SENADO FEDERAL
Gabinete do Senador **ESPERIDIÃO AMIN**

Avaliação de Políticas Públicas
(Resolução nº 44, de 2013)

Proposta de Plano de Trabalho

Avaliação da Política Nacional de Cibersegurança

Presidente: Senador **RENAN CALHEIROS**

Vice-Presidente: Senador **CID GOMES**

Relator: Senador **ESPERIDIÃO AMIN**

1. APRESENTAÇÃO

A avaliação de políticas públicas tem como objetivo principal aprimorar a gestão do Estado, por meio da mensuração de sua eficiência, eficácia e efetividade. O resultado da avaliação é fundamental para orientar as ações do Poder Público.

A Resolução do Senado Federal n° 44, de 2013, prevê que a Casa Legislativa realize a avaliação de políticas públicas, que buscará, entre outras medidas, adequar os dispositivos normativos às necessidades sociais.

Nos termos do art. 1º dessa normativa, "as comissões permanentes selecionarão, na área de sua competência, políticas públicas desenvolvidas no âmbito do Poder Executivo, para serem avaliadas".

Mediante a aprovação, no dia 25 de abril de 2024, do Requerimento nº 6, de 2024, a Comissão de Relações Exteriores e Defesa Nacional (CRE) decidiu avaliar a Política Nacional de Cibersegurança, o que será impulsionado no âmbito da Subcomissão Permanente de Defesa Cibernética, instalada no dia 14 de maio de 2024.

No Brasil, os assuntos relacionados às vulnerabilidades digitais foram tratados, inicialmente, sob a égide da Segurança da Informação, pelo Decreto nº 3.505, de 2000, que instituiu a Política de Segurança da Informação, que foi revogado pelo Decreto nº 9.637, de 2018 (alterado pelo Decreto nº 9.832, de 2019; Decreto nº 10.631, de 2021; Decreto nº 10.641, de 2021; Decreto nº 10.849, de 2021; Decreto nº 11.856, de 2023).

O Decreto nº 10.222, de 2020, aprovou a Estratégia Nacional de Segurança Cibernética, válida para o quadriênio 2020-2023. Por fim, o Decreto nº 11.856, de 2023, instituiu a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Importa ressaltar que a Política Nacional de Cibersegurança envolve a Estratégia Nacional de Segurança Cibernética e o Plano Nacional de Cibersegurança. Já o Comitê Nacional de Cibersegurança foi criado no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, com a finalidade de acompanhar a implementação e a evolução da Política Nacional de Cibersegurança. Estes serão os pontos centrais de atenção para a avaliação da política pública em questão.

No âmbito da Defesa, o denominado Setor Cibernético foi destacado pela Estratégia Nacional de Defesa (END), aprovada pelo Decreto

nº 6.703, de 2008, e considerado, ao lado do setor espacial e do setor nuclear, como um dos três setores estratégicos e essenciais para a Defesa Nacional. Desde então, o setor tem sido contemplado em destaque pelas demais Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END) formuladas. Pela Portaria Normativa nº 3.010/MD, de 18 de novembro de 2014, foi aprovada a Doutrina Militar de Defesa Cibernética, substituída pela nova doutrina, expressa na Portaria GM-MD n° 5.081, de 16 de outubro de 2023.

O interesse da Casa por esse tema não é novo. Em 2013, o Senado Federal instaurou uma Comissão Parlamentar de Inquérito (CPI) destinada a "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".

Na Câmara dos Deputados, em 2015, também foi instaurada Comissão Parlamentar de Inquérito (CPI), destinada a *"investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país"*, para qual fui designado relator. O relatório final da CPI concluiu pela apresentação de cinco projetos de lei para aprimorar a legislação e tipificações penais relacionadas aos crimes cibernéticos, além disso, o trabalho também recomendou ao Executivo a adoção de diversas medidas para melhorar a segurança da infraestrutura de tecnologia da informação na Administração Pública.

De todos os projetos apresentados pela CPI, somente um ainda tramita, o PL nº 5200, de 2016, que tem como escopo a *ampliação da abrangência do crime de invasão de dispositivo informático*. A proposição foi aprovada na CCJ em agosto de 2018 e, desde então, aguarda análise da Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados. O projeto segue apensado a outros 21 projetos de lei. Os demais projetos foram arquivados em 2019, em decorrência do fim da legislatura. Por fim, a CPI também recomendou a aprovação de vários projetos que foram considerados pertinentes por preencherem lagunas legais verificadas durante os trabalhos.

Desses projetos, cinco ainda tramitam na Câmara dos Deputados e o PL nº 2801, de 2022, que já foi aprovado naquela Casa irmã, encontra-se na CCJ, do Senado, aonde aguarda designação de relator. A proposta *aumenta a pena dos crimes contra a dignidade sexual de crianças e adolescentes* que envolvam, inclusive, o uso de qualquer meio de comunicação de massa ou sistema de informática ou telemática, dentre outros.

Em 2019, a Comissão de Relações Exteriores avaliou a política sobre defesa cibernética, da qual tive a oportunidade de relatar e, como um dos resultados, justamente provocou a criação dessa Comissão da Subcomissão Permanente de Defesa Cibernética.

Conforme levantamento divulgado pela empresa de soluções de cibersegurança FORTINET, com base dos dados do FortiGuard Labs, o Brasil foi o segundo país mais atingido da América Latina e Caribe em 2022,

com 103,16 bilhões de tentativas de ataques cibernéticos. O número implica aumento de 16% com relação ao ano anterior (88,5 bilhões) e representa quase 30% do número total dos países da região que sofreram com mais de 360 bilhões de tentativas de ciberataques.

Não podemos nos omitir de enfrentar esse tema com o cuidado que ele merece. Por uma omissão, perde-se um aviso, por um aviso, perde-se uma ocasião, por uma ocasião perde-se um negócio, por um negócio perde-se um reino.

Analisando-se o cenário regional latino-americano, deve ser também objeto de preocupação por parte desta Casa o ataque perpetrado contra os bancos de dados do Ministério das Finanças da Costa Rica e de outras instituições públicas do país, em 12 de abril de 2022, o que levou à declaração do "Estado de Emergência Nacional em todo o setor público do Estado da Costa Rica".

É evidente que organizações transnacionais do crime organizado são ameaças concretas não somente à estabilidade da região, como também do Brasil, uma vez que suas estratégias e métodos, embora diferentes na busca de seus objetivos, baseiam-se na aplicação limitada de boas práticas e padrões de cibersegurança nos níveis empresarial e estatal.

De acordo com a Cybersecurity Ventures, o crime cibernético deve custar ao mundo US$ 9,5 trilhões em 2024. Se fosse um país, o crime cibernético seria a terceira maior economia do mundo.

No âmbito das relações internacionais, avaliar as iniciativas do Ministério das Relações Exteriores nesse campo, portanto, é de suma importância. É fundamental avaliar a participação do país em fóruns internacionais, redes de partilha de informações, exercícios conjuntos e esforços de investigação colaborativa. Tais atividades não apenas fortalecem a capacidade nacional de resposta às ameaças cibernéticas, mas também promovem normas globais de segurança cibernética, contribuindo para um ambiente digital mais seguro e resiliente.

Nesse contexto, entre 10 e 12 de abril de 2024, tive a felicidade de ir ao Panamá representar o Brasil na I Conferência STIC de Cibersegurança promovida pelo Governo da Espanha e apoiada pela Organização dos Estados Americanos - OEA e pelo Banco de Desenvolvimento Interamericano - BID.

Nesse evento, foi concordada entre os principais especialistas e profissionais de cibersegurança, bem como entre os Senadores e parlamentares ibero-americanos, a necessidade de formar uma “Bancada Digital", como forma de preparação de uma futura convenção que abranja medidas de interesse coletivo para a cibersegurança. Assim, foi aceito e adotado pelos participantes o mote por mim sugerido, baseado em conceito matemático do MDC: “Mínimo Denominador Comum” que, em breve resumo, se revestiria na busca pelo desenvolvimento de uma legislação convergente entre países da América Latina sobre o tema.

As iniciativas de cibersegurança existentes na área de inteligência também merecem atenção especial dessa avaliação de política pública.

No âmbito da Agência Brasileira de Inteligência (ABIN), dada a competência do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC) em áreas cruciais como tecnologia da informação, inteligência cibernética e segurança de dados, conforme o art. 7º, do Decreto nº 11.816, de 6 de dezembro de 2023, sua liderança tem um entendimento profundo das necessidades do País e dos desafios por nós enfrentados. Haja vista sua experiência em questões de segurança nacional e estratégias de combate a ameaças cibernéticas, a participação da ABIN nessa avaliação de política, como principal órgão responsável pela Inteligência brasileira, é, de igual modo, fundamental.

Desse modo, o CEPESC-ABIN pode oferecer percepções valiosas e contribuir significativamente para o aprimoramento das políticas públicas relacionadas à cibersegurança, fortalecendo a defesa digital do País e protegendo os seus interesses estratégicos.

Não se pode olvidar da dimensão humana que essa avaliação também carrega em seu âmago.

Avaliar os esforços nacionais na construção de uma força de trabalho capacitada em segurança cibernética é fundamental, seja por meio de programas educacionais, de treinamento ou de desenvolvimento profissional. É crucial dispor de um conjunto robusto de talentos para atender

à crescente demanda por *expertise* em segurança cibernética. Este exame pressupõe a análise das iniciativas das estruturas da administração pública para fazer frente a essas novas ameaças, bem como a reflexão sobre como o Congresso pode atuar para que uma nova geração de talentos capacitada surja e seja, ao mesmo tempo, retida em território nacional. Com efeito, a fuga de cérebros em busca de melhores condições de vida dificulta a retenção de profissionais qualificados em cibersegurança. Cumpre analisar o orçamento de investimentos em Pesquisa e Desenvolvimento, além de iniciativas promovidas pelo Ministério da Educação e pelo Ministério da Ciência, Tecnologia e Inovação, na área, até o momento.

Assim, essa avaliação de política proposta pela CRE constitui importante e valioso instrumento para, a partir das análises a serem realizadas, retificar ou ratificar os planejamentos para a cibersegurança no País, sem desconectá-la da defesa cibernética. Reconhecemos que tais elementos podem indicar diferentes níveis de desenvolvimento da sociedade em termos de segurança cibernética, sendo essencial compreendermos como abordar essas questões para promovermos um ambiente digital mais seguro e resiliente.

Diante da relevância e considerando a transversalidade do setor cibernético para a segurança e a defesa do País, as perguntas que a presente avaliação de políticas públicas buscará responder são:

1) Como se encontra o diálogo institucional entre segurança e defesa cibernética no País?

2) Qual razão de o Poder Executivo não ter enviado o projeto de lei que instituiria a Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança (SNCiber)?

3) Necessitamos de uma Agência Nacional de Cibersegurança?

4) A falta de um órgão coordenador da segurança cibernética implica diferentes níveis de maturidade cibernética entre os entes públicos?

5) Os atuais instrumentos jurídicos sobre o setor de cibersegurança foram efetivamente implementados? Eles são eficazes?

6) Qual a participação do País em fóruns internacionais, redes de partilha de informações, exercícios conjuntos e esforços de investigação colaborativa em cibersegurança?

7) O que o Congresso Nacional tem feito e pode fazer para a melhora legislativa e de controle no setor de cibersegurança?

8) Qual o grau de capital humano existente em cibersegurança, quais iniciativas o governo empreende para que essa força de trabalho seja formada e o que o Congresso pode fazer para o aprimoramento legislativo nessa dimensão?

9) Qual o nível de interoperabilidade dos órgãos e agência governamentais no campo cibernético?

10) Qual o grau de independência tecnológica do Brasil no campo?

11) Qual tem sido o grau do desenvolvimento da cultura e dos conhecimentos tecnológicos acentuadamente úteis na sociedade?

2. ATIVIDADES PROPOSTAS

Para levar a contento a avaliação desses instrumentos, sugere-se que a CRE segmente suas análises em cada um deles, para os quais são previstas as seguintes ações:

- Solicitar informações Gabinete de Segurança Institucional da Presidência da República sobre as medidas que estão sendo implementadas;
- Convidar o Ministro do Gabinete de Segurança Institucional da Presidência da República para audiência pública;
- Convidar a chefia do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações da

Agência Brasileira de Inteligência (CEPESC-ABIN) para audiência reservada.

- Convidar a chefia do Departamento de Assuntos Estratégicos, de Defesa e de Desarmamento do Ministério das Relações Exteriores (MRE) para expor as iniciativas e diretrizes de política externa do Brasil em temas relacionados à segurança cibernética, inclusive, a interação entre os legislativos dos países do Mercosul objetivando um Marco Legal continental, a exemplo da União Europeia;
- Convidar o Comando do Exército, por intermédio do Comando de Defesa Cibernética (ComDCiber), para tratar do relacionamento desejável com o setor de segurança cibernética;
- Identificar atores sociais e agentes econômicos relacionados ao tema, convidando-os para audiência pública;
- Compilar projetos em trâmite no Congresso Nacional sobre o assunto;

Com base nessas atividades, será elaborado o relatório final para apreciação pela Comissão até novembro deste ano.

3. PROGRAMAÇÃO

Propomos a seguinte programação para o trabalho de avaliação desses instrumentos:

Atividade	Local	Convidados	Temas
1) Reunião de instalação dos trabalhos	Brasília	Membros da Subcomissão Permanente de Defesa Cibernética	Apresentação e debate do plano de trabalho
2) Reuniões técnicas	Brasília	Senadores e assessorias	Reunião interna: avaliação dos trabalhos e calibragem de cronogramas. Definição de datas para as audiências públicas.
4) Audiência Reservada com Membros da CRE	Brasília	- Ministério da Defesa; - Gabinete de Segurança Institucional da Presidência da República; - Comando do Exército, da Marinha e da Força Aérea; - Ministério das Relações Exteriores; - Ministério da Justiça. - Agência Brasileira de Inteligência	I - Diagnóstico de ameaças sensíveis do setor cibernético e gargalos do Estado para implementar uma política de Segurança e Defesa Cibernética, com foco: 1) na definição de marcos legais; 2) no fortalecimento da estratégia de superação dos gargalos verificados; II – Avaliação da efetividade de colaboradores nacionais e internacionais, identificando medidas necessárias para a obtenção de resultados.
5) Três Audiências Públicas	Brasília	1ª) Órgãos públicos: - Ministério da Defesa; - Gabinete de Segurança Institucional da Presidência da República; - Comandos do Exército, da Marinha e da Força Aérea. 2ª) Representantes da sociedade civil	I – Política Nacional de Cibersegurança: Estratégia Nacional de Segurança Cibernética e Plano Nacional de Cibersegurança II – Relações entre Segurança e Defesa Cibernética III – Anteprojeto de lei sobre Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança (SNCiber).
6) Visitas Técnicas	Brasília	Membros da CRE	I – Identificação das instalações do ComDCiber e ferramentas utilizadas; II – Análise dos gargalos para a implementação das infraestruturas adequadas aos cenários de curto, médio e longo prazos.
Apresentação e Votação do Relatório Final (NOVEMBRO DE 2024)			

Sala da Comissão,

, Presidente

, Relator