizar uma cultura de segurança. Os sistemas não resolverão tudo por nós. Basta lembrar que a NSA, a grande espiã do mundo, foi espionada da forma mais antiga que existe, por um funcionário de terceiro escalão de uma empresa terceirizada: Edward Snowden.

Finalizada a primeira parte, foi passada a palavra ao Relator da CPI para que este iniciasse questionamento aos palestrantes, ao que foi seguido pelos Senadores Eduardo Suplicy, Vanessa Grazziotin e Pedro Taques.

Pergunta 1 (Senador Ricardo Ferraço). Considerando que, em audiência anterior, o Sr. Greenwald disse que as empresas de telecomunicações são parceiras-chave no processo de espionagem, perguntou se as empresas representadas na reunião possuem algum acordo de entrega de dados ou relatórios a algum governo.

Resposta do Sr. Marcos Augusto Coelho: O Sr. Marcos Augusto Coelho negou a existência de qualquer tipo de acordo de repasse de dados.

Resposta do Sr. Ivan Campagnolli: Negou a existência de qualquer tipo de acordo de transferência de dados com entidades nacionais ou internacionais. A única hipótese de repasse de dados é sob determinação judicial.

Resposta do Sr. Ari Sérgio Falarini: Disse não haver nenhum tipo de acordo de entrega de dados para governos ou entidades externas.

Pergunta 2 (Senador Ricardo Ferraço). Questionou como é feito o repasse de dados de usuários, quando solicitado por mecanismo legal.

Resposta do Sr. Marcos Augusto Coelho: O convidado explicou que, nos casos de interceptação legal, não há nenhuma participação da companhia na escuta da operação. A autoridade policial faz a escuta e, terminada a investigação, o *link* é cortado, sem que haja qualquer envolvimento da empresa com o conteúdo das comunicações.

Pergunta 3 (Senador Ricardo Ferraço). Indagou onde e como poderia haver interceptação de dados nas redes das companhias, bem como se seria possível ocorrer interceptação sem que nenhum funcionário tenha conhecimento. Se sim, quando a operação poderia ser percebida e quais seriam as providências tomadas.

Resposta do Sr. Marcos Augusto Coelho: O Sr. Marcos Augusto Coelho disse que toda experiência de vazamento de dados de

clientes acabou gerando uma melhora na capacidade de evitar esse tipo de falha. Destacou que o ponto fraco geralmente é o ser humano, a pessoa que comete o crime. Citou um caso em que um funcionário, apesar de ter passado por um processo seletivo rigoroso, recebeu um apelo externo para repassar dados dos clientes. No entanto, o procedimento foi rastreado em seu equipamento e ele acabou sendo preso. Assim, ressaltou que o fundamental é que o sistema se previna contra esse tipo de interferência. Caso isso não seja possível, que o ponto de fragilidade seja rastreável. Segundo ele, imediatamente após a identificação do ponto frágil, é feito um trabalho de revisão de procedimentos e aumento da capacidade de segurança.

Resposta do Sr. Ivan Campagnolli: Inicialmente, enfatizou que o crime de interceptação acompanha a evolução tecnológica, muda com o tempo e de maneira individualizada, buscando falhas no sistema, na manutenção no momento específico do crime. Quando identificado, o procedimento normal é a abertura de um boletim de ocorrência para apurar se alguém, de posse de informações confidenciais, agiu de maneira criminosa. Reforçou que a empresa possui todo um procedimento e cuidado com a rede para evitar que isso ocorra, pela responsabilidade que tem na proteção de seus ativos. Ademais, defendeu que todo acordo de conexão com uma operadora legalmente estabelecida seja redigido por um contrato que contenha cláusulas que garantam a preservação da integridade dos dados.

Resposta do Sr. Nelson de Sá: O Sr. Nelson de Sá reforçou que o elo de fragilidade no sistema é a pessoa que comete o crime. Segundo informou, a TIM realiza auditorias praticamente de hora em hora para verificar tudo o que foi solicitado legalmente. É feita a varredura de todas

as centrais e, se houver alguma programação que não esteja atrelada a um ofício, o processo é desfeito e é aberta uma investigação. Se houvesse um vazamento de dados – o que nunca ocorreu na empresa – o fato seria comunicado oficialmente aos órgãos competentes.

Resposta do Sr. Ari Sérgio Falarini: Lembrou que qualquer frequência liberada para uso no Brasil passa por um controle feito pela Anatel, que também a fiscaliza. Ademais, qualquer intervenção na rede é rapidamente sinalizada pelos sistemas de alarme das operadoras. As ações necessárias são tomadas de imediato, até mesmo para não haver nenhuma perda de tráfego. No caso da fibra ótica, disse ser praticamente impossível utilizar um aparato que, em um curto espaço de tempo, consiga mapear volume de informações transmitidas.

Pergunta 4 (Senador Eduardo Suplicy). Perguntou se as empresas possuem algum mecanismo para garantir a privacidade dos usuários de seus sistemas, tanto nas comunicações por telefone quanto por internet.

Resposta do Sr. Ivan Campagnolli: Disse que existe uma série de mecanismos, proteções codificadas de senha, quem tem acesso, com que perfil e para qual atividade. O processo é auditado e os mecanismos protegem a rede contra ataques externos ininterruptamente. Afirmou com convicção que a rede da empresa é segura.

Resposta do Sr. Nelson de Sá: Explicou que os mecanismos para garantir a comunicação privada são implementados pelo próprio protocolo GSM, mas que, atualmente, já existem mecanismos que utilizam aparelhos de criptografia. No caso da internet, salientou que se trata de uma rede aberta, passível de diversos mecanismos de quebra de sigilo. Assim,

muitas vezes, por desconhecimento, ao aceitar um contrato de adesão referente ao uso de um programa, a pessoa abre mão de sua liberdade.

Resposta do Sr. Ari Sérgio Falarini: Ratificou a importância de o usuário ficar atento no momento de aceitar os termos e condições de uso de um aplicativo ou ferramenta adquirido, para ter a consciência do uso que pode ser feito daquilo.

Pergunta 5 (Senador Ricardo Ferraço). Questionou quais são os aspectos enfocados nas auditorias realizadas periodicamente pela Agência Nacional de Telecomunicações (Anatel), se os aspectos segurança de rede e sigilo das informações são considerados.

Resposta do Sr. Marcos Augusto Coelho: O representante da Oi disse não saber os pontos de checagem da Anatel nas auditorias, pois não atende a fiscalização. Contudo, disse acreditar que a Anatel tenha programas de auditagem que cubram todos os aspectos da operação de telecomunicações. Acrescentou que, por ser cotada em bolsas internacionais, a Oi é obrigada a obedecer a padrões internacionais em boa parte de seus processos. Por isso, é auditada por entidades externas constantemente, para garantir que sejam mantidos certos padrões de gerenciamento, tanto em aspectos operacionais quanto financeiros e de segurança.

Resposta do Sr. Ivan Campagnolli: Informou que a Anatel considera diversos fatores nas auditorias. Disse não se lembrar de nenhuma auditoria específica de segurança, mas que nem todos os casos passam pelo Comitê Executivo. Em sua opinião, após os eventos recentes, a agência certamente tratará de forma mais específica do tema.

Resposta do Sr. Nelson de Sá: Explicou que as fiscalizações da Anatel possuem variados modelos e formas, além de ocorrerem periodicamente. Segundo relatou, recentemente foram questionados e testados os padrões de controle da empresa. Destacou que a TIM também é uma empresa cotada nas bolsas internacionais, passando, portanto, constantemente por auditorias de *Sarbanes-Oxley*, que incluem a verificação dos níveis de controle de segurança.

Resposta do Sr. Ari Sérgio Falarini: Informou que são realizadas regularmente auditorias da Anatel, tanto para SLAs técnicos operacionais quanto para verificação dos dispositivos de segurança na rede. No procedimento, são informados os funcionários que tiveram acesso à rede, o horário em que a acessaram, bem como o tipo de atuação realizada. Há ainda a auditoria interna, que verifica se as programações estão corretas. Caso não estejam, o problema é rapidamente identificado e corrigido.

Pergunta 6 (Senadora Vanessa Grazziotin). Considerando que o Sr. Nelson de Sá declarou que a TIM possui um *data center* instalado no Brasil e que todos os *data centers* de internet estão localizados nos Estados Unidos, perguntou que tipo de informações as empresas armazenam em seus centros. Além disso, solicitou que os palestrantes opinassem se a obrigatoriedade de as empresas de internet manterem *data centers* no Brasil aumentaria a segurança dos brasileiros.

Resposta do Sr. Marcos Augusto Coelho: Ponderou que, se tratasse do tema de forma superficial, responderia que a Oi é favorável à manutenção de *data centers* de internet no Brasil, que essa medida aumentaria a clientela da empresa. Contudo, lembrou que esse debate, incluído na discussão do marco civil da internet, deriva da ideia de que se o

Brasil possuir dados armazenados em seu território, sob sua jurisdição, poderá requisitá-los para efeito de investigação. No entanto, pontuou que o grande problema nessa questão reside no fato de o usuário, para utilizar um serviço, concordar com termos de uso de uma empresa estrangeira. Assim, acaba aceitando que qualquer demanda sobre aquele serviço deva ser feita em um foro no exterior, abrindo mão da proteção da legislação brasileira, o que dificulta imensamente o procedimento, caso necessário. Dessa forma, sublinhou que o foco da discussão deve ser a jurisdição dos dados, e não a guarda propriamente dita, pois o problema permanecerá se os dados forem guardados em território nacional, mas mantida a jurisdição do país de origem. O local onde os dados são armazenados não afeta em nada a questão da privacidade propriamente dita, já que estarão submetidos às mesmas regras internacionais de qualidade e operacionalidade. Informou ainda que há um projeto de lei na Câmara dos Deputados que trata de forma eficiente sobre o tema.

Resposta do Sr. Ivan Campagnolli: Afirmou que a Claro é favorável à manutenção de *data centers* no Brasil.

Resposta do Sr. Nelson de Sá: Esclareceu que são armazenados nos *data centers* os metadados de uma ligação ou de início de uma comunicação de dados, mas nunca o conteúdo. Quanto à obrigatoriedade de *data centers* de internet no País, ponderou que a medida em si não resolveria o problema, uma vez que muitas empresas manteriam os dados no Brasil, mas não os forneceriam dada a matriz ser estrangeira. Apesar disso, defendeu que haja incentivos e investimentos para que esses dados tenham polos tecnológicos de armazenamento no País, já que com o uso da nuvem será cada vez mais difícil saber a localização dessas informações no mundo.

Resposta do Sr. Ari Sérgio Falarini: Disse que a Vivo defende a existência de *data centers* locais.

Pergunta 7 (Senadora Vanessa Grazziotin). Relembrando que até mesmo a Presidenta Dilma teve suas comunicações interceptadas – inclusive telefônicas – perguntou o que os palestrantes sabem sobre o caso, além do divulgado pela imprensa. Tomando esse caso como exemplo, perguntou o que garante a segurança das comunicações.

Resposta do Sr. Marcos Augusto Coelho: Informou que não sabia que tinha havido interceptação de conteúdo das comunicações da Presidenta. Reafirmou que, mesmo nos casos de interceptação legal, não há nenhuma participação da empresa na escuta da operação.

Resposta do Sr. Ivan Campagnolli: Disse não saber mais detalhes do ocorrido, mas que a preocupação com o assunto existe, tanto que há equipamentos celulares criptografados.

Resposta do Sr. Nelson de Sá: Sobre a segurança das comunicações, afirmou que ela é garantida por protocolos, mas que, infelizmente, não há limites tecnológicos para a prática de crimes.

Pergunta 8 (Senador Ricardo Ferraço). Questionou se, quando as empresas de telecomunicações nacionais fazem alianças com empresas estrangeiras, a legislação permite que estas tenham acesso ou possam ter acesso, caso demandem, às comunicações realizadas.

Resposta do Sr. Marcos Augusto Coelho: O representante da Oi disse que não há nenhum tipo de acordo de repasse de dados. Há apenas questões relacionadas a faturamento, que permitem que o titular de uma rede externa possa cobrar do cliente da Oi quando este utilizar sua rede,

como ocorre em ligações de longa distância. Nesse caso, a empresa precisa saber quem ligou, quando e o tempo da ligação para fazer a tarifação, mas nada relacionado ao conteúdo da comunicação.

Resposta do Sr. Ivan Campagnolli: Ratificou que a aliança com outras empresas é segura, é uma relação comercial estabelecida por um contrato válido, juridicamente perfeito e que preserva, por obrigação, todos os dados dos clientes. Não há entrega de metadados para nenhuma operadora e acredita que os acordos sejam respeitados.

Resposta do Sr. Nelson de Sá: Informou que a TIM mantém alianças apenas comerciais, que não há nenhum acordo de troca de dados.

Resposta do Sr. Ari Sérgio Falarini: Afirmou que a Vivo não inclui nenhuma cláusula que permita a abertura de informações dos clientes em seus contratos comerciais. Os contratos prezam por um padrão de qualidade, de disponibilidade e de preservação do conteúdo da informação do cliente.

Pergunta 9 (Senador Pedro Taques). Solicitou que os palestrantes comentassem sobre os processos, instrumentos e mecanismos necessários para a interceptação das comunicações telefônicas da Presidenta Dilma fora do sistema de rede das empresas. Perguntou se os palestrantes têm conhecimento se é possível fazer no Brasil interceptação sem a participação das companhias, por meio de malas, *notebooks, tablets* e outros apetrechos, dado que a literatura informa que, em alguns países podem-se adquirir esses equipamentos.

Resposta do Sr. Marcos Augusto Coelho: O palestrante sublinhou que a rede não armazena nada, mas que existe a rede doméstica do cliente, que está fora do gerenciamento da Oi. Assim, a empresa não

consegue certificar sua segurança. Salientou que tudo que precisa utilizar a rede da companhia é detectável, identificável e rastreável. Segundo o Sr. Marcos Augusto Coelho, o primeiro ponto de fragilidade na comunicação a ser analisado é a estrutura interna do cliente. A rede é a última coisa a ser olhada.

Resposta do Sr. Nelson de Sá: Confirmou a existência de maletas que capturam a informação, que na última feira de segurança havia um estande expondo essas ferramentas. Em sua opinião, a interceptação da Presidenta Dilma pode ter ocorrido de forma mais próxima do que se imagina, inclusive utilizando essas maletas.

Resposta do Sr. Ari Sérgio Falarini: Afirmou ter a convicção de que a interceptação das comunicações da Presidenta Dilma ocorreu de uma maneira mais próxima do que se imagina.

Pergunta 10 (Senador Pedro Taques). Considerando a hipótese de a agência americana estar acessando o conteúdo das comunicações da Presidenta Dilma dos Estados Unidos, questionou se as redes das companhias nacionais constatariam essa invasão. Ademais, perguntou se existem protocolos internacionais que tratem disso. Por fim, indagou se é possível fazer essa interceptação remotamente, por um método não invasivo na rede, mas por meio de ondas de rádio.

Resposta do Sr. Leandro Henz (gestor de rede da Oi, representando o Sr. Marcos Augusto Coelho): De acordo com o Sr. Leandro Henz, seria inviável, do ponto de vista prático, fazer uma interceptação nos cabos submarinos (que transportam grandes quantidades de dados entre as operadoras) para se obter dados, por serem extremamente pesados, com um alta voltagem e comportarem um tráfego de 500 *gigabits*

por segundo. Portanto, se ocorresse uma interceptação, seria indetectável. No caso da comunicação por celular, por sua vez, há relatos na literatura de que existem equipamentos que, se colocados próximos ao usuário conseguem, com certo tempo, captar esses dados móveis. Outra maneira de fazer uma interceptação seria por meio do próprio aparelho celular. Como os *smartphones* são pequenos computadores, ao aceitar a instalação de um aplicativo, o usuário pode, equivocadamente, autorizar um *spyware* ou um *malware* que vai enviar toda a informação contida no dispositivo para determinado lugar.

Resposta do Sr. Ivan Campagnolli: O Sr. Ivan Campagnolli informou que é muito mais difícil ter o mecanismo para detectar uma interceptação por ondas de rádio. Por outro lado, se realizada por meio da conexão de fio, dependeria de uma informação sigilosa – que, se repassada, configuraria crime – e poderia ser descoberta por um processo normal de recuperação. Segundo ele, até mesmo uma improvável interceptação nos cabos submarinos seria detectada.

Resposta do Sr. Ari Sérgio Falarini: Retomando o que foi dito pelos demais convidados, ratificou que as empresas trabalham para prover segurança ao usuário, mas que existem artifícios comercializados – como as maletas já citadas – que podem ser utilizados de maneira maliciosa. Sobre a vulnerabilidade das redes, reforçou que os cabos submarinos são de difícil manuseio, pois requerem equipamentos e veículos extremamente especializados, sofisticados e custosos para tanto. Lembrou que as intervenções na rede são rapidamente sinalizadas pelos sistemas de alarme das operadoras. No caso da fibra ótica, disse ser praticamente impossível utilizar um aparato que, em um curto espaço de tempo, consiga mapear volume de informações transmitidas.

12ª Reunião, realizada no dia 12/11/2013 (Serpro e Prodasen)

Objeto: Audiência Pública com os representantes do Serviço Federal de Processamento de Dados (Serpro) e da Secretaria Especial de Informática do Senado Federal (Prodasen).

No dia 12 de novembro de 2013, a CPI da Espionagem, com base em entendimento firmado pelos membros da Comissão, promoveu uma audiência pública para ouvir os Srs. Marcos Vinícius Ferreira Mazoni, Diretor-Presidente do Serviço Federal de Processamento de Dados (Serpro) e Victor Guimarães Vieira, Diretor da Secretaria Especial de Informática do Senado Federal (Prodasen). O objetivo desta audiência pública foi conhecer as preocupações desses órgãos – referenciados como algumas das melhores empresas de processamento do País – com relação à segurança da informação e as soluções que eles adotam quanto a isso. A reunião foi presidida pela Senadora Vanessa Grazziotin, estando presente o Senador Eduardo Suplicy. Participou da rodada de questionamentos, também, o Sr. André Luiz Bandeira Molina, coordenador da área de Infraestrutura de Tecnologia da Informação do Prodasen.

Marcos Vinícius Ferreira Mazoni

O Diretor-Presidente do Serpro concentrou-se em apresentar as vulnerabilidades de segurança e privacidade a que as informações governamentais estão expostas e o que entende como soluções a esses problemas.

Inicialmente, esclareceu a relação do Serpro com o tema da segurança da informação. Embora a empresa pública não seja a responsável direta pela segurança cibernética do Governo, lida com sistemas

estratégicos para o funcionamento do País, o que exigiu o desenvolvimento, ao longo do tempo, de soluções com foco na segurança da informação. Entre esses sistemas estratégicos, citou os que permitem gerenciar serviços de importação e exportação, transferências de recursos do Governo Federal para outros entes federativos, arrecadação e despesas do Governo. Uma interrupção nos serviços da empresa implicaria prejuízos ao País e acarretaria uma paralisação do próprio Estado.

Para a apresentação à CPI, o convidado apresentou vulnerabilidades e soluções em seis áreas: rede mundial de computadores; rede de governo; nuvens de governo; centros de dados de governo; aplicações de governo; e correio eletrônico utilizado pelo governo.

Rede mundial de computadores

As principais vulnerabilidades da rede mundial de computadores são:

a) A concentração da governança da internet nos Estados Unidos. O Brasil tem um modelo de gestão de governança da internet que deveria servir como modelo internacional, pois conta com a participação da sociedade, de órgãos governamentais e de entidades privadas;

b) Quanto à rede física da internet, muitos dos cabos e satélites utilizados pelo Brasil não são controlados pelo País, mas por empresas privadas. Noticia-se, atualmente, a existência de submarinos dedicados à coleta de dados diretamente dos cabos que cruzam os mares;

c) Já a rede lógica da internet (incluindo as rotas, os servidores centrais da internet e o sistema de nomes de domínios – DNS) concentra-se principalmente nos Estados Unidos, o que sujeita os dados que transitam por esses grandes centros de roteamento à legislação daquele país;

d) Por fim, liga-se a isso o fato de que grande parte dos dados é armazenada em centrais norte-americanas, o que permite que essas informações sejam acessadas pelo Departamento de Defesa dos Estados Unidos.

As soluções apresentadas a essas vulnerabilidades da rede mundial são, conforme o expositor:

a) Governança mundialmente democratizada da internet, uma das ideias defendidas pela presidenta Dilma na abertura da 68ª Assembleia-Geral das Nações Unidas;

b) Distribuição geográfica e política dos servidores centrais da internet, fazendo com que a tráfego de informações comece a ocorrer também fora dos Estados Unidos;

c) Instalação de um maior número de cabos de conexão de redes no continente sul-americano, o permitiria um controle mais efetivo da rede física;

d) Desenvolvimento de satélites, o que faz parte da política aeroespacial brasileira;

e) Fortalecimento do Comitê Gestor de Internet (CGI), responsável pela governança da internet no Brasil e que é modelo de participação de diferentes atores.

Rede de Governo

O segundo rol de vulnerabilidades e soluções refere-se à rede de Governo. Hoje, toda a infraestrutura física da "infovia" que atende aos órgãos governamentais é operada pelo Serpro. Mas isso não garante proteção total a essa rede, que está exposta às seguintes vulnerabilidades:

a) Predominância de redes de operadoras de telecomunicações, o que representa um problema na medida em que, para reduzir custos, a

troca de tráfego entre operadoras normalmente ocorre fora do Brasil, principalmente em Miami (EUA);

b) Costuma-se trabalhar com dados não criptografados.

c) Fragilidades de segurança contidas nos *softwares*, como *backdoors*. Isso porque esses produtos obedecem à legislação norte-americana, que dá ao Departamento de Segurança dos Estados Unidos o direito de acesso aos dados manipulados por esses programas. Classificou alguns destes como "caixas pretas", pois eles não permitem saber ao certo que informações enviam pela rede.

d) A exposição de roteadores de borda, que traz vulnerabilidade à informação sempre que a parte da rede sobre a qual há controle se liga a outras redes.

e) Por último, apontou que o domínio da infraestrutura (equipamentos de rede) e das aplicações utilizadas (sistemas operacionais e bancos de dados) pertence a empresas privadas, especialmente norte-americanas. Assim, mesmo que o ambiente seja gerido com a máxima segurança, o aparato por trás dele carece de controle.

Sobre as vulnerabilidades apontadas nesta segunda etapa, ofereceu como possíveis soluções:

a) Uso de uma infraestrutura pública de comunicação. Explicou que fibras óticas estão ligando as capitais do País e que a "infovia" de Brasília está em expansão. Isso garantirá que o País tenha um maior controle das informações que saem da rede. Muita ênfase foi dada ao reconhecimento de qualquer tentativa de entrada não autorizada no ambiente controlado pelo Serpro. Mas o movimento inverso também é necessário, pois ainda não se tem um controle efetivo das informações que saem pelas *backdoors* de equipamentos e *softwares*.

b) Liga-se a esse objetivo a meta de ampliar a capacidade governamental de gestão, monitoramento e auditoria de equipamentos. Conforme detalhou, o Instituto Nacional de Tecnologia da Informação (ITI) contrata o Centro de Pesquisa da Universidade de São Paulo (USP) para auditar todos os equipamentos utilizados pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). É o mesmo Instituto que audita os equipamentos utilizados pelo sistema bancário brasileiro. Isso não torna o sistema bancário livre de tentativas de ataque. Contudo, quanto mais protegido o sistema, maior a capacidade de processamento necessária para quebrar suas chaves, o que consome muita energia e torna o processo extremamente oneroso.

c) Outra meta é o investimento em protocolos de segurança da informação que sejam seguros e livres. Ao contrário do que se pensa, os *softwares* livres não são menos seguros. Por terem código aberto, eles podem ser auditados e podem ser alterados para ampliar o nível de segurança, diferentemente de um *software* proprietário.

d) Relacionou também o investimento em *hardware* nacional de rede. O meio universitário brasileiro já detém capacidade de desenvolver roteadores com taxa de transferência (*throughput*) compatível com os internacionais. Já há, também, roteadores comerciais desenvolvidos no Brasil com capacidade próxima aos internacionais. Até 2015, os equipamentos centrais do projeto Infovia Brasil deverão ser de origem nacional. Ainda sobre esse assunto, o expositor explicou que o mundo acadêmico desenvolve um método para subtrair a inteligência de roteamento (camada três) dos equipamentos e construí-la novamente por meio de programação, o que torna o equipamento mais seguro. Em breve, essa tecnologia será aplicada aos equipamentos nacionais.

e) Outra solução apontada é o uso de criptografia, que deve ser associada com o desenvolvimento nacional de *hardware*, deixando os ambientes virtuais mais protegidos contra ataques cibernéticos. Porém, esse conhecimento de criptografia deve ser associado com o desenvolvimento nacional de *hardware*, deixando os ambientes virtuais mais protegidos contra ataques cibernéticos. A criptografia do ICP-Brasil e do Serpro é desenvolvida em parceria com universidades brasileiras. Já o *hardware* é nacional, desenvolvido em conjunto com a Universidade Federal de Santa Cataria (UFSC) e com a Universidade de Campinas (Unicamp) e produzido por uma empresa no Centro de Tecnologia da Unicamp.

f) Finalizando, citou a necessidade de ampliar investimento na indústria nacional de defesa cibernética. À medida que essas empresas avançarem, elas serão capazes de oferecer equipamentos competitivos e desenvolver proteção contra ameaças externas.

Criptografia

Nesse tocante, o expositor explicou que o recurso de criptografia, quando utilizado, destina-se ao chaveamento do caminho das mensagens, mas não do conteúdo delas. Soma-se a isso o fato de que os algoritmos de criptografia e os equipamentos criptográficos são criados ou controlados por países estrangeiros. Além do mais, é preciso cuidado com a construção de chaves criptográficas fracas, a depender dos algoritmos empregados nelas.

A solução a esses problemas passa pelo investimento em projetos de formação e pesquisa em criptografia. O Serpro, por exemplo, desenvolve, em parceria com a USP e a UFSC, um projeto de formação de técnicos nessa área. É preciso que os órgãos governamentais façam amplo uso do recurso de criptografia e das chaves públicas fornecidas pelo ICP-

Brasil. A parceria com outros países aprimora esse processo, já que a cooperação permite que se construa uma rede cada vez mais segura para todos. Por fim, é preciso auditar os equipamentos e programas em uso para a descoberta de falhas e vulnerabilidades.

Nuvem de Governo

Passando a tratar de computação em nuvem para o Governo, o palestrante considerou de extremo risco a contratação de serviços privados nessa área. Segundo ele, embora nove das dez maiores nuvens no mundo sejam feitas a partir de *software* livre, o acesso do contratante ao conjunto de dados alocados é dificultado, o que não resolveria o problema de salvaguardá-los. Há ainda a ressalva de que muitos serviços obedecem às leis americanas, que facilitam o acesso do Governo dos EUA aos dados. Outro problema apontado é a falta integração entre diferentes nuvens, pois de nada adianta haver uma nuvem governamental que não consiga se relacionar com outras.

Explicando possíveis saídas a essas questões, disse que o Serpro desenvolve, desde 2012, um projeto nacional para criar a nuvem de Governo, feita a partir de *software* livre, o que oferecerá à nuvem um nível de segurança que o *software* proprietário não alcançaria. Além disso, a empresa busca construir uma ferramenta de comunicação entre diferentes nuvens, também feita com código aberto. Para isso, conta com equipes especializadas nos seus onze polos de desenvolvimento, trabalhando com diferentes tipos de tecnologias. Ainda utilizando *software* livre, o Serviço desenvolve redes sociais que se conectam com as redes mais comuns, como Facebook e Twitter, mas não alocam dados nelas. A rede Participatório, da Presidência da República, é um exemplo.

Centros de dados de governo

O próximo tópico discutido foi o tratamento dado os centros de dados (*data centers*) governamentais. As principais vulnerabilidades, nesse caso, são:

a) A possibilidade de acesso indevido a dados e aplicações, pois os programas utilizados neles são dependentes de sistemas operacionais fechados;

b) A contratação de centros de dados privados, seja dentro ou fora do Brasil, também implica certo risco, uma vez que esses, buscando renovar de contratos, muitas vezes aprisionam dados como forma de pressionar o governo, como se essas informações fossem propriedades deles.

A isso, o palestrante apresentou como soluções:

a) Ações de gestão e classificação de documentos e dados, o que evita a superproteção de informações que não são sigilosas e, que, devem, inclusive, ser de conhecimento público.

b) Gerenciamento de identidades, que busca tratar as fragilidades internas. Na construção do programa para declaração do imposto de renda anual, por exemplo, são alocados mais de quatrocentos profissionais. Deve haver registro de todas as ações feitas, e de sua autoria. Mas os ambientes externos também devem ser monitorados e geridos, permitindo reconhecer qualquer tentativa de acesso indevido a dados.

c) Uso de protocolos de segurança abertos e livres, evitando programas de código fechado, que podem passar informações aos seus fabricantes.

d) Análise de licenciamento de *softwares*, de forma que eles passem a respeitar a legislação brasileira e eliminem quaisquer formas de *backdoor*.

e) Uso progressivo de *softwares* livres, o que por si só já elimina o problema de *backdoors*. No Serpro, 70% dos programas utilizados são em *software* livre. O programa para declaração do imposto de renda disponibilizado em 2012, por exemplo, é todo desenvolvido em *software* livre, o que atende também à necessidade de portabilidade. Assim, o programa passou a ser aberto em qualquer ambiente operacional, e não somente no da Microsoft.

f) Por fim, auditoria dos equipamentos e programas em uso, o que, no caso do Serpro, é feito em parceria com universidades.

Aplicações de Governo

Prosseguindo a exposição, o Sr. Marcos falou das principais vulnerabilidades das aplicações de governo, que se referem a programas com *backdoors*, sem possibilidade de auditoria (pois não são feitos em código livre) e com licenças sujeitas à legislação estrangeira, especialmente a norte-americana. Citou também, o despreparo dos gestores públicos responsáveis pelas contratações quanto ao tema de segurança. Nesse sentido, muitos juristas apontam que o Brasil pode estipular a obrigação de atendimento à lei nacional nos editais para a compra de produtos ou contratação de serviços. Mas esse recurso, não raro, é ignorado, porque a segurança da informação ainda não é vista como preocupação relevante.

As soluções para isso, apontou o expositor, passam por:

a) Uso de *software* livre, o que o Serpro busca desde 2007. Esses programas permitem alterações sem que se dependa do fabricante, o que aumenta o padrão de segurança;

b) Uso de *softwares* públicos, que são replicáveis. Por meio deles, as boas experiências e soluções podem ser compartilhadas.

c) Análise de licença de *software* nas aquisições governamentais, de forma que os termos dessas licenças obedeçam à legislação brasileira.

d) Promoção de capacitação em normas de segurança.

e) Por último, o aumento do número de profissionais com formação sólida em segurança da informação e a criação de centros de excelência nessa área.

Correio eletrônico

Por último, o expositor fez considerações quanto ao uso de correio eletrônico. O uso de programas sujeitos à legislação estrangeira facilita a interceptação de mensagens e o monitoramento de comunicações por outros países. Segundo narrou, a existência de *backdoors* nos programas Outlook e BlackBerry já foi identificada. Ainda falta conscientização dos usuários sobre o problema. Muitos utilizam emails particulares em serviço, outro problema apontado.

Apresentando soluções e esses problemas, o expositor destacou que o Serpro desenvolve o programa de correio eletrônico Expresso que, por determinação da Presidência, será utilizado por toda a gestão pública Federal. O Expresso é desenvolvido em *software* livre e já tem reconhecimento internacional. Os dados das mensagens trocadas serão todos hospedados nos servidores do Serpro. Preocupada com a gestão segura de arquivos, a nova versão do programa criptografará não só o caminho da mensagem, como todo o conteúdo dela. Além de oferecer o Expresso, o Serpro, em parceria com universidades, analisa a segurança de outros programas de correio eletrônico.

Sr. Victor Guimarães Vieira

Em sua apresentação, o Sr. **Victor Guimarães Vieira** trouxe informações acerca das atividades do Prodasen, órgão de gestão de informação do Senado Federal.

Atribuições: gerir a informação, implementar a estratégia de tecnologia da informação, prover serviços, soluções, suporte e infraestrutura tecnológica da informação àquela Casa Legislativa, além de gerir os riscos operacionais com origem em tecnologia da informação.

Produtos e serviços: a) soluções tecnológicas aos processos finalísticos da Casa – atividade legislativa, gabinetes de Senadores e orçamento; b) soluções tecnológicas aos processos administrativos, financeiros e de recursos humanos do Senado; e c) padronização dos sistemas desenvolvidos, em código aberto, pelo próprio Prodasen.

Controles de segurança adotados: a) legais, com políticas e normas de segurança no âmbito do Senado Federal e fiscalização externa realizada pelo Tribunal de Contas da União (TCU); b) de gestão corporativa de segurança da informação, com análises e avaliação de riscos; c) técnicos, com a utilização de *firewalls* de rede e de aplicação, IPS, proxy e proxy reverso, criptografia, antivírus, *antispam* e outros produtos complementares para o funcionamento e a preservação do Datacenter; e d) administrativos, com a segregação de funções, segurança perimetral, capacitação de usuários, auditorias e processos de trabalho, podendo envolver outros setores da Casa, como a Polícia do Senado e a Telefonia.

Dados relevantes sobre as atividades de controle de segurança na rede do Senado: a) 35 milhões de mensagens maliciosas bloqueadas de janeiro a outubro de 2013, correspondendo aproximadamente a 30% das

mensagens externas recebidas; b) cerca de 3 milhões tentativas bloqueadas de ataques à rede somente no mês de outubro de 2013.

Melhores práticas adotadas em segurança da informação: recomendações do TCU e orientações do *Control Objectives for Information and related Technology* (COBIT) e da *Information Technology Infrastructure Library* (ITIL).

Indicadores de segurança utilizados: análises de segurança, relatórios de segurança e comunicados de usuários e da comunidade.

Normativos de segurança da informação no Senado Federal: a) Política de Gestão de Riscos Organizacionais do Senado Federal – Ato da Comissão Diretora nº 16/2013; b) acesso e uso da Internet e das redes sociais por meio da Rede do Senado Federal – Ato do Primeiro-Secretário nº 14/2011; c) uso e administração do sistema de correio eletrônico do Senado Federal – Ato do Primeiro-Secretário nº 6/2010; d) uso e administração dos recursos computacionais e da rede do Senado Federal: Ato do Primeiro-Secretário nº 54/2009; e) uso e administração do serviço de acesso à rede sem fio nas dependências do Senado Federal – Ato do Primeiro-Secretário nº 7/2008; f) uso e administração do serviço de acesso remoto da rede local do Senado Federal – Ato do Primeiro-Secretário nº 25/2003; e g) Regulamento Administrativo do Senado Federal que dispõe sobre áreas e uso de tecnologia da informação no Senado Federal.

Encerrada esta primeira parte, os convidados foram questionados pelos parlamentares. A sequência foi iniciada pelo Sr. Eduardo Suplicy.

Pergunta 1 (Senador Eduardo Suplicy). Pediu a definição de *software*, *hardware*, nuvem e e-mail seguro.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: esclareceu que *hardware* é a máquina, a parte física. Já o *software* é o programa.

Nuvem é um conceito atual e complexo. Trata-se de uma tecnologia nova de armazenamento de dados, realizado em múltiplos ambientes, possibilitando maior disponibilidade de acesso.

Um sistema de e-mail é seguro quando se tem o controle de sua programação, conhecendo a cada um dos seus elementos, e se tem o controle sobre o ambiente de proteção. Assim, por exemplo, é o caso do Expresso V3 desenvolvido pelo Serpro a ser adotado no Governo Federal brasileiro, uma vez que foi feito em plataforma de *software* livre e está no ambiente de proteção do próprio Serpro. Ainda quanto ao Expresso V3, disse ser resultado da cópia das melhores funções oferecidas nos *softwares* de mercado, como o Gmail, Exchange e Lotus Notes e que possui alto grau de segurança por ter somente uma porta de acesso a todos os seus componentes, podendo o Serpro alterar o grau de proteção de acordo com as necessidades apresentadas.

Pergunta 2 (Senador Eduardo Suplicy). Pediu o levantamento de quantos e-mails cada senador recebe e envia, para verificar grau de comunicação com a população brasileira. Contou sobre a importância de se acessar os dados pela *internet*, principalmente para controle de gastos públicos.

Resposta do Sr. Victor Guimarães Vieira: afirmou que irá fazer o levantamento do número de e-mails recebidos e enviados pelos senadores e enviará para o gabinete do senador Suplicy.

Pergunta 3 (Senadora Vanessa Grazzioti). Questionou se o Serpro teria condições de promover auditagem nas máquinas da administração direta e indireta.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: sobre auditagem, o convidado afirmou que, atualmente, toda rede bancária se comunica de forma exclusiva com o Sistema Integrado de Administração Financeira da União (Siafi), através do sistema SOTN, desenvolvido pelo Serpro. Assim, o sistema de mensageria é direto para todos os pagamentos feitos para e pela União, controlado pelo Serpro, portanto, auditáveis.

Há, ainda, produtos como o Portal dos Convênios, com auditabilidade em prefeituras, ONGs ou hospitais, com necessidade de pacote de serviços para virtualização de ambientes. Citou a comunicação com os DETRANs do País.

Explicou que o *software* de gestão de segurança utilizado pelo Serpro é o Zabbix, que, apesar de ser aberto e livre internacionalmente, é controlado por aquela empresa pública, possibilitando toda a auditabilidade.

Pergunta 4 (Senadora Vanessa Grazzioti). Perguntou se o Serpro e o Prodasen terceirizam serviços. Em caso afirmativo, indagou quais serviços seriam terceirizados. Se a manutenção das redes e do equipamento no Serpro e no Prodasen é realizada por terceirizados e quais são as medidas de proteção em relação às informações que estão contidas.

Resposta do Sr. André Luiz Bandeira Molina: afirmou que existem vários contratos com terceirizados, mas que há requisitos de segurança, como o termo de confidencialidade. A maioria dos contratos é de cunho operacional, como a central de atendimentos, que realiza

atendimento e monitoramento de chamados. Ademais, quando as prestações de serviço são de manutenção e intervenção no sistema, há o acompanhamento do trabalho. Mas ressaltou que a gestão dos equipamentos e dos *softwares* é realizada pelos servidores do Senado Federal.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: todos os serviços de suporte são realizados pelo Serpro, não terceirizam desenvolvimento e operações de sua rede. Os fornecedores são chamados, apenas eventualmente, quando a equipe técnica não consegue solucionar o problema. Entretanto, o trabalho é realizado em conjunto.

Pergunta 5 (Senadora Vanessa Grazzioti). Perguntou qual o percentual de tecnologia nacional presente nos equipamentos e *softwares* de segurança que são utilizados pelo Serpro e pelo Prodasen. Se existe iniciativa no sentido de se alcançar a autonomia brasileira nessa tecnologia. Se há algum comitê público brasileiro de desenvolvimento de tecnologia da informação ou de segurança da informação.

Resposta do Sr. Victor Guimarães Vieira: afirmou que não sabe precisar exatamente o percentual de tecnologia nacional utilizado pelo Prodasen, mas o índice de importação de tecnologia na questão de *hardware* é bem alto. Entretanto, o mesmo não se dá com os *softwares*, pois o sistema utilizado na área finalística do Senado Federal é desenvolvido internamente.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: esclareceu que existe maior dependência de tecnologia internacional na questão do *software*, mas também é expressiva no *hardware*. O investimento deve ser feito nos dois aspectos.

Pergunta 6 (Senadora Vanessa Grazzioti). Fez referência ao Expresso V3, que é o e-mail público utilizado pelo Governo Federal de utilização exclusiva do Governo. Indagou se há possibilidade de ser desenvolvido um e-mail similar para a população em geral, quem caberia desenvolvê-lo e qual a viabilidade financeira desse projeto.

Resposta do Sr. Victor Guimarães Vieira: afirmou que o desenvolvimento de um correio eletrônico nacional, capaz de atender a população, encontra óbices na concorrência e no elevado custo. Afirmou que o Serpro teria como dimensionar o custo com mais precisão. Para que o projeto seja realizado, o convidado acredita que o incentivo deva ser muito grande.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: informou que a Anatel, empresa pública de telecomunicações do Uruguai, está contratando o Serpro para desenvolver e-mail público e disponibilizar para a população.

Se fosse implantado em um país com as dimensões continentais do Brasil, seria necessária uma infraestrutura mais robusta. Em sua opinião, a Telebrás seria a responsável pelo projeto. Mas sugeriu que as operadoras de telecomunicações ofereçam o serviço aos seus clientes. Frisou que o esforço é universalizar o Expresso V3, apesar do foco do Serpro ser o atendimento à Administração Pública Direta Federal.

Pergunta 7 (Senadora Vanessa Grazzioti). Pediu a opinião dos convidados sobre a criação de uma agência nacional de segurança da informação.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: defendeu a criação de uma agência nacional de segurança da informação, para que se discuta o tema. Elogiou o trabalho que o Exército Brasileiro realiza com a segurança cibernética no País, entretanto frisou que o foco é mais o patrimônio físico do que o cibernético.

Pergunta 8 (Senadora Vanessa Grazzioti). Pediu a opinião dos convidados sobre *data centers* e neutralidade da rede, questões polêmicas do projeto do marco civil da *internet*.

Resposta do Sr. André Luiz Bandeira Molina: o convidado acredita ser importante ter *data centers* nacionais. Entretanto, irá aumentar o custo na prestação do serviço, sendo importante se observar se a informação é crítica ou não.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: disse que neutralidade da rede é fundamental. Segundo ele, significa a obrigação das operadoras em não abrir o pacote de dados dos clientes, como estes utilizam a capacidade de internet contratada.

Defendeu a criação de *data centers* como parte de uma política de desenvolvimento do País, mas não como solução de segurança. A solução tem a ver com respeitar a legislação brasileira.

Pergunta 9 (Senadora Vanessa Grazzioti). Diante da afirmação dos convidados de que todos os equipamentos, inclusive os nossos telefones, possuem *backdoor*, indagou o que garante a segurança no tráfego e no armazenamento das informações, visto que a maior parte dos aparelhos é importada dos Estados Unidos.

Resposta do Sr. Victor Guimarães Vieira: disse que o que garante a segurança é a criptografia.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: a respeito de *backdoor*, o Serpro acredita ser importante trabalhar com auditabilidade, criptografia e *software* livre. Deve-se realizar controle sobre códigos e sistemas estratégicos para o País. Toda importação e exportação passa pelo sistema computacional do Serpro, através da Marinha Mercante, Anvisa, Receita Federal e Polícia Federal – o sistema "Porto sem Papel" foi desenvolvido todo no *software* livre Demoiselle do Serpro.

Assim, o investimento nacional deve ser em criptografia, em *hardware* nacional e *software* livre, para melhor controle dos ambientes da rede.

Pergunta 10 (Senadora Vanessa Grazzioti). Diante da informação que o Governo Federal, em Brasília, utiliza a rede de fibra ótica e questionamento o uso fora da cidade, perguntou o que acontece quando sai da rede governamental e entra em uma rede privada. Afirmou que há vulnerabilidade, pois o Estado brasileiro não dispõe de cabeamento e nem de satélite. O satélite que o País possuía no passado foi vendido junto com a Embratel. E quem forneceu a consultoria para o Governo brasileiro, na época da privatização das comunicações, foi formalmente, a empresa Booz Allen, que trabalha e presta serviços diretamente à NSA. Assim, questionou sobre a necessidade de expandir o cabeamento público.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: afirmou que o Serpro utiliza redes fora de seu ambiente. Os grandes *backbones* são contratados de operadoras, pois a rede pública não tem capacidade de atender, via Telebrás, a necessidade do Serpro. Assim, contratam circuitos

no nível 2, que chegam aos seus centros de dados e, a partir desse momento, os *switches* são administrados pelo Serpro. Há uma diminuição da vulnerabilidade, mas não sua eliminação, visto que há nos *switches* equipamentos importados.

Ainda, comentou a venda do Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD), juntamente com a Embratel. O Brasil era um dos únicos países que produzia emenda de fibra ótica. O Estado desenvolvia a tecnologia e colocava para a indústria, se comprometendo com a demanda. Porém, com a perda do CPqD, o País também perdeu tal tecnologia de central telefônica.

Pergunta 11 (Senadora Vanessa Grazzioti). Perguntou como os órgãos têm alcançado a capacidade tecnológica. É realizado apenas com pessoal próprio, ou conta com o apoio das universidades e convênios? Seria o caso de se criar um comitê de desenvolvimento de tecnologia da informação?

Resposta do Sr. Victor Guimarães Vieira: Existe, no Governo Federal, a TI Controle, que são órgãos do Governo que se mobilizam mensalmente para explicitar as melhores práticas e trocar informações; as próprias contratações. São reuniões mensais para discutir as melhores práticas no Governo Federal. Entretanto, não há um órgão específico para tratar de tecnologia e desenvolvimento entre as universidades e pesquisadores.

Resposta do Sr. Marcos Vinícius Ferreira Mazoni: discorreu sobre o projeto brasileiro na área de segurança realizado pela Universidade de São Paulo. Trata-se de um laboratório de pesquisa de alta tecnologia, com destaque para o projeto de desenvolvimento de *hardware*.

Prestam consultoria para o ITI e várias empresas em todo o mundo. Em parceria com o Serpro, pretendem, até o ano de 2014, produzir *hardware* nacional robusto, com criptografia nacional. Elencou outras universidades que possuem projetos na área de segurança: Universidade de Santa Catarina e Universidade de Pernambuco.

Ademais, afirmou que não existe um comitê público de segurança. Visando troca de informações, existe, na esfera federal, o Gabinete de Segurança Institucional (GSI); nas empresas estaduais, a Associação Brasileira de Entidades Públicas de Tecnologia de Informação (ABEP); nas empresas municipais, a Associação Brasileira das Entidades Municipais de Informática (ASBEMI). Entretanto, dizem respeito mais a troca de experiência das melhores práticas do que segurança em si. Destacou a importância de serem criados comitês e trocas de experiências, na lógica do *software* livre.

Por fim, informou que o Serpro possui um centro de pesquisa, com investimentos em tecnologia. Desenvolveram ferramentas, nuvem, Expresso e rede social. Possuem vários projetos com as Universidades dos Estados de São Paulo, Santa Catarina, Rio Grande do Sul, Paraná, Minas Gerais, Pernambuco e Amazonas.

ANEXO III

I. Sugestões apresentadas pela presidente da CPI, senadora Vanessa Grazziotin, acolhidas pelo relator.

Considerações e recomendações a serem incluídas no relatório final da CPI.

Prezados senhores

Cumprimento o trabalho de nosso relator, que ao longo dos últimos sete meses pode compilar e reunir um retrato minucioso de nossas falhas na área de segurança cibernética.

Para corroborar com este relatório, sugiro a inclusão das seguintes recomendações que foram fruto de um encontro muito frutífero que tive em SP com empresas do setor:

AÇÃO 1 – "Compras Educativas" – Criação de um Comitê Gestor no Governo, com alocação de R$50 milhões/ano para compras educativas no setor cibernético. A compra Educativa serve para que a indústria mantenha o seu pessoal do núcleo duro (talentos chave) em atividade e desenvolvendo projetos de menor porte, com o objetivo de se obter ou manter domínio tecnológico em áreas estratégicas.

AÇÃO 2: "Inovação Direcionada" - Criação de edital de subvenção FINEP especifico para o setor cibernético com valor da ordem de 100 milhões. Idealmente, tal edital deve ser coordenado com compras garantidas pelo Governo, tal qual preconizado pela medida MP.6 do Anexo I deste documento.
Adicionalmente, esta ação pode estar coordenada com a AÇÃO 1, acima, e com as medidas 1.2, 4.1 e 4.2 do Anexo I.

Nesta seção são apresentadas medidas viabilizadoras para o setor cibernético no país. Tais proposições se apoiam em parte na publicação "Medidas Viabilizadoras ABIMDE", de Dezembro de 2013.

MEDIDA VIABILIZADORA 1.1 – "Compre Brasil" – Elaboração de legislação objetiva que instrua, oriente e motive os responsáveis pelas aquisições de sistemas e produtos de defesa a priorizar sua compra na BID brasileira. A Constituição Federal estabelece, em seu Artigo 219, que o mercado interno integra o patrimônio nacional e que sua exploração deve visar o desenvolvimento, o bem-estar da população e a autonomia tecnológica do País.

MEDIDA VIABILIZADORA 1.2 – "Programas e Projetos Estratégicos" – Definição e divulgação, com a necessária antecedência, dos principais projetos estratégicos do Ministério da Defesa. A visibilidade antecipada do escopo, do cronograma e do orçamento desses projetos permitirá que a BID brasileira se prepare adequadamente (tanto em termos

de capacitação tecnológica e industrial, quanto de recursos humanos e financeiros) para atender às necessidades.

MEDIDA VIABILIZADORA C.1.5 – "Segurança, Defesa e Infraestruturas Críticas" – Extensão, aos setores de segurança pública e Infraestruturas Críticas, da legislação e dos conceitos aplicados aos produtos e às empresas do setor de defesa.

MEDIDA PONTUAL MP.1 – "Aplicação da Lei 12.598/2012" – Estímulo e, se preservadas condições de concorrência, obrigatoriedade no setor público no uso da Lei 12.598/2012.

MEDIDA PONTUAL MP.2 – "Maior Alcance da Lei 12.598/2012" – Ampliação do escopo da Lei 12.598/2012 para atender compras não só pelas Forças Armadas, mas também sistemas aplicados infraestruturas críticas de Estado, alinhando-se ainda mais com a END.

MEDIDA PONTUAL MP.3 – "Ampliação do escopo do Decreto nº 8.186/2014 de 17 de Janeiro de 2014 (CERTICS)" – Ampliação do referido Decreto para abarcar, além de software, o projeto e o desenvolvimento de hardware e semicondutores, atendendo assim a todo o segmento de TIC. Provê-se, assim, benefícios de concorrência para os sistemas projetados e desenvolvidos no país (maior valor agregado) e não somente para os aqui fabricados.

MEDIDA PONTUAL MP.4 – "Compliance" – Estabelecimento e monitoramento de requisitos de segurança cibernética mínimos a serem observados por provedores de serviços públicos e operadores de

infraestruturas críticas no país, como por exemplo, controle de tráfego, telecomunicações, serviços financeiros, e distribuidores de energia.

MEDIDA VIABILIZADORA 2.1 – "Promoção da Exportação" – Criação de mecanismos, regras e normas governamentais que promovam a exportação de produtos de defesa e segurança e orientem os servidores públicos a participar e contribuir na conquista de clientela estrangeira para os produtos nacionais. A assinatura de acordos bilaterais incentivará as vendas de governo a governo, atendendo àqueles países desejosos de comprar produtos de defesa do Brasil, e permitirá oferecer "garantias de Estado", por meio de um sistema facilitador do tipo, por exemplo, do FMS (Foreign Military Sales) norte-americano.

MEDIDA VIABILIZADORA 3.2 – "Desoneração da Folha de Pagamento" – Desoneração da folha de pagamento das empresas de defesa e segurança, visando dar maior proteção e competitividade ao setor que depende extraordinariamente de mão-de-obra especializada, aplicada em produtos com longos ciclos de desenvolvimentos, e que, em geral, não conta com encomendas regulares.

MEDIDA VIABILIZADORA 4.1 – "Orçamento Público" – Aperfeiçoamento da legislação orçamentaria (LRF – Lei de Responsabilidade Fiscal, PPA – Orçamento Plurianual de Investimentos, LDO – Lei de Diretrizes Orçamentarias e LOA – Lei Orçamentaria Anual) para permitir o comprometimento de recursos orçamentários de longa duração, plurianuais e em volumes compatíveis com as necessidades nacionais de investimento em programas de defesa e segurança. Migração

dos programas de investimento do Ministério da Defesa para os programas prioritários de Governo (como o PAC) garantindo, de imediato, o planejamento de longo prazo e a continuidade dos orçamentos.

MEDIDA VIABILIZADORA 4.2 – "Contra-Garantias" – Criação de mecanismos legais para o reconhecimento do acervo tecnológico das empresas de defesa e segurança como um bem a ser preservado e que possa ser oferecido em contra-garantia às operações financeiras ligadas ao Governo. A indústria de defesa e segurança é, acima de tudo, uma indústria do conhecimento, e o maior patrimônio das empresas é o conhecimento por elas acumulado.

Observação: tais garantias devem servir ao aparato público de financiamento, independente do cliente e do mercado final.

MEDIDA VIABILIZADORA 4.5 – "Continuidade dos Programas" – Criação de mecanismos legais garantidores da execução, financeira e física, e da continuidade dos programas de segurança e defesa, em níveis que garantam o atendimento das necessidades estratégicas nacionais e o fortalecimento da BID.

MEDIDA VIABILIZADORA 4.7 – "Crédito Especial para Ciência, Tecnologia e Inovação" – Criação de arcabouço legal e de mecanismos para a agilização do fornecimento de crédito para o financiamento de programas de interesse estratégico de defesa e segurança, com prazo alongado para sua utilização.

MEDIDA VIABILIZADORA C.5.1 – "Nível Superior – Formação e Aperfeiçoamento" – Ampliação dos esforços de formação, treinamento, especialização e reciclagem de recursos humanos para a área cibernética. Criação de estágios e cursos de nível superior e de pós-graduação, no País e no exterior, nas diversas especialidades necessárias ao projeto, pesquisa, desenvolvimento, inovação, produção e manutenção de produtos de defesa e segurança cibernéticas, aproveitando oportunidades como as oferecidas pelo Programa Ciência sem Fronteiras.

MEDIDAS PONTUAIS MP.5 - "Escola de Cibernética e Spin-Offs" - Criação de Escola Nacional de Cibernética, envolvendo a Academia (Universidades Federais, Estaduais), Empresas, Centros de Pesquisa e a Administração de forma a reunir competências teóricas, técnicas, operacionais e aplicadas. O currículo deve ser amplo em termos de tecnologias e áreas de conhecimento, focando a formação no desenvolvimento e na operação de soluções na área cibernética. Tal escola deverá incentivar, de forma coordenada com os instrumentos de fomento existentes e a serem criados, "spin-offs" (na forma de "start-ups") na área cibernética.

MEDIDA VIABILIZADORA 6.1 – "Projeto, Pesquisa e Desenvolvimento" – Atualização da Política de Ciência, Tecnologia e Inovação para a Defesa Nacional, sua aprovação pelo Legislativo Federal, e edição dos instrumentos normativos decorrentes. Investimentos em capacitação para defesa, por imposição dos países desenvolvidos, não estão sujeitos às regras restritivas da Organização Mundial do Comércio (OMC)

e, usados corretamente, podem se tornar importantes e eficazes instrumentos de política industrial.

MEDIDAS PONTUAIS MP.6 - "Garantias de Compras" – Criação de mecanismos que garantam a coordenação entre recursos de fomento e aquisições mínimas por parte do poder público, no modelo do FINEP INOVA Medicamentos. Garantias adicionais deverão ser providas para à micro e pequena empresa inovadora.

MEDIDA VIABILIZADORA MV.1 – "Monitoramento e Responsabilização na Cadeia Produtiva de Cibernética" – Criação de arcabouço legal, coordenado com um sistema de certificações e homologações, que estabeleça mecanismos de monitoramento dos atores envolvidos na cadeia produtiva de produtos sensíveis da área cibernética, incidindo essa responsabilização nas pessoas naturais, nas pessoas jurídicas envolvidas e na solidariedade entre elas.

MEDIDA VIABILIZADORA C.9.2 – "Homologação e Certificação" – Fortalecimento do sistema nacional de certificação e metrologia (SINMETRO), com a consequente redução dos períodos e dos custos para a homologação de produtos de defesa e segurança e para a certificação internacional dos produtos brasileiros. Concretização de acordos com outras nações para reconhecimento mútuo de tais certificações (por exemplo, a ISO/EIC 15.408 – "Common Criteria"), abrindo o mercado externo para produtos brasileiros.

MEDIDA VIABILIZADORA MV.2 – "Coordenador para a Área Cibernética" – Elevação ou criação de ente executivo para a área cibernética nos escopos civil e militar, com capacidade e autoridade para coordenar os esforços e programas na área.

Este é apenas o início de um longo trabalho de construção de uma segurança cibernética à altura de nossa importância geopolítica.

Senadora Vanessa Grazziotin (PCdoB-AM)

II. Manifestação do Ministro de Estado da Defesa, Celso Amorim, em audiência pública na Comissão de Relações Exteriores e Defesa Nacional, em 27 de março de 2014

"....

Bem, mas além de todas essas funções ligadas à defesa da Pátria e esses projetos e essa permanente luta para ter os recursos necessários, ainda que sempre compreendendo que o País tem também outras necessidades, nós temos que lidar com situações, de certa forma – não diria – imprevistas, mas cuja dimensão não era prevista. Uma delas é a questão da espionagem. O Senador conhece isso hoje em dia melhor do que todos nós, porque esteve muito envolvido na comissão sobre este tema, e

isso nos levou a buscar reforçar ainda mais o que já estava na estratégia nacional de defesa e que já vinha sendo implementado, que é a parte de defesa cibernética. Nós temos um centro de defesa cibernética que está a cargo do Exército, mas é claro que cada força também tem as suas ações nessa área e elas estão sendo coordenadas. E eu determinei, em função dessas questões de espionagem, que fosse feito um grupo de trabalho, que nos dessem recomendações mais imediatas. Na realidade, essas recomendações estão ainda sendo objeto de exame de como implementar. Há várias, mas eu vou salientar duas: uma é uma escola de defesa cibernética, que pode servir, inclusive, para outros órgãos da administração – aliás, queremos trabalhar com eles –, porque a questão de recursos humanos é absolutamente fundamental nesse campo, pois não adianta você ter o equipamento perfeito e ter que depender de uma empresa estrangeira para fazer a revisão, por exemplo. Então, é absolutamente fundamental entre parênteses entre os programas que nós temos apoiado, seja diretamente, seja em conjunto com o MCTI, num programa de nova defesa, tem estado sempre presente a questão de software adequado à defesa. Este é um aspecto: a escola. O outro aspecto – e já é uma coisa dentro do Exército, ainda sendo estudado, mas é importante que se saiba como passar de um centro para um comando de defesa cibernética.

....."

III. Malware da NSA encontrado – documento encaminhado à senadora Vanessa Grazziotin em 8 de abril de 2014

VirusImmune

http://twitter.com/virusimmune
contato@infovirus.com.br

Malware da NSA encontrado

A empresa de segurança de dados Virusimmune (www.virusimmune.com.br) anuncia a descoberta de três exemplares de malware da NSA (National Security Agency), direcionados exclusivamente ao governo brasileiro e empresas do Brasil:

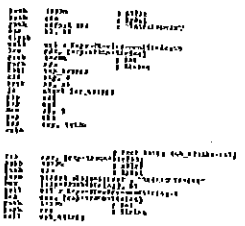
O funcionamento entre eles é muito semelhante e grande parte do código é comum, o que comprova que foram criados pela mesma pessoa ou grupo.

A seguir alguns detalhes:

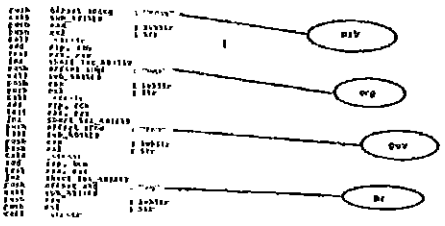
Informações	Exemplar 1	Exemplar 2	Exemplar 3
MD5	(Disponível para parceiros)	(Disponível para parceiros)	(Disponível para parceiros)
Tamanho do arquivo (em bytes)	102.400	172.032	45.056
Inicialização automática?	Não	Não	Não
Ícone	Não	Não	Não
Possui resources?	Não	Não	Não
Assinatura digital?	Não	Não	Não
Compactado?	Não	Não	Não
Strings criptografadas?	Sim	Sim	Sim
Data de compilação	09/05/2012	10/07/2012	01/08/2012
Leitura do Domínio/Workgroup	petr, org, gov, br	petr, org, gov, br	petr, org, org, gov, br
Arquivos que captura	'.doc', '.ppt', '.xls', 'pass', 'senha'.	'.doc', '.ppt', '.xls', 'pass', 'senha'.	
Método de envio dos arquivos	e-mail para NIASC@nsa.gov via porta 587 (email autenticado) Senha do email: ******* (Disponível para parceiros)	POST para um site na Ásia	Grava dados em um arquivo criptografado: %WINDIR%\windowsupdatereport.log
Keylogger	Não	Não	Sim

Funcionamento:

- Ao iniciar, o malware tenta ler o conteúdo das variáveis do ambiente: USERDOMAIN e LOGONSERVER, para tentar obter o nome do domínio e/ou workgroup:

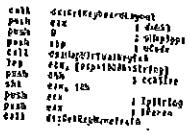


- Em seguida é feita uma checagem por um dos seguintes textos: "petr", "org", "gov" ou "br" (Exemplares 1 e 2) e também por "ong" (Exemplar 3):

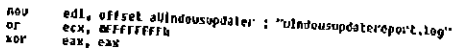


- Caso NÃO encontre nenhum dos textos, ele simplesmente sai do malware (isso dificulta a análise por analisadores automáticos de malware, pois os mesmos teriam que ler os nomes de domínio/workgroup com algum dos textos anteriores).

- Keylogger (Exemplar 3):

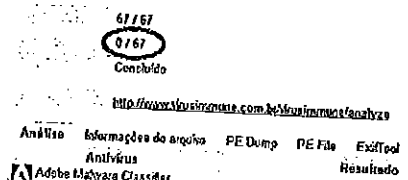


- O keylogger, grava tudo o que é digitado pelo usuário no arquivo %WINDIR%\windowsupdatereport.log em modo criptografado (Exemplar 3);



- Como o keylogger (exemplar 3) não possui qualquer tipo de método de envio do arquivo, existe a possibilidade de algum outro módulo ler este arquivo e envia-lo para um site, FTP ou email.
- Após todas as unidades serem checadas, ele encerra o malware.

Do acordo com a análise feita pelo site www.virusImmune.com.br, nenhum dos 67 antivirus disponíveis na época detectaram qualquer tipo de infecção no arquivo:



Conclusões:

- Pelas características dos exemplares e pela falta de código de inicialização automática, acreditamos que existam módulos específicos que façam a execução dos mesmos. Possivelmente um módulo central que execute os mesmos através de comandos, controle a segurança, faça o controle dos mesmos contra firewalls e etc;
- Os exemplares foram desenvolvidos com intenção de ataque específico e direcionado, como pode ser determinado pelos textos encontrados: petr, gov, org, br;
- A dificuldade em ter o domínio/workgroup com os textos específicos, reduz a chance de um analisador automático de malware identificar os exemplares, necessitando fazer análise manual;
- Após a identificação dos três exemplares pelas empresas de antivirus, possivelmente serão encontrados outros com padrões semelhantes.
- Os três exemplares foram enviados para o site www.virusimmune.com.br em dias diferentes, mas pela mesma fonte, um IP localizado em Nova York (EUA) - (Disponível para parceiros);
- As redes do Governo e das empresas estatais precisam urgentemente de uma checagem minuciosa para identificar outros possíveis problemas/exemplares que devem existir;
- Lembramos que não basta ter uma solução de antivirus instalada, pois nenhum identificou os exemplares. A solução do problema requer conhecimento profundo de arquivos e análise de malware para que seja feita uma pesquisa avançada.

Sala das Sessões,

Senador **RICARDO FERRAÇO**

SENADO FEDERAL
SECRETARIA DE COMISSÕES

Reunião:15ª Reunião da CPIDAESP
Data: 09 de abril de 2014 (quarta-feira), às 14 horas
Local: Ala Senador Alexandre Costa, Plenário nº 13
CPI DA ESPIONAGEM - CPIDAESP

Assinam o Relatório:

TITULARES	SUPLENTES
Bloco Parlamentar da Maioria(PV, PSD, PMDB, PP)	
VAGO	1. Eunício Oliveira (PMDB)
Ricardo Ferraço (PMDB)	2. VAGO
Benedito de Lira (PP)	3. VAGO
Sérgio Petecão (PSD)	
Bloco de Apoio ao Governo(PSOL, PT, PDT, PSB, PCdoB)	
Vanessa Grazziotin (PCdoB)	1. Eduardo Suplicy (PT)
Walter Pinheiro (PT)	2. Lídice da Mata (PSB)
Anibal Diniz (PT)	
Bloco Parlamentar Minoria(PSDB, DEM)	
Pedro Taques (PDT)	1. VAGO
VAGO	
Bloco Parlamentar União e Força(PTB, PRB, PSC, PR)	
Eduardo Amorim (PSC)	1. Antonio Carlos Rodrigues (PR)
VAGO	