SENADO FEDERAL
SECRETARIA-GERAL DA MESA
SECRETARIA DE REGISTRO E REDAÇÃO PARLAMENTAR

REUNIÃO
30/06/2026 - 22ª - Comissão de Ciência, Tecnologia, Inovação e Informática

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC. Fala da Presidência.) - Bom dia a todos.

Havendo número regimental, declaro aberta a 22ª Reunião da Comissão de Ciência, Tecnologia, Inovação e Informática da 4ª Sessão Legislativa da 57ª Legislatura, que se realiza nesta data, 30 de junho de 2026.

A presente reunião será dividida em duas partes: a primeira deliberativa e, na sequência, audiência pública interativa.

Passamos à primeira parte, destinada à deliberação do Requerimento 50, de 2026, da CCT, de nossa autoria.

Passo à leitura do requerimento.

Requeiro, nos termos do art. 93, inciso I, do Regimento Interno do Senado Federal, que, na audiência pública objeto do Requerimento 18, de 2026, com o objetivo de instruir o PL 4.752, que institui o Marco Legal da Cibersegurança, cria o Programa Nacional de Segurança e Resiliência Digital e altera a Lei nº 13.756, de 12 de dezembro de 2018 sejam incluídos os seguintes convidados: o Sr. Vinícius Malacco, Especialista em Cibersegurança da Tokio Marine; e a Sra. Luana Tavares, representante da Aliança Multissetorial pela Cibersegurança Nacional e do Instituto Nacional de Combate ao Cibercrime.

Em votação o requerimento.

Os Senadores que concordam com o requerimento permaneçam como se encontram. *(Pausa.)*

Aprovado.

Está concluída a parte deliberativa da sessão.

Declaro aberta a segunda parte da reunião, destinada à realização de audiência pública com o objetivo de instruir o PL 4.752, de 2025, que institui o Marco Legal da Cibersegurança, cria o Programa Nacional de Segurança e Resiliência Digital e altera a Lei 13.756, de 12 de dezembro de 2018, em atenção aos requerimentos desta Comissão nºs 18, 40, 42, 44, 45, 46, 47 e 50, todos de 2026.

Participarão presencialmente, e os convido para tomarem lugar nas primeiras filas, os Srs. Jacy Barbosa Junior, General de Divisão do Comando de Defesa Cibernética do Ministério da Defesa; Marcelo Antonio Malagutti, Secretário-Executivo do Comitê Nacional de Cibersegurança - vamos uniformizar, eu mesmo já me contradisse aqui, eu vou usar cibersegurança, em português -; Demi Getschko, Diretor-Presidente do Núcleo de Informação e Coordenação do Ponto BR (NIC.br); Rodrigo Pereira Pacheco, Diretor Substituto do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações da Agência Brasileira de Inteligência (Cepesc/Abin); Rodrigo Jonas Fragola, Vice-Presidente de Articulação Política da Confederação das Associações das Empresas Brasileiras de Tecnologia da Informação; Luiz Henrique Barbosa, Presidente Executivo da Associação Brasileira das Prestadoras de Serviços de Telecomunicações Competitivas (TelComp); Luca Belli, Professor da Fundação Getulio Vargas Rio Direito, Coordenador do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas; Belisario Contreras, que vai falar em português hoje aqui, Diretor-Executivo da Digi Americas Alliance - até porque já completou o estágio, fez o exame de admissão, foi aprovado, hoje vai mostrar que foi aprovado de verdade. Mas serão tolerados alguns toques latinos. Nós estamos nos habituando com o treinador da Seleção Brasileira, de forma que pode falar qualquer língua aí que nós vamos entender -; Patricia Peck, Presidente do Instituto Peck de Cidadania Digital e integrante titular do Instituto Empoderar; Marta Helena Schuh

- pronunciei certo? -, Diretora de Seguros Cibernéticos da Howden Brasil; Patrick Aron Rinski, Diretor-Executivo da Unidade 42 da Palo Alto Networks; e Rodrigo Marinho, CEO do Instituto Livre Mercado e editor em geral.

Participarão, por meio de videoconferência, os seguintes convidados: Rony Vainzof, Diretor Titular da Divisão de Cibersegurança da Federação das Indústrias do Estado de São Paulo (Fiesp) e Consultor em Proteção de Dados da Fecomercio, São Paulo; Luana de Brito Tavares Diniz, fundadora e CEO do Instituto Nacional de Combate ao Cibercrime (INCC); Vinícius Malacco Ferreira, Gerente de Subscrição de Linhas Financeiras da Tokio Marine Seguradora.

Antes de passar a palavra aos nossos convidados, eu comunico que esta reunião será interativa, transmitida ao vivo e aberta à participação dos interessados por meio do Portal e-Cidadania, na internet, no endereço senado.leg.br/ecidadania, ou pelo telefone 0800 0612211.

O relatório completo, com todas as manifestações, estará disponível no portal, assim como as apresentações que forem utilizadas pelos expositores.

Como percebem, aqui eu entro num particular de autorregulação do nosso tempo e da nossa produtividade e da nossa eficiência.

Estou aqui ladeado pelo Senador Hermes Klann, que, em verdade, é o Relator de fato do projeto. Portanto, ele hoje será o recipiendário, está certo? Que é a versão legal do receptor, aliás, do receptador. Ele vai receber o quê? As contribuições para que ele, na condição de Relator em exercício, e o Relator efetivo, que é o Senador Jorge Seif, que está em período de licença, mas ainda assim contribui com a sua presença - pelo que nós ambos agradecemos muito, e o Senado agradece, porque com isso nós otimizaremos o aproveitamento das contribuições.

Então, nós vamos ter que nos restringir ao verdadeiro objeto desta sessão. O objeto desta sessão não é apresentar um projeto. O projeto já foi apresentado, já houve audiências públicas. Esta parte eu acho que cumpri com razoável exação, posto que me dei ao trabalho de analisar todas as críticas, positivas e negativas - e, neste primeiro momento, contei com a contribuição do Delegado Diego Araújo e do nosso amigo Eduardo Siqueira, especialmente estes dois.

Na média, as críticas feitas foram de que o projeto tinha o essencial. Agora, todos sabemos que este é um tema sensível por natureza, e mais sensível ainda pela evolução dos fatos - o que era perigoso há dois meses, hoje pode inexistir, ou pode ter surgido algo novo, ou pode ter evoluído dramaticamente. Então, vai ser muito difícil transformar este projeto numa estátua. Ele será sempre irresignado com a paralisia, ele vai sempre se mexer. E nós temos que dar a ele corpo para que tramite, então nós temos que equilibrar sugestões com o espírito do projeto e com a tramitação legislativa. Isso não é uma tramitação de gabinete de pesquisa, que surgiu, defendeu, passa a ser operacionalizada. Não é assim; é um processo legiferante - nós estamos construindo uma lei. De sorte que, da maneira mais cordial possível, eu repito: nós todos queremos aprender, mas hoje nós queremos colher sugestões, se possível com o apoio da Consultoria Legislativa prévio ou posterior, que dá forma ao texto da lei e das suas emendas. Temos que seguir a Lei Complementar 95, de 1998, que fala o quê? Sobre legística. Temos que seguir o princípio de querer fazer uma lei boa, ou uma boa lei, no sentido formal da palavra.

De sorte que, eu consulto se podemos fixar um prazo limite. Claro que não existe limite no sentido de interromper o que se está falando, mas nós temos que pôr um limite - são 15 participantes, se cada um ocupar cinco minutos, vai dar 75 minutos. Se cada um ocupar três, dentro do possível, teremos 45 minutos. Eventuais necessidades de mais tempo...

(Soa a campainha.)

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) - Ó, eu também estou estourando *(Risos.)*, mas é para economizar. Estou gastando para economizar.

Vamos fixar em três minutos, e o Presidente - e tanto poderei ser eu no início quanto o Senador Hermes, que aqui representa o mandato do Senador Seif -, nos conduziremos com a maior polidez possível, mas com o objetivo de colher sugestões. Então fica estabelecido em três minutos.

A palavra será concedida de forma alternada entre os convidados que participam presencialmente e de modo remoto. Ao final das exposições, a palavra será concedida aos Parlamentares inscritos para fazerem suas perguntas ou comentários.

Então, passo a palavra ao eminente General Jacy Barbosa Junior, do Comando de Defesa Cibernética do Ministério da Defesa - não é do Comando de Defesa Cibernética do Exército, ou seja, não é no Forte Marechal Rondon, é na estrutura do Ministério da Defesa.

Está concedida a palavra ao senhor.

Vou mudar de lugar.

Passo a Presidência para o Senador Hermes e permanecerei aqui.

O SR. JACY BARBOSA JUNIOR (Para expor.) - Prezado Senador Hermes, prezado Senador Esperidião Amin, prezado Senador Jorge Seif, em suas pessoas eu cumprimento todos os presentes. Agradeço, em nome do Ministério da Defesa, em nome do Comando de Defesa Cibernética, a oportunidade de conversarmos sobre um assunto que é muito caro para a Defesa: segurança cibernética, que é uma das grandes preocupações hoje, em qualquer lugar do mundo, e não é diferente nem no Ministério da Defesa, nem no Comando de Defesa Cibernética ou no Exército.

Antes de mais nada, falando sobre o projeto de lei, dentro dos três minutos que me deram, a primeira coisa que eu gostaria de dizer - e eu coloquei alguns eslaides justamente para que nós não perdêssemos tempo - é que essa iniciativa é excelente, urgente e já estamos há bastante tempo nessa discussão. Eu acredito que o Ministério da Defesa tem todo o interesse em que esse projeto siga em frente. Ele preenche uma lacuna muito relevante no nosso ordenamento jurídico e está alinhado com as melhores práticas do mundo - nós vamos olhar, e o próprio Malagutti vai mostrar alguma coisa sobre isso -, está alinhado com o que existe de melhor no mundo em termos de legislação.

O que eu gostaria de... Acho que eu vou... Primeiro, eu sempre tenho o benefício da dúvida. Isto.

Passou um.

Quando nós falamos de ataques cibernéticos - é importante frisar e é essa a visão da Defesa -, muitas vezes, podem começar, e normalmente começam com motivação financeira, mas não é o único momento ou não é a única forma de isso acontecer. Então, na verdade, eles podem partir para a busca de segredos industriais, para segredos de Estado, para promover o caos social e tem uma série de outras motivações que, muitas vezes, escapam do dia a dia comum do cidadão. Quando eles se tornam um problema de defesa? Quando eles afetam serviços essenciais ou infraestruturas críticas. E é sempre neste momento em que a gente olha - a Defesa olha - com um olhar diferenciado, lembrando que atualmente todas as grandes nações, todos os países têm, em suas doutrinas, o ataque cibernético como uma de suas armas. Então nós não podemos nos esquecer disso.

Indo direto ao ponto, as principais considerações sobre o PL são que nos parece que falta uma diferenciação clara entre cibersegurança e ciberdefesa - ou defesa cibernética. Esse é um ponto que eu gostaria de colocar porque isso tem um impacto muito grande, particularmente no próximo ponto, inclusive, que a gente coloca lá, sobre a ambiguidade de competências, e porque nós temos o problema de, muitas vezes, nós termos outros atores que precisam atuar, não apenas a autoridade nacional de cibernética que se pretende criar, a qual nós julgamos extremamente importante que seja criada.

(Soa a campainha.)

O SR. JACY BARBOSA JUNIOR - Mas, quando você tem alguma ambiguidade de competências, nós podemos ter problemas sérios. O próprio conselho nacional de cibersegurança fez uma proposta submetida a esta Casa em que tem uma separação bastante interessante, nós julgamos.

O outro ponto a ser colocado em relação às nossas contribuições é a questão de compartilhamento de informações. Cibersegurança se faz com compartilhamento de informações; tratamento de incidente se faz com compartilhamento de informações. Então é importante que isso seja colocado, e isso vem sendo colocado como uma atividade necessária. E nós julgamos... A própria proposta que nós vimos coloca esse ponto, e a nossa preocupação passa por quando as informações a serem trocadas ou a obrigatoriedade dessas informações possam expor vulnerabilidades de infraestruturas críticas ou vulnerabilidades de serviços essenciais, por que isso, esse assunto, tem que ser tratado de uma forma bastante pormenorizada na lei para evitar uma obrigatoriedade de expor uma infraestrutura crítica nossa.

E o último ponto que eu gostaria de colocar é a questão de ter indicadores objetivos de quando deixa de ser um problema de segurança e passa a ser um problema de defesa. Se nós não tivermos na lei algum direcionamento em relação a isso, a gente pode ter conflito de competências - e a gente volta ao primeiro ponto.

Inclusive, eu coloquei uma proposta de níveis de incidentes cibernéticos com gradações e com termos basicamente simples, para que a gente possa entender a diferença entre o que é um incidente técnico, que vai ser resolvido pelo próprio pessoal de TI do órgão; o que é um incidente de relevância nacional, onde você não compromete infraestruturas críticas; o que é um incidente de uma crise cibernética que pode ter impacto sistêmico, e aí você tem um problema de resiliência de Estado. Quando você tem uma degradação de infraestruturas críticas de interesse da Defesa, onde efetivamente você precisa mobilização da Defesa, o GSI e outros órgãos, você tem um problema interministerial para resolver; e também, quando você tem efetivamente um ataque ao Estado, uma ameaça à soberania, isso são índices, são períodos diferentes que fazem com que você tenha respostas diferentes.

A proposta, então, seria que alguma coisa nesse sentido nós pudéssemos agregar à lei em si.

Bom, acredito que, fechando, apenas gostaria de colocar aqui - e aí já não mais como na parte de defesa, mas porque são assuntos caros à defesa, que a gente julga interessante estarem de alguma forma abordados na lei - sobre falarmos

explicitamente sobre as tecnologias computacionais emergentes - IA, tecnologias quânticas -, porque elas já se tornaram assunto de Estado em muitos países, já se tornaram elementos de...

Talvez fosse uma oportunidade de a gente começar a regular essa parte também. Estimular o fomento de soluções nacionais, isso é do interesse total da defesa, justamente por haver essa preocupação com as tecnologias emergentes, particularmente nós termos autonomia em relação ao desenvolvimento disso é do nosso interesse. E a criação de uma plataforma neutra para compartilhamento de ameaças, onde a gente conseguisse efetivamente fazer essa troca de informações de uma maneira simples e segura. Esses são aspectos de bastante relevância, que a gente acredita como oportunidade para a Defesa.

Fechando o meu tempo - eu acredito que eu tenho 50 segundos -, só gostaria de colocar o que a Defesa tem feito nesse período já em relação a essa questão de cibersegurança. Eu coloco aqui o Exercício Guardião Cibernético, que é uma atividade que nós realizamos já há quase uma década, onde nós colocamos, fazemos exercícios de simulação constitutiva e virtual, onde discutimos problemas de impacto estratégico - certo? -, particularmente em relação a serviços essenciais e infraestruturas críticas. Então, acredito que esse tipo de discussão é mais do que uma melhoria técnica, ele dá melhoria institucional para as atividades. Nós o estamos realizando anualmente, neste ano vamos realizá-lo em setembro. Já aproveito aqui a oportunidade para convidar a todos para assistir à atividade que será aqui em Brasília, e nós teremos ainda em outras seis cidades, sendo conduzidas em paralelo.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC. *Fora do microfone*.) - Quando é que vai ser?

O SR. JACY BARBOSA JUNIOR - De 21 a 25 de setembro.

Bom, senhores, em relação à minha participação, seriam essas as contribuições que o Ministério da Defesa gostaria de apresentar.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado.

Eu quero registrar e agradecer a presença do nosso Senador Astronauta Marcos Pontes.

E quero passar agora a palavra para o nosso Senador Jorge Seif, em seguida, ao Sr. Marcelo.

O SR. JORGE SEIF JÚNIOR - Sr. Presidente, Sras. e Srs. Parlamentares, convidados, especialistas e todos que acompanham esta audiência, quero inicialmente agradecer a presença de todos e destacar a importância deste momento para aprimoramento do Projeto de Lei 4.752, de 2025, que institui o Marco Legal da Cibersegurança.

Embora temporariamente licenciado, continuo acompanhando de perto a construção dessa matéria e sigo plenamente comprometido com a elaboração do relatório. Trata-se de um tema que exige diálogo, responsabilidade e, sobretudo, a capacidade de reunir diferentes visões para construir uma legislação sólida e preparada para os desafios do presente e do futuro.

Eu vejo aqui muitos amigos que ao longo desses dois, três anos têm acompanhado a nossa luta e quero dizer a vocês que é um projeto de lei que está sendo construído a várias mãos. Para que os senhores saibam, viajamos, fizemos missões por vários países, visitamos várias instituições. Posso mencionar aqui o Senador Amin, Senador Marcos Pontes, Senador Sergio Moro e outras pessoas que, junto conosco, têm contribuído e participado para que façamos um marco legal que, ao mesmo tempo, consiga proteger a infraestrutura e contemple realmente a cibersegurança no Brasil e, por outro lado, não engesse, não impeça a inovação da nossa nação. Isso é um grande desafio.

E para que vocês saibam, o meu objetivo...

Temporariamente o Senador Hermes Klann, gentilmente, está de Relator desse projeto, justamente por conta do meu afastamento. Mas temos consultado, inclusive, aqui a Consultoria Legislativa do Senado, porque o meu objetivo é transformar essa legislação numa legislação viva. O Senador Esperidião Amin comentou, no início já de sua fala, que nós estamos tentando fazer uma estátua. Mas, como ele também comentou, os problemas, os desafios, as novas ameaças cibernéticas, etc., são diárias, são contínuas, são vivas, são organismos vivos.

Por isso, para que vocês entendam a importância da participação das senhoras e dos senhores, o que nós queremos fazer - e já conversei, inclusive na minha última viagem, com o Senador Marcos Pontes - é colocar, por exemplo, nessa legislação, de alguma forma, os *frameworks* internacionais sobre segurança e padrões para cyber, como o Nist, o RMF, o ISO 27000, o CIS, o ASP, e o Saif - que parece que é meu homônimo, mas não é -, é Security AI Agent, de forma que essa legislação não fique engessada, impedindo que nós, como país, como nação, fiquemos obsoletos ou defasados diante das ameaças que nós podemos sofrer no futuro.

Outra questão importante é, ao nós vermos outras nações, outros continentes, que já tem uma legislação dessa aprovada. No entanto, o Brasil parece estar um pouco atrasado, mas os erros dessas legislações de outros países acabam nos ensinando

muito. Nós temos estudado, inclusive, alguns exageros da lei europeia, da lei asiática, da lei americana, e podemos aprender com os erros de colegas internacionais, de outros países, de outras nações, para que nossa legislação fique o mais moderna, contemplativa e viva possível.

Para finalizar a minha fala, a transformação digital trouxe enormes avanços para a sociedade e também ampliou a nossa exposição a riscos cada vez mais sofisticados. Ataques cibernéticos, órgãos públicos, empresas, instituições financeiras, serviços essenciais, demonstram que a cibersegurança deixou de ser uma preocupação restrita à área de tecnologia, tanto que o nosso glorioso Exército brasileiro está aqui mostrando também suas preocupações, ou seja, trata-se de soberania nacional. Hoje é uma questão de soberania, de desenvolvimento econômico, de proteção de dados dos cidadãos e de continuidade dos serviços públicos. Esta audiência pública representa uma etapa essencial desse processo.

Eu também queria tranquilizar todas as senhoras e senhores que nos honram com a sua presença. Apesar do tempo limitado, General - demos três minutos, pela quantidade de pessoas que estão participando, e isso é muito benéfico para a legislação -, nós vamos dar um tempo, um prazo, e enviar para vocês, mostrar para vocês um *e-mail* para que as contribuições sejam por escrito, como muitos de vocês, das instituições aqui presentes, já têm colaborado. Então, não fiquem preocupados: "Poxa, viajei para Brasília, me desloquei ao Senado, e vou apenas contribuir com três minutos." Nós sabemos que é completamente insuficiente. Mas vamos então deixar aqui um *e-mail* à disposição.

Eu já peço à mesa aqui da Secretaria que coloque um e-mail à disposição das entidades e instituições aqui presentes para que todas as contribuições, os trabalhos que vocês certamente fizeram de estudo, de consultar vossas empresas, as pessoas que são associadas nas vossas instituições, etc., etc., etc., sejam incluídos para que quando eu, Senador Hermes, Senador Amin, formos apresentar essa legislação, ela seja o mais contemplativa e democrática possível, ouvindo as diversas experiências de instituições públicas, privadas, empresas de tecnologia, Governos, segurança, Exército, forças armadas, forças de segurança pública.

Tenho convicção de que as contribuições que serão apresentadas pelas senhoras e senhores enriquecerão o debate, serão fundamentais para a elaboração de um relatório técnico, equilibrado e à altura da relevância dessa matéria para todos nós.

Agradeço a disponibilidade de todos os convidados e reitero meu compromisso, junto com o Senador Hermes Klann, de conduzir esse trabalho com diálogo, responsabilidade e espírito colaborativo, não esqueçam isso, sempre buscando o melhor resultado para o nosso Brasil.

Muito obrigado.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado, Senador Seif. Eu passaria a palavra agora ao Marcelo, mas, antes disso, passarei, se me permite, a palavra para o Senador Astronauta Marcos Pontes.

O SR. ASTRONAUTA MARCOS PONTES (Bloco Parlamentar Vanguarda/PL - SP. Para expor.) - Obrigado, Presidente, bom dia. Bom dia a todos.

De forma curta, mas só para ressaltar a importância deste marco, a importância deste assunto para o país e, quando eu digo do país, eu estou falando inteiramente no país. Segurança cibernética é um assunto extenso e profundo, imóvel, ou seja, falando com o Exército aqui, é o pior tipo de alvo que nós temos, porque ele se move rápido e você não sabe onde ele está. Ele pode afetar, basicamente, geograficamente, todo o país. Ele pode afetar tanto em profundidade em nível de país como em nível de instituições, em nível de empresas, em nível de cidadão.

Então, é algo extremamente profundo, extremamente amplo e, infelizmente, o nosso sistema Legislativo é lento, e não possui todas as ferramentas que nós gostaríamos de ter para que uma lei emitida, para que uma lei criada aqui, se adapte rapidamente ao que deveria fazer.

Quando a gente vê, por exemplo, as medidas que têm que ser tomadas em nível de regulação também, isso tem que conversar muito rapidamente com a lei; a lei tem que ser flexível, a lei tem que ser adaptável às situações que vão aparecer. Eu estou falando isso pensando aqui, na minha cabeça, para quem trabalha com gerenciamento de risco, em relação à probabilidade, impacto de alguma coisa que hoje tem pouca probabilidade de acontecer, e um impacto muito grande, de repente, vai ter grande probabilidade no futuro, o que vai elevar muito o nível de risco. E a mitigação desse risco, o trabalho tem que ser feito dentro das estruturas, em todos esses níveis que eu falei aí, tem que ser rápido também.

Então, essa adaptação tem que ser muito rápida, tanto na maneira como nós tratamos a lei aqui que, do meu ponto de vista, tem que ser algo mais principiológico e com acesso rápido à regulação nos vários setores, já que isso transcende todos os setores, está em todos os setores. Então, nós temos que achar uma maneira de fazer desse marco um piloto também ou uma lei que possa ser rapidamente copiada para outros setores, como inteligência artificial, que segue o mesmo padrão e o mesmo princípio.

Aliás, um conversa com o outro. Essas três pernas conversam diretamente, que são a segurança cibernética, a inteligência artificial e a proteção de dados; e, quando eu digo proteção de dados, não se resume simplesmente à proteção de dados de pessoas. A gente está falando de proteção de dados gerais, dados do país de forma geral, dados de treinamento para inteligência artificial e como que isso pode ser ou não parcial. Quando digo parcial também, entendam parcial tanto incompleto quanto parcial em termos de ter *nuances* ou *bias* colocados ali dentro desse banco de dados, ou seja, é um assunto extremamente complexo, um assunto extremamente amplo, muito profundo e vai afetar até o cidadão. Isso vai lá da inclusão digital do velhinho que está lá em casa, não sabe usar o computador e vive sendo vítima de fraudes, e isso vai aumentar.

Sem dizer que o avanço natural desse tipo de tecnologia ou das tecnologias que apoiam os ataques cibernéticos também é muito evolutivo. A gente está falando de mudança e utilização de várias aplicações de inteligência artificial cada vez mais entranhadas dentro dos sistemas. Há criação, por exemplo, de milhões, eu diria, de agentes que permeiam todas as áreas. Esses agentes não têm atualmente nenhum tipo de controle, e isso também significa que a pessoa, de uma forma ingênua, acaba colocando todos os seus dados à disposição desses agentes e acaba transformando e abrindo dados de uma forma absurda.

Quero lembrar também que isso transpassa fronteiras; isso vai para outros países ou vem de outros países para cá; então é outro cuidado que tem que se ter. E isso vai ser ainda mais complicado com a entrada de computação quântica ou outros tipos de tecnologias novas, ou seja, eu pintei um quadro meio sinistro, mas é para, justamente, chamar atenção para a importância que nós temos desse marco, que não pode ser, como o Senador Seif falou, alguma coisa travada; não pode se travar o nosso desenvolvimento aqui, no país, e tem que se tomar muito cuidado para que o medo não transforme uma lei como essa em uma lei que prejudique o país, e aí prejudique em dois sentidos: prejudique no desenvolvimento e prejudique na segurança também.

Às vezes, com o medo que você tem de uma certa tecnologia, você acaba abrindo mais vulnerabilidades para que as pessoas, as instituições e as empresas sejam atacadas. Então, é um trabalho grande e certamente vamos precisar do esforço de todo mundo. A segurança cibernética é o típico exemplo de algo que precisa da participação de todos. Não é uma questão de um só; a própria pessoa que está ali desavisada fica clicando em coisas no *e-mail*. Até a educação básica precisa ser atingida com isso.

Então, obrigado. Eu estou aqui à disposição para poder ajudar. São muitos anos trabalhando com esses tipos de sistemas, ainda mais na parte técnica, mas agora aqui também na parte legislativa, para poder ajudar nesse sentido.

Obrigado a todos, e parabéns, Presidente.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Obrigado, Senador Astronauta Marcos Pontes.

Quero registrar a presença da Senadora Damares e convidá-la a fazer parte da mesa.

A SRA. DAMARES ALVES (Bloco Parlamentar Aliança/REPUBLICANOS - DF. *Fora do microfone*.) - Obrigada.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Passo a palavra, agora sim, para o Marcelo Antonio Oslller Malagutti, Secretário-Executivo do Comitê Nacional de Cibersegurança (CNCiber).

Com a palavra.

O SR. MARCELO ANTONIO OSLLER MALAGUTTI (Para expor.) - Bom dia, Senador Hermes, Senador Amin, Senador Seif, Senador Astronauta, Senadora Damares, nas pessoas de quem cumprimento as demais autoridades que nos assistem.

Eu aqui represento neste momento o Comitê Nacional de Cibersegurança, a Secretaria Executiva, e vou falar um pouco a respeito da urgência e relevância de uma política de Estado nessa linha. As palavras já proferidas pelos senhores e pelo General Barbosa, que me antecedeu, já dão um resumo do que eu tenho a falar. Então, com isso, acho que consigo cumprir o tempo.

Bom, eu vou falar aqui sobre a importância que nós vemos, no Comitê Nacional de Cibersegurança, em uma fusão do texto proposto originalmente por essa frente, que o senhor assinou, Senador Esperidião, com a nossa proposta de regulação elaborada pelo Comitê Nacional.

Trago aqui duas mensagens importantes que a gente gostaria de destacar. Uma é do Tribunal de Contas da União, que destaca que a cibersegurança é um dos três pilares, uma das três dimensões da soberania digital, um tema muito caro a todos nós. E, por fim, é uma observação da mensagem presidencial ao Congresso no início deste ano, em que o Presidente

apregoa a necessidade de termos uma nova governança da cibersegurança nacional ainda em 2026. Então, essa mensagem de urgência nós temos trabalhado com ela como uma regra dentro dos nossos trabalhos.

Nós temos, basicamente, um problema simples que é o paradoxo digital brasileiro. Nós somos o país com o maior Governo digital do mundo, a maior oferta de serviços do mundo, mas somos um país que sempre aparece também como um dos três maiores, dependendo das diferentes pesquisas, atacados no mundo. Portanto, nós temos uma oferta, uma vitrine muito grande e muito exposta, sujeita a fraudes e diferentes tipos de incidentes.

A solução que nós temos visto no comitê nos últimos três anos é a melhoria da governança dessa cibersegurança. Nós temos trabalhado forte na linha de termos regulação, fiscalização, coordenação e controle. E o benefício esperado é a melhoria da proteção da nossa economia digital, maior...

(Soa a campainha.)

O SR. MARCELO ANTONIO OSLLER MALAGUTTI - ... segurança jurídica, proteção aos cidadãos e soberania digital nacional.

Nós tivemos incidentes graves envolvendo o Ipen. Tivemos, recentemente, o caso da "misantropia", que foi o maior incidente de negação de serviço que acabamos tendo, em que um único *hacker*, um único ataque desabilitou o serviço de defesa civil nosso por vários dias. Nós ainda continuamos inoperantes nesse caso.

Bom, nós temos um movimento geopolítico muito importante no sentido de que a melhor defesa é o ataque. Vários países estão adotando essas medidas recentemente.

E, no tocante às tecnologias, recentemente mencionadas pelo Senador Seif e pelo Senador Astronauta, nós temos duas que chamam particularmente a atenção num rol de 35 que nós estamos monitorando lá no GSI e acompanhando. Uma delas é a IA. E a gente vê aí uma movimentação consistente dos países em trazerem seus órgãos reguladores de IA, seus órgãos gestores de IA, a trabalharem junto com o pessoal de cibersegurança, muito mais do que com os órgãos de proteção de dados. Por quê?

(Soa a campainha.)

O SR. MARCELO ANTONIO OSLLER MALAGUTTI - Porque observa-se a necessidade de termos essa proximidade maior.

Ontem, a China anunciou o Mythos dela, os americanos tinham anunciado o Mythos, ontem os chineses anunciaram um que dizem que é superior ao americano. Nós não tivemos tempo de avaliar ainda, mas dá para a gente ver que a guerra está aberta, está declarada, que o espaço está sendo ocupado muito rapidamente e que nós estamos atrasados. Então, nós temos que pelo menos nos proteger; se não seremos ofensivos, porque não é da nossa cultura, pelo menos temos que nos proteger do uso dessas ferramentas contra nós.

O Presidente Trump assinou uma ordem executiva relevante em que ele Departamento de Defesa - nossos colegas militares aqui estão acompanhando isso - vai implementar sensores quânticos já a partir de 2027. E eles terão - o Departamento de Energia, que faz os supercomputadores, que compra os supercomputadores americanos - um computador quântico plenamente operacional em breve, até 2030, e que os americanos já vão utilizar a criptografia pós-quântica, um outro item mencionado pelos senhores, a partir de 2031, exclusivamente pós-quântica. Os franceses, por sua vez, a partir de 2027, não homologarão nenhum produto ou serviço novo que não tenha criptografia pós-quântica, ou *quantum-safe*, como eu prefiro chamar.

Bom, nós temos aí, na nossa proposta do CNCiber, um conjunto de órgãos que passariam a ser serviços essenciais e infraestruturas críticas, com seus devidos reguladores.

(Soa a campainha.)

O SR. MARCELO ANTONIO OSLLER MALAGUTTI - E a nossa proposta elaborada lá traz uma ideia de que a gente teria uma autoridade nacional que faria uma regra padrão, a regra geral, e que cada um dos reguladores setoriais desenvolveria as regulações específicas. Parece-nos uma proposta melhor, mais completa, eu diria, não melhor no sentido qualitativo, mas mais completa do que a proposta, por exemplo, que se discutiu no projeto da IA, em que havia apenas uma coordenação-geral e não uma regra geral estabelecida por um órgão específico.

Nós temos quatro objetivos importantes, aspectos positivos, que são a segurança jurídica; a estabilidade regulatória e a harmonia regulatória, que facilitem a economia de dados; o esforço na cultura e educação - foi mencionada há pouco também pelos Senadores a necessidade de se educar a população desde os níveis das idades mais tenras até os níveis profissionais mais avançados; e, o que é muito caro para o GSI e para o Ministério da Defesa, a questão da soberania nacional no sentido de inserção do Brasil na cadeia de valor, de nós termos produtos e serviços brasileiros não apenas sendo

utilizados no Brasil, mas também sendo exportados, oferecidos ao mundo e termos uma maior resiliência, particularmente no tocante à operação dos nossos serviços essenciais.

Para concluir a junção dessas duas propostas, teria cinco elementos relevantes para nós no tocante à governança: um sistema nacional de cibersegurança, que atenderia o âmbito político; um conselho nacional, diferente do comitê, envolvendo os outros Poderes - Legislativo, Judiciário, Ministério Público -, estados e municípios; as autoridades nacionais, sendo tanto a Autoridade Nacional de Cibersegurança como os órgãos reguladores setoriais, daquele eslaide anterior que eu mostrei; um Centro Nacional de Cibersegurança, que seria o operador da segurança, aquele que monitora, que tem os sensores, que vê a onda de ataques acontecendo em tempo real, é a parte do controle daquelas quatro funções mencionadas inicialmente; e, claramente, um grande ganho que haveria seria a manutenção dessa proposta extremamente importante, apresentada pelo Senador Esperidião e pelos colegas da frente parlamentar, no sentido de um programa voluntário. Nós teríamos, então, um conjunto de órgãos obrigados pela importância, pela essencialidade dos serviços que prestam, pelas infraestruturas críticas que administram, mas também aqueles outros que gostariam de aderir, de ser voluntários e adotarem o programa.

(Soa a campainha.)

O SR. MARCELO ANTONIO OSLLER MALAGUTTI - Eu encerro aqui com os quatro itens mencionados há pouco e deixo o meu contato para aquelas pessoas que quiserem ter mais detalhes, mais informações a respeito da proposta de fusão, como poderia ser realizada.

Agradeço muitíssimo a oportunidade e a confiança.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado, Sr. Marcelo.

Eu passo agora a palavra ao Sr. Demi Getschko - será que eu pronunciei certo? -, Diretor-Presidente do Núcleo de Informação e Coordenação do Ponto BR (NIC.br).

O SR. DEMI GETSCHKO (Para expor.) - Bom dia a todos.

Muito obrigado pelo convite. É uma honra estar presente aqui.

Tenho uma pequena apresentação, mas vamos reduzir aos pontos essenciais, já que o tempo é curto e temos que avançar.

Então, a primeira coisa que eu vou dizer em relação ao NIC, que é o órgão que eu teoricamente represento aqui, é que o NIC...

Vou passar. Opa, perdão! Já chegamos ao obrigado. A coisa não funcionou. *(Risos.)*

É mais rápido do que eu imaginava, mas não é tão rápido.

Pronto. Eu vou colocar aqui. Vamos lá. Então, muito bem.

O NIC é um órgão privado que usa recursos privados, não públicos - não tem um centavo público -, que cuida do .br. O .br, como vocês sabem, é um sobrenome que funciona bem na internet brasileira, foi bem adotado pelos brasileiros. O .br foi obtido em 1989 da administração central da internet e a gente tem mantido isso aí de uma forma bastante, espero eu, sensata. Por exemplo, nós nunca abrimos o segundo nível do .br para ninguém, tanto que leg.br não pertence a Luiz Eduardo Gonçalves, mas sim ao Legislativo; o gov.br é do Governo; foi criado o bet.br por causa das apostadoras e tudo mais. Então, o fato de manter o segundo nível fechado é útil para ter uma semântica no processo.

E um dos órgãos do NIC - que, teoricamente, estaria nessa apresentação em algum lugar - é o Cert, que é o nosso centro de emergências em informática, que tem uma longa trajetória - vai completar 30 anos o ano que vem - e gera cursos nessa área e tudo mais. A gente tem oito cursos por ano em tratamento de incidentes.

E o meu ponto de alerta seria o seguinte: primeiro, essa temática é uma temática multifacetada. É totalmente diferente do que a Defesa tem de tratamento de cibersegurança e do que tem o cidadão comum, que é sujeito a fraudes, a golpes. Nós geramos cartilhas a cada mês sobre coisas desse tipo.

(Soa a campainha.)

O SR. DEMI GETSCHKO - Então, o tema é multissetorial e é diferente.

É fundamental que o tema seja tratado como colaboração, tem que ser um tema colaborativo. A internet brasileira é muito bem vista lá fora. A gente tem uma boa trajetória na área. E o Cert também é muito bem visto lá fora. A gente tem integração com n órgãos internacionais que tratam disso, então isso é importante. A gente participa do Guardião Cibernético e tudo mais.

Eu me beneficio do que foi falado aqui. Certamente, segurança é um alvo móvel e, como qualquer alvo móvel, qualquer doença, nós precisamos saber qual é o sintoma para poder gerar um tratamento. Então, é fundamental que a gente preserve a aquisição de denúncias na área do que acontece, porque, se você não tiver um centro que recebe as informações de problemas na área de segurança, você não tem como retrabalhar isso aí e gerar bons aconselhamentos a quem vai ser eventual vítima disso.

Vou usar uma frase que foi dita aqui: de fato, o Brasil é um dos...

(Soa a campainha.)

O SR. DEMI GETSCHKO - ... alvos principais de ataques cibernéticos. Por exemplo, o .br é um dos domínios mais seguros do mundo, porque a gente mantém a exibição de quem é o dono do domínio, a gente sabe quem é, isso não é oculto. Então, ao mesmo tempo que nós somos alvo, nós temos o melhor serviço digital, o governo - o gov.br é um sucesso -, e nós temos o .br muito na região dos domínios seguros. Você raramente é atacado por um domínio .br.

Então, o que eu queria dizer é o seguinte: se você não proteger a identidade de quem denuncia, você perde as denúncias. Nós temos um arquivo gigantesco de denúncias de problemas na área de segurança, o que não indica que nós sejamos inseguros; indica que o pessoal que recebe as denúncias é considerado seguro, pode recebê-las e só assim nós podemos fazer um retrabalho, uma engenharia reversa para chegar ao ponto final. Então, eu acho que isso é importante.

Em relação à legislação, eu acho que é fundamental o que foi dito aqui: países, às vezes, avançaram além do ponto e tiveram que recuar.

E nós aprendemos com isso.

Veio-me à cabeça uma frase latina, que é: *festina lente*, que significa apressa-te devagar. É importante que a gente se apresse de uma forma cautelosa, neutra e, certamente, equilibrada.

E eu diria que o ponto fundamental do que foi dito de ataques a brasileiros é um problema de letramento, que nós teremos que trabalhar pesadamente em chamar a atenção do cidadão, das empresas, do que for, de que esse é um alvo móvel e que você tem que estar o tempo todo se reconfigurando, para poder se mostrar resiliente a esse tipo de serviço. Eu acho que essa é a grande jogada.

Então, eu ressaltaria que, primeiro, o Brasil tem uma boa trajetória na área da internet, é muito bem visto lá fora nesse assunto, o Cert.br têm uma bela participação internacional e intercâmbio com outros órgãos, além dos cursos de multiplicação que dá, e esse é um problema que não pode ser tratado monoliticamente; tem que ser tratado multissetorialmente, multifacetadamente, porque cada área da sociedade...

(Soa a campainha.)

O SR. DEMI GETSCHKO - ... tem as suas devidas dores com isso e não há uma solução única para tudo isso.

O que é útil para áreas de Governo, para áreas de segurança, de serviços públicos não é obrigatoriamente útil para crianças e adolescentes, não é obrigatoriamente útil para cidadãos no dia a dia, e só o trabalho cooperativo na área vai poder gerar algo que seja sólido.

Eu espero não ter avançado muito no tempo, mas é isso.

Um último comentário pedante: a gente está usando ciber o tempo todo. Ciber vem da palavra grega *kybernan*, que dá a palavra Governo. Então, cibernética é "governética". Então, na verdade, cibercrimes são crimes de controle.

Obrigado.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado.

Eu acho que todos têm contribuição para a gente anexar a isso tudo, mas eu passo agora ao Sr. Rodrigo Pereira Pacheco, Diretor Substituto do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, da Agência Brasileira de Inteligência (Cepesc/Abin).

O SR. RODRIGO PEREIRA PACHECO (Para expor.) - Bom dia a todos.

Gostaria de cumprimentar os Exmos. Senadores, demais autoridades, membros da mesa e todos os presentes e agradecer o convite desta Comissão de Ciência, Tecnologia, Inovação e Informática.

É com grande satisfação que participo desta audiência pública como Diretor Substituto do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações.

O Cepesc é a unidade da Agência Brasileira de Inteligência regimentalmente responsável por segurança e inteligência cibernética. Foi o primeiro órgão do Brasil especificamente dedicado à segurança da informação e possui 44 anos de sólida experiência, tendo ampliado suas atividades de acordo com a evolução tecnológica.

Nós estamos aqui hoje para debater um tema que transcende a segurança cibernética convencional. Estamos tratando fundamentalmente da preservação da soberania nacional, da higidez das nossas instituições e da proteção das infraestruturas críticas do país.

No atual cenário geopolítico, o ciberespaço tornou-se uma arena de disputas complexas, onde atores estatais e não estatais operam de forma sofisticada. Por essa razão, a governança da cibersegurança no Brasil não pode ser reduzida a uma atividade puramente computacional ou de combate ao crime cibernético. Ela exige uma articulação profunda com a atividade de inteligência e com a alta tecnologia criptográfica de Estado, visando a diminuir a superfície de ataque relacionada a ameaças persistentes avançadas, cujo principal objetivo é a ciberespionagem e a cibersabotagem.

Gostaria de estruturar nossa visão em quatro pilares fundamentais que justificam as centralidades do Cepesc e da Abin nesse domínio.

Primeiro, a inteligência cibernética como função de Estado e do Sisbin.

Em primeiro lugar, é preciso registrar que a inteligência cibernética é uma área temática da própria inteligência de Estado, levada a cabo pelo Sistema Brasileiro de Inteligência, o Sisbin, hoje composto por mais de 40 órgãos parceiros, sob a coordenação central da Agência Brasileira de Inteligência.

Essa atividade está formalmente prevista na doutrina da atividade de inteligência e responde diretamente às ameaças prioritárias identificadas na Política Nacional de Inteligência, desde 2016.

A inteligência cibernética é político-estratégica, analisa dados para entender o macro cenário e subsidiar o processo decisório nacional.

Segundo, a conexão indissociável com a cibersegurança.

A inteligência cibernética está diretamente conectada e serve de suporte à cibersegurança. Ela atua como camada de governança e assessoramento que viabiliza essa proteção em nível de Estado, garantindo que as políticas de resiliência cumpram os padrões de alta segurança exigidos para a preservação dos segredos nacionais.

Terceiro, as múltiplas fontes da inteligência de ameaças.

Para cumprir sua missão estratégica, a inteligência cibernética se alimenta de várias fontes, entre as quais a inteligência de ameaças. Enquanto a primeira atua em nível macro e preventivo, a inteligência de ameaças cumpre um papel tático e operacional, analisando dados de incidentes cibernéticos para consolidar conhecimento estratégico.

Finalmente, a missão do Cepesc-Abin: enfrentamento de APTs e pesquisa em desenvolvimento de fronteira.

É neste cenário de alta complexidade que se insere a missão da atuação do Cepesc-Abin. Nossa atuação diária é direcionada para identificação, tratamento e neutralização de ameaças no nível mais sensível da administração pública.

Atuamos na linha de frente contra ataques cibernéticos sofisticados, levados a cabo por grupos de ameaças persistentes avançadas ligados a governos estrangeiros contra infraestruturas críticas e setores estratégicos do Brasil. Monitoramos e avaliamos os impactos das tecnologias computacionais emergentes, as TCEs, compreendendo inteligência artificial, computação quântica, sistemas autônomos e arquiteturas avançadas de conectividade, antecipando as novas dinâmicas de risco que elas introduzem.

Mais do que analisar, nós desenvolvemos soluções. O Cepesc é o braço tecnológico que lidera a pesquisa em desenvolvimento em *hardware* e *software* de segurança, com foco na criação de algoritmos proprietários com criptografia pós-quântica.

A proteção do fluxo de dados das autoridades máximas da República e o desenvolvimento do algoritmo criptográfico de Estado encontram-se sob nossa coordenação técnica.

Por meio da utilização de algoritmos de estado desenvolvidos internamente, preparamos as comunicações críticas para resistir, inclusive, às capacidades futuras da computação quântica, minimizando riscos de espionagem inerentes a soluções comerciais.

Finalmente, se observarmos as nações de referência global, como o Reino Unido, com o National Cyber Security Centre, dentro da Agência de Inteligência de Sinais, ou os Estados Unidos, com a atuação da NSA e da Cisa, ou a Espanha, com o Centro Criptológico Nacional integrado ao Centro Nacional de Inteligência, veremos, de forma inequívoca, que a inteligência civil e o desenvolvimento criptográfico soberano são o núcleo duro da resiliência digital de qualquer país.

A expertise e o *know-how* acumulados pelo Cepesc-Abin são ativos indispensáveis e insubstituíveis. Garantir e fortalecer esse papel nas políticas gerais de resiliência cibernética é a única forma de assegurar que o Brasil não seja apenas um espectador reativo, mas um ator soberano e protegido na era digital.

Obrigado.

(Soa a campainha.)

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado.

Eu vou passar a palavra agora, remotamente, ao Sr. Rony Vainzof, Diretor Titular da Divisão de Cibersegurança da Fiesp e Consultor em Proteção de Dados da Fecomercio de São Paulo.

O SR. RONY VAINZOF (Para expor. *Por videoconferência*.) - Olá, bom dia a todos e a todas.

Prezados Senadores Hermes Klann, Esperidião Amin, Jorge Seif, Marcos Pontes, Damares e demais colegas, bom dia.

Desculpem-me entrar *online*. Eu já tinha uma viagem marcada, mas logicamente fiz questão de participar desse honroso convite, mesmo que remotamente.

Tive a oportunidade também de compor a mesa de instalação da frente parlamentar, que teve, se eu não me engano, o maior público da história das frentes no auditório do Senado. Isso já demonstra a importância desse tema.

Eu tenho muito orgulho aqui de representar a Fiesp e a Fecomercio nesta audiência, bem como o setor empresarial no Comitê Nacional de Cibersegurança, ao lado de tantos outros colegas brilhantes.

Quero desde já ressaltar a importantíssima iniciativa do Senado com o PL 4.752 e de como ela se complementa com o texto que nós trabalhamos no CNCiber ao longo desses últimos quase dois anos.

Essa junção do texto do PL 4.752 com o texto que nós propusemos no CNCiber caracteriza uma verdadeira ação de Estado, pois a aprovação do marco legal é urgente e relevante - e eu vou tentar aqui explicar um pouquinho o porquê.

Se a gente observa vários relatórios em relação ao custo anual de incidentes e fraudes cibernéticas, ele pode chegar a um número de 10,5 trilhões anualmente. Esse tipo de custo envolve custos diretos, como interrupção operacional ou multas regulatórias, e custos indiretos também, como redução de valor de mercado de empresas e também perdas de clientes.

Quando a gente olha para o Brasil, esse custo com golpes digitais pode chegar a R$100 bilhões por ano, somente envolvendo golpes digitais.

Quando a gente olha para a criticidade da pauta com o avanço de novas tecnologias, como a inteligência artificial, criminosos que levavam quase 25 dias para explorar vulnerabilidades, hoje, com a IA, podem levar minutos.

É de 27 anos a idade do *bug* mais antigo descoberto recentemente com o uso da IA. E pior: menos de 1% das vulnerabilidades conhecidas já foram efetivamente corrigidas. Fora a questão do *quantum day*, que o Marcelo Malagutti comentou, previsto para 2029.

Então, esse paradoxo brasileiro que nós estamos enfrentando, enquanto lideramos em inovação, mas também nos tornamos alvo - estamos cada vez mais expostos a ataques cibernéticos -, com uma alta adoção de novas tecnologias, mas baixa maturidade e segurança, fez com que o TCU alertasse, nessa risca de alto risco, em termos de soberania, confiança e aceleração digital. E o TCU falou: "Não há organização oficial no Brasil capaz de zelar pelo nível de maturidade de segurança cibernética e orientar as atividades no país".

É por isso que a nossa proposta aqui é a do marco legal com o órgão central de cibersegurança - não uma questão de mais regulação, mas sim a melhor regulação, um marco horizontal que organize o tema, para mitigar riscos sistêmicos, econômicos e de infraestrutura; para uma questão de soberania, uma abordagem baseada em risco, com obrigações legais para infraestruturas críticas e serviços assistenciais; e, para os demais agentes, apenas boas práticas.

Cibersegurança exige coordenação nacional. Fora isso, a função principal desse órgão deve ser coordenadora, técnica e preventiva. A gente precisa ter um cuidado para evitar uma sobreposição sancionatória, o chamado *bis in idem*.

Fora isso, o incidente não pode significar culpa automática. O foco deve ser em avaliação de maturidade, diligência, governança e resposta adequada.

Com harmonização, com a experiência internacional, diversos países, de fato, caminham nesse sentido, e a cybersegurança empresarial é pragmática, ou seja, uma lei bem desenhada com a junção do PL com a proposta do CNCiber reduz custo, melhora a previsibilidade, fortalece a confiança digital, protegendo cadeias críticas, e torna o Brasil mais competitivo.

E só para concluir aqui, eu queria dizer que o CNCiber é um órgão plural que representa toda a sociedade, e nós votamos nessa 8ª Reunião, Ordinária, que foi realizada no final do ano passado com 20 instituições representativas da sociedade. E

foi aprovada, por votação unânime, tanto a proposta de um marco legal quanto de um órgão central, ou seja, juntos e com eventuais ajustes pontuais, o PL 4.752, com a proposta do CNCiber, eles se complementam, para que a transformação digital no Brasil avance com segurança e confiança, ou seja, a pauta é urgente diante do custo da inação.

Muito obrigado e fico à disposição depois para os debates.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado ao Sr. Rony Vainzof.

Eu passo agora a palavra ao Sr. Rodrigo Jonas Fragola, Vice-Presidente de Articulação Política da Confederação das Associações das Empresas Brasileiras de Tecnologia da Informação (Assespro).

Com a palavra.

O SR. RODRIGO JONAS FRAGOLA (Para expor.) - Bom dia, Presidente, bom dia demais da mesa e meus colegas.

Bem, a Confederação Assespro representa 3,5 mil empresas, na área de tecnologia de informação, que são desenvolvedoras de *software*, e muitas delas desenvolvedoras de tecnologia de pequeno e médio porte. Eu estou aqui representando esse pequeno grupo amostral das empresas brasileiras.

Além disso, eu sou membro do CNCiber, sou bacharel em Ciência da Computação pela Universidade de Brasília e sou especialista em Política e Estratégia Cibernética pela Escola Superior de Guerra.

Eu só tenho 30 anos de experiência na área de *cybersecurity*. Além disso, a minha empresa desenvolveu tecnologia na área de *cybersegurança*. E eu sei o quão é bom e o quão é ruim você conseguir ter o domínio sobre uma tecnologia que está fazendo a segurança de um povo ou de uma nação.

Então, existem três pontos que são bem interessantes para a gente avaliar.

O primeiro, já foi dito pelo Sr. Marcelo e completado agora pelo Sr. Rony, que a união desses dois projetos é o que vai viabilizar a possibilidade de se ter uma ação real e efetiva na segurança do país. Esses dois movimentos que nós estamos fazendo agora vão cumprir, sim, com a capacidade do alvo móvel, que foi dito no início da reunião, porque isso é inerente na área de *cyber*. E quanto à agência, diferente de outras agências, a gente entende que ela é uma agência que deve avaliar a maturidade, que deve ajustar e coletar informações, enfim, que deve ajudar o mercado e ajudar o Governo a melhorar a segurança como um todo, já que o risco não é mais individual. O risco agora é holístico, é compartilhado com outras entidades.

(Soa a campainha.)

O SR. RODRIGO JONAS FRAGOLA - Uma outra questão que nos preocupa muito é a questão da soberania nacional. A área de *security* sem desenvolvimento de tecnologia e sem desenvolvimento de autonomia é simplesmente inútil.

Não adianta gastar bilhões e bilhões de reais com produtos, sejam eles de falha ou de antivírus, EDRs, enfim, milhões de outros tipos de produtos que existem no mercado, de nações que sabidamente têm se utilizado de processos de espionagem e captura de dados ilegais ou legais que sejam, não é? Então, não adianta a gente pensar em desenvolver esse tipo de situação, esse tipo de autonomia... desculpa, esse tipo de segurança, sem autonomia e soberania.

Outro ponto que nos preocupa é a questão das multas. Como empresas privadas, a gente quer participar desse processo, a gente quer ajudar, mas a gente tem que entender que muitas das estruturas críticas, e até daqui da própria Casa...

(Soa a campainha.)

O SR. RODRIGO JONAS FRAGOLA - ... são mantidas por empresas privadas. E a gente não pode ser, digamos, punido excessivamente com as multas. Então a gente entende que as multas que estão citadas dentro do documento sejam, assim, em último caso, em caso de negligência, em caso de não observância, aplicadas de formas bem didáticas, e que a posição da Anciber, caso seja criada, seja uma posição muito mais de ajudar dentro do processo, apontar direções, até mesmo para que nós da iniciativa privada possamos contribuir.

Obrigado.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC. Pela ordem.) - Quero pedir permissão aqui para o nosso Presidente da sessão, o Senador Hermes Klann, para aproveitar a sua colocação, gabaritada pelos 30 anos de experiência: texto, apresente um texto.

O SR. RODRIGO JONAS FRAGOLA - Sim, sim, faremos.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - A reflexão nós entendemos. E é importante apresentar um texto e, com a sua experiência, um texto em forma legislativa, quer dizer: que emenda, que parágrafo, que artigo. Essa será a melhor contribuição para os Relatores, eu vou dizer...

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Perfeito.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - ... ao tempo em que eu me permito registrar a presença do nosso Governador, quero dizer, ainda Senador *(Risos.)* Sergio Moro. Seja bem-vindo.

A SRA. DAMARES ALVES (Bloco Parlamentar Aliança/REPUBLICANOS - DF) - Presidente, pela ordem...

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Pois não, Senadora.

A SRA. DAMARES ALVES (Bloco Parlamentar Aliança/REPUBLICANOS - DF. Pela ordem.) - ... para completar o que o Senador Amin falou.

Eu estou vendo as apresentações dos senhores aqui, que vocês não estão tendo tempo de mostrar, apresentações incríveis. Tem apresentação aqui que dá uma aula de mestrado e doutorado.

O SR. JORGE SEIF JÚNIOR (*Fora do microfone*.) - Verdade.

A SRA. DAMARES ALVES (Bloco Parlamentar Aliança/REPUBLICANOS - DF) - Mas aí eu vou para a tramitação do projeto e não estou vendo nenhum parecer dos senhores juntado no projeto. Eu não sei se eu estou enganada, Secretaria. Eu estou vendo aqui. Não tem nenhum. Eu acho que todas as apresentações dos senhores... Claro, elas vão ficar disponíveis agora para o público nacional, para todo mundo que quiser. Atenção, Brasil, está disponível no *site* da Comissão, agora, as espetaculares apresentações que eles não estão tendo tempo de mostrar. Mas eu iria sugerir que todos os senhores transformassem essas apresentações - e também aqueles que não têm - em forma de parecer e juntassem na tramitação do projeto...

(Intervenção fora do microfone.)

A SRA. DAMARES ALVES (Bloco Parlamentar Aliança/REPUBLICANOS - DF) - ... porque as contribuições aqui... Eu estou ouvindo, tentando acompanhar, anotar aqui, e não estou conseguindo.

Parabéns a todos pelas contribuições que estão trazendo, mas, assim como o Amin falou para o Rodrigo Fragola - eu estava numa expectativa muito grande para te ouvir, Rodrigo -, transformem isso, por favor, em parecer e juntem ao nosso projeto de lei.

Obrigada.

O SR. JORGE SEIF JÚNIOR - Pela ordem aqui, Senador.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - Não foi nenhuma inveja de penteado.

O SR. JORGE SEIF JÚNIOR - Só pela ordem.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Pois não, Senador.

O SR. JORGE SEIF JÚNIOR - Senadora Damares, exatamente o objetivo dessa audiência pública foi realmente convidar pessoas gabaritadas com reconhecimento, empresas, instituições, Governo, para nos ajudar, contribuir com esse parecer, com esse relatório que nós vamos apresentar.

Na minha fala - a senhora ainda não estava aqui -, repito, reitero e peço que todos realmente anexem os seus pareceres, as suas observações sobre o texto proposto, onde estão as fragilidades, as críticas, como disse o Senador Amin, as críticas positivas e negativas, que nós vamos fazer um compilado de todas as contribuições. Inclusive, estamos fazendo isso com as legislações internacionais, estamos colocando a nossa assessoria para analisar, tanto governamentalmente quanto da imprensa e dos órgãos correlatos, quais são as críticas às legislações que já foram implementadas em outros países, para que nós acertemos quando fizermos a nossa proposição.

Obrigado, Senador Damares, pela sua contribuição.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Obrigado, Senadora Damares, Senador Jorge Seif.

Quero registrar, mais uma vez, a presença do nosso Senador Sergio Moro e convidá-lo para fazer parte da mesa, se assim quiser.

Eu vou passar a palavra agora ao Sr. Luiz Henrique Barbosa, Presidente-Executivo da Associação Brasileira das Prestadoras de Serviços de Telecomunicações Competitivas (TelComp). Com a palavra.

O SR. LUIZ HENRIQUE BARBOSA (Para expor.) - Bom dia a todos. Obrigado pela oportunidade. Cumprimento aqui os Senadores presentes nesta importante audiência: Esperidião Amin, Marcos Pontes, Presidente Hermes, Jorge Seif, Senadora Damares e Senador Sergio Moro.

A TelComp é uma associação que representa empresas privadas, prestadoras de serviços de telecomunicações, e que atua em toda a cadeia de telecomunicações. Então, por assim dizer, nós temos empresas associadas que operam cabos submarinos, conectando o país com outros países, no Atlântico, no Pacífico, conectando com a África, os Estados Unidos, a Europa; empresas que têm redes de transporte, que estão conectando diversas regiões do Brasil - a gente chama essas redes de longa distância de *backhaul*, *long haul*, mas basicamente são empresas que operam em longa distância. Temos, entre as associadas, operadores de *data centers*, satélites, redes móveis que operam no mercado de IoT, VoS, que, de alguma forma, atendem o cliente final, atendem o Governo, atendem empresas.

Nesse sentido, esta prévia aqui é para dizer que todas as empresas que fazem parte da TelComp estão sujeitas a uma crise sobre cibersegurança, pelo simples fato de serem provedoras de conectividade. Então, já tivemos algumas empresas com essa experiência e, por isso, entendemos que esse projeto de lei é muito importante.

Nesse sentido, então, reforço aqui que o que a gente chama hoje, na sociedade, de transformação digital, transformou telecomunicações em mais um setor entre diversas camadas de infraestrutura digital que devem ser consideradas quando a gente fala de segurança cibernética.

O risco cibernético hoje percorre uma cadeia enorme, não só dos provedores de conectividade, mas a gente está falando de operadoras que operam o que a gente chama de nuvem, plataformas digitais, sistemas operacionais, os mais diversos, porque está tudo conectado, dispositivos que estão na mão das pessoas, que a gente chama...

(Soa a campainha.)

O SR. LUIZ HENRIQUE BARBOSA - ... de internet das coisas, com inteligência artificial, a gente tem diversas aplicações que estão sujeitas a essa questão da segurança cibernética.

Então é importante esse marco legal: não existe mais uma situação de só as telecomunicações estarem sujeitas a essa obrigação. Ao que a gente quer chamar a atenção, então, é que a responsabilidade tem que estar colocada para toda uma cadeia, não é criar burocracia, mas é ter essa visão e realidade; e que todo mundo que captura, trata, armazena, processa dados tem que ter uma obrigação compatível ao seu impacto, ao risco que gera. Não faz sentido ter só dever obrigatório sobre só quem transporta dados, a gente tem essa experiência já, nós temos a Anatel, que tem uma resolução sobre segurança cibernética já há algum tempo. A TelComp, inclusive, com as suas associadas fazem parte do Exercício Guardião Cibernético, mas o que a gente acha dentro do processo desse projeto de lei é que tem um princípio único, mas as obrigações são diferentes, proporcionais aos riscos que estão envolvidos nos diversos atores.

(Soa a campainha.)

O SR. LUIZ HENRIQUE BARBOSA - Então, como a contribuição aqui é muito breve, queria deixar consignada esta necessidade de uma cooperação dos setores privado e público - nenhum governo resolve sozinho esse tema, tampouco o setor privado. A gente, de alguma forma, detecta boa parte dessas ameaças, antes mesmo do Estado, e tem que ter um mecanismo de cooperação, de reporte seguro dessas informações, com proteção jurídica para a comunicação desses incidentes.

Novamente, quando existe uma crise, às vezes ela vai, essa crise, para a mídia, e aí tem impacto, os nomes que saem têm um risco de reputação, impacto econômico direto. Então, a necessidade de ter a agência nacional, uma coordenação nacional é importante para a proteção dos eventualmente envolvidos numa crise dessa, que muitas das vezes tomaram as devidas precauções. Mas isso é uma realidade que a gente tem hoje na sociedade.

A gente já possui, de alguma forma, a LGPD, a agência que protege dados, a Anatel como agência que trabalha já há muito tempo na segurança cibernética, e especialmente segurança das redes de telecomunicações, então a gente vem aqui para dizer que é importante esse projeto de lei para buscar integrar, harmonizar...

(Soa a campainha.)

O SR. LUIZ HENRIQUE BARBOSA - ... e ter uma preocupação com a duplicidade de fiscalização e com que se evite conflito entre diversos órgãos, pois ele precisa ter as responsabilidades bem definidas.

Então, quero agradecer a oportunidade e dizer que esse marco legal representa uma oportunidade histórica para o Brasil, de fato, adotar uma visão integrada e construir uma política de Estado voltada ao ecossistema digital como um todo e a toda essa cadeia de transformação digital pela qual a sociedade passa.

Obrigado.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado, Sr. Luiz Henrique, e nos coloque à disposição esse texto, para poder agregar, o.k.?

Eu passo a palavra agora ao Sr. Luca Belli.

O SR. LUCA BELLI (Para expor.) - Bom dia - boa tarde, aliás, a todos e todas.

É um grandíssimo prazer, uma honra estar aqui com vocês hoje.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Desculpe-me. Deixe-me completar aqui, Luca.

Eu vi aqui "Belli", e eu tenho um monte de conhecidos Belli, e olhei para você para ver se conhecia, mas o Luca é Professor da Fundação Getulio Vargas Direito Rio, Coordenador do Centro de Tecnologia e Sociedade da Fundação Getulio Vargas.

Pode continuar agora.

O SR. LUCA BELLI - Muito obrigado, Senador. Confirmo a identidade.

Eu queria agradecer muito a disponibilidade, a oportunidade, a liderança dos Senadores Esperidião Amin, Hermes Klann, Marcos Pontes, Seif, Sergio Moro e, claramente, da Senadora Damares Alves nessa pauta. Eu trabalho não há 30, mas há 20 anos com regulação de tecnologias digitais, inclusive cibersegurança. Eu queria frisar que os elementos que eu vou compartilhar são frutos de anos de pesquisa empírica.

Já em 2023 lançamos esse livro, que, aliás, foi apresentado na última audiência do G6, sobre a ideia de um marco de cibersegurança em 2023, no qual também encontrei o Senador Esperidião Amin. Nesse livro, destacamos a necessidade, a urgência, já em 2023, há quatro anos, de cinco elementos essenciais para construir a cibersegurança no Brasil: um marco regulatório, uma agência, um conselho multissetorial, um sistema e uma estratégia, que, idealmente, inclua também uma política industrial. Foi criado o CNCiber, um conselho multissetorial. Foi adotada a estratégia que, aliás, contribuímos a desenvolver com o Decreto 12.573 do ano passado, em agosto. Talvez estejamos ainda um pouco tímidos com a política industrial, porém, ainda falta, claramente, um marco legal, falta uma agência e falta um sistema para conectar todas as entidades que estão com as mãos na massa e que criam a cibersegurança deste país, e coordená-las.

Então, nesse sentido, nesse segundo estudo que foi publicado em dezembro do ano passado sobre governança e cibersegurança no Brasil, analisamos o que foi definido aqui, de maneira muito pertinente, como um paradoxo: o Brasil, ao mesmo tempo, está avançando em retrocesso com a cibersegurança. Como é possível essa situação paradoxal? Em 2024 somente, o Brasil foi alvo de 356 bilhões de tentativas de ataques. No ano passado, o Brasil teve R$100 bilhões de prejuízo. O Brasil enfrenta uma escassez de mais 700 mil funcionários especializados em cibersegurança. Mas, ao mesmo tempo, o Brasil está subindo em todos os *rankings* internacionais de cibersegurança. Isso é o que eu chamo, no livro, de "cibersegurança de Schrödinger" - é como o gato de Schrödinger, que, ao mesmo tempo, é vivo e morto.

A cibersegurança está avançando e retrocedendo no Brasil nos últimos anos. Como é possível? A explicação é simples: nos últimos cinco anos foram adotadas várias regulamentações setoriais, aliás, muito elogiadas, muito na vanguarda. Porém, são regulações setoriais. Existem nove setores que regulamentam a cibersegurança no Brasil, todos analisados nos pormenores nesses livros, porém, para nenhum deles, a cibersegurança é a sua prioridade. Então, fora da Anatel e do Banco Central, que priorizam a cibersegurança há 20 anos, porque é essencial para evitar riscos sistêmicos nas telecomunicações e no setor bancário, para nenhum outro setor é uma prioridade. E não existe coordenação entre esses setores.

(Soa a campainha.)

O SR. LUCA BELLI - Então, eu acho que é o grande avanço que aporta o PL 4.752, mas também pode ser complementado com anos de estudo. Literalmente, passamos um ano e meio trabalhando a cada semana, duas horas, com um colega do CNCiber, para criar também um texto que possa subsidiar esse processo. Então, todas essas sugestões já estão lá também nessa minuta de Lei Geral de Cibersegurança. É identificado como critério fundamental a comunicação, a coordenação regulatória, mas também entendimento do caráter multidimensional da cibersegurança. Eu vou falar para vocês, muito sinceramente, 20 anos de experiência me levam a acreditar que a lei e a agência sejam o mínimo. Não podemos dizer que com uma lei e uma agência vamos resolver a cibersegurança, mas vamos começar a construir a cibersegurança no país.

Então eu acredito que a identificação dessa complementaridade...

(Soa a campainha.)

O SR. LUCA BELLI - ... seja o mínimo indispensável para construir a cibersegurança no país. Precisamos entender que a lei é essencial, porém a proteção da infraestrutura crítica precisa dialogar com a ciberdefesa, precisa dialogar com a proteção dos direitos das pessoas, precisa dialogar com a segurança da informação, precisa transformar também - como foi falado muito claramente - as pessoas, neste momento no Brasil, que são um elo fraco da cibersegurança, no elo forte, com capacitação, educação e uma política industrial que possa investir no desenvolvimento de tecnologia brasileira, de soluções brasileiras, como foi falado muito bem pelo colega Fragola. Eu não me canso de falar - há cinco anos, temos também mais um estudo sobre a soberania digital e inteligência artificial no Brasil - que a construção da cibersegurança e a construção da soberania digital não são um custo, são um investimento, são uma oportunidade de ouro para se criar um novo setor da economia, para se aprimorar a proteção da infraestrutura crítica, para se aprimorar a proteção de direitos de brasileiros e brasileiras...

(Soa a campainha.)

O SR. LUCA BELLI - ... e tudo isso criando empregos.

Então, eu agradeço muito pela oportunidade, mais uma vez. Eu peço desculpas por ter falado demais e fico à disposição, claramente, para contribuir nesse processo, em nome meu pessoal, mas também da FGV, do Centro de Tecnologia e Sociedade da FGV.

Muito obrigado.

A SRA. DAMARES ALVES (Bloco Parlamentar Aliança/REPUBLICANOS - DF. *Fora do microfone*.) - Você pode dar um livro de presente para mim?

O SR. LUCA BELLI - Eu vou dar os três livros de presente para você, especialmente, que me pediu.

(Manifestação da plateia.)

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado, Sr. Luca.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - Como é que diz? Quem não chora, não mama. *(Risos.)*

O SR. LUCA BELLI - Todos os livros têm acesso livre na biblioteca da FGV, eu não estou aqui para vender o livro, é para divulgar conhecimento. Então, cada livro está em acesso livre.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - No caso concreto, chorou e levou. *(Risos.)*

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado.

Eu passo agora a palavra ao Sr. Belisario Contreras, Diretor-Executivo da Digi Americas Alliance.

O SR. JORGE SEIF JÚNIOR - Seu português está em teste, Belisario.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - Muito bem! Força!

O SR. BELISARIO CONTRERAS (Para expor.) - Boa tarde, senhoras e senhores. Gostaria de agradecer o convite para participar desta importante audiência.

Eu, antes de tudo, gostaria de parabenizar o Brasil pela emocionante vitória de ontem sobre o Japão, foi muito importante.

Em nome da Digi Americas Alliance, gostaria de parabenizar o Brasil pela liderança em uma base de cibersegurança e governança digital. Há muito tempo, é uma referência na América Latina para políticas digitais e a legislação atualmente em discussão representa mais uma importante oportunidade para fortalecer o futuro digital do país.

Parabenizamos também os Senadores Amin, Moro, Seif, Astronauta Marcos Pontes e colega Diego Araújo por sua liderança, visão e compromisso à frente da Frente Parlamentar de Cibersegurança.

Manifesto também, em nome próprio, meu sincero desejo de que o Senador Amin seja reeleito para que possamos continuar contando com sua valiosa liderança e dedicação na promoção da agenda estratégica no Brasil.

Hoje, gostaria de concentrar minha apresentação principalmente na proteção infantil *online*, um dos maiores desafios da política pública digital da nossa região, e, ao final, compartilhar algumas observações gerais sobre o projeto de lei de cibersegurança em debate.

Em toda a América Latina, cada vez mais crianças utilizam tecnologias digitais para educação, comunicação, saúde, entretenimento e participação na sociedade. A conectividade digital torna-se essencial para o desenvolvimento econômico e social. Ao mesmo tempo, o cenário de riscos evolui significativamente. As crianças enfrentam cada vez mais riscos, como

aliciamento *online*, exploração do abuso sexual infantil, *cyberbullying*, conteúdos prejudiciais, violações de privacidade, amplificação algorítmica de conteúdos nocivos e novos desafios decorrentes da inteligência artificial e de tecnologias emergentes. Esses riscos continuam crescendo na escala da complexidade. Um relatório recente elaborado pela Digi Americas analisa esses desafios em toda a América Latina e identifica tanto lacunas nas políticas públicas quanto soluções práticas para enfrentá-las.

O estudo apresenta algumas conclusões centrais.

Primeiro, proteger crianças no ambiente digital não deve ocorrer à custa da privacidade, da liberdade de expressão e do acesso significativo a tecnologias digitais. Segundo, nenhum ator conseguirá enfrentar esse desafio sozinho. Governo, setor privado, sociedade civil, educadores e pais são responsáveis pelas próprias crianças terem papel fundamental nessa agenda.

(Soa a campainha.)

O SR. BELISARIO CONTRERAS - Terceiro, a experiência internacional demonstra que os modelos mais bem-sucedidos combinam segurança e privacidade, regulação baseada em riscos, cooperação estrutural entre o Governo e o setor privado, cooperação internacional e educação digital.

O Brasil já possui importantes ativos nessa agenda, incluindo instituições sólidas de proteção de dados, iniciativas como o SaferNet, e capacidades crescentes em cibersegurança. Sobre o projeto de lei, há recomendações específicas - novamente, parabéns por todo o texto -, primeiro, sobre algumas práticas internacionais. A primeira recomendação é garantir clareza na governança e na definição de responsabilidades institucionais. A definição de infraestruturas críticas e dos agentes regulados devem estar harmonizadas com o marco jurídico já existente, evitando sobreposição de competências, conflito regulatório e insegurança jurídica.

Esperamos também que a futura...

(Soa a campainha.)

O SR. BELISARIO CONTRERAS - ... Agência Nacional de Cibersegurança seja concebida como uma instituição autônoma, com independência técnica, capacidade de coordenação e recursos adequados, sem estar subordinada a outro órgão federal. Um país com a relevância estratégica e o protagonismo global do Brasil merece um compromisso sólido, responsável e de longo prazo com a cibersegurança e as tecnologias emergentes, reconhecendo que esses temas são fundamentais para a segurança nacional, competitividade econômica, inovação e confiança digital.

Segundo, abordar uma abordagem baseada em riscos. As obrigações de cibersegurança devem ser proporcionais ao risco efetivamente apresentado, especialmente em temas como cibersegurança de cadeias e suprimentos, gestão de vulnerabilidades e requisitos de conformidade.

Terceiro, reconhecer o modelo de responsabilidade compartilhada. Serviços digitais modernos, especialmente computação em nuvem e plataformas digitais, operam sob o modelo de responsabilidade compartilhada. A legislação deve definir claramente as responsabilidades de provedores, operadores e usuários, refletindo a realidade tecnológica atual.

E o quarto: promover segurança jurídica e implementação viável. Definições claras, critérios objetivos para aplicação de lei...

(Soa a campainha.)

O SR. BELISARIO CONTRERAS - ... prazos racionais para adaptação e um regimento sancionatório proporcional contribuem para ampliar a resiliência cibernética, estimular investimentos e incentivar inovação.

O Brasil tem oportunidade de consolidar sua posição como referência regional, tanto na proteção infantil como na construção de um marco modelo moderno de cibersegurança. As políticas públicas mais eficazes serão aquelas capazes de conciliar segurança, inovação, direitos fundamentais e colaboração multissetorial.

Muito obrigado.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado, Sr. Belisario. Eu vou conceder a palavra agora à Sra. Luana de Brito Tavares Diniz, remotamente.

A SRA. LUANA DE BRITO TAVARES DINIZ (Para expor. *Por videoconferência*.) - Bom dia, bom dia a todos e a todas. Quero agradecer muito pela audiência de vocês, pelo convite; agradecer...

Só um minutinho, por gentileza, eu vou tentar bloquear o ruído. Talvez esteja passando aí para vocês, um segundo. *(Pausa.)*

Vocês estão me ouvindo?

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Positivo.

A SRA. LUANA DE BRITO TAVARES DINIZ (*Por videoconferência*.) - Obrigada, obrigada. Bom dia a todos. Queria agradecer novamente o convite. Meu nome é Luana Tavares, eu represento aqui a Aliança Multissetorial pela Cibersegurança e o INCC (Instituto Nacional de Combate ao Cibercrime).

Quanto à Aliança, só para reforçar aqui, diversas organizações que já falaram, especialistas e outros participantes aqui, fazem parte dela. Ela é composta pela Fecomércio SP, a Febraban, Fiesp, Abes, Abramed, FIM, Acrefi, Acate, Brasscom, a Gasa (Global Anti-Scam Alliance), Capítulo Brasil, Assespro, Fenainfo, a Anvint (Associação Nacional das Vítimas de Internet) e o Instituto Peck de Cidadania Digital.

Então, a gente tem, no nosso grupo, o setor produtivo, financeiro, tecnológico, academia, sociedade civil, atuando em consenso. Quero agradecer aqui novamente ao Senador Esperidião e, na pessoa dele, cumprimentar todos os demais Senadores e autoridades presentes.

Quero dizer que é um prazer para o INCC, para a Aliança, colaborar na construção desse processo desde o início, desde a criação da frente parlamentar, na construção inicial do primeiro texto do marco legal e, agora, nesta audiência para instruir a partir da maturidade que nós ganhamos ao longo desse processo.

Eu tenho uma apresentação, mas eu vou falar, porque eu acho que eu aproveito melhor o tempo, compartilho com vocês essa apresentação e também uma nota técnica que foi elaborada pelo nosso time e pelos membros da Aliança, com as contribuições escritas da nossa análise aqui em relação ao marco legal, em que nós concentramos a maior parte das nossas sugestões justamente em pontos que já foram mencionados aqui - alguns deles - da integração entre o anteprojeto, a proposta feita pelo GSI, pelo Comitê Nacional de Cibersegurança, integrando ao marco nacional, entendendo que eles são extremamente complementares.

Nós temos ali, no trabalho do marco legal, um trabalho programático e federativo; e, na minuta do CNCiber, a gente já olha de uma forma mais regulatória e operacional, tornando um pouco mais tangível a governança, a gestão de riscos e a fiscalização.

O que a gente sugere, nesse substitutivo, é que a gente institua, então, o Sistema Nacional de Cibersegurança - já foi mencionado aqui -, a autoridade nacional com autonomia técnica e harmonização regulatória, preservando Bacen, ANPD, Anatel, Aneel, sem duplicar obrigações; a regulação baseada em risco, que já está mais detalhada também nessa minuta do CNCiber; o reporte unificado de incidentes, que já foi muito mencionado aqui também; a proteção de infraestruturas críticas; e a integração com o combate a crime, com a cooperação entre PF, polícias civis, MP, Judiciário, inteligência, e, então, trazer esse princípio de granularizar e de detalhar um pouco mais essas responsabilidades e a integração.

Eu queria deixar aqui uma última sugestão, Senadores e Senadora Damares, de que nós também aproveitemos este momento de discussão do debate do marco legal para falar sobre os cidadãos vulneráveis, idosos, crianças, as vítimas pessoas físicas. Aqui a gente tem falado, no momento em que a gente está de maturidade da discussão, de uma infraestrutura um pouco maior, uma coordenação nacional maior, com definições mais claras em relação à regulamentação, mas um estágio que nós precisamos dar atenção especial - talvez dentro desse texto, para aproveitar a tramitação, ou talvez num outro texto que seja complementar a esse - é aos cidadãos vulneráveis, às PMEs, à educação digital, que já foi colocada aqui, inclusive sugerindo incluir na Base Nacional Comum Curricular, como já vem sendo discutido no Conselho Nacional de Educação, e atenção às tecnologias emergentes, como foram colocadas aqui.

Acredito que a gente conseguiu sintetizar aqui num documento praticamente a maior parte das colaborações que foram feitas, e vamos compartilhar essa nota com todos, para que a gente consiga avançar na elaboração do texto e, talvez, incluir também essas questões adicionais, que são tão críticas, para que a sociedade consiga sentir, de uma forma mais rápida, os efeitos do marco legal, entendendo que a gente ainda tem algumas etapas para serem complementadas.

Então, encerrando aqui, para cumprir o tempo acordado, eu agradeço, em nome da Aliança e em nome do INCC, a oportunidade de participar e de contribuir com este processo, colocando o nosso time todo à disposição dos Senadores, da equipe, das consultorias e de todos os membros aqui presentes.

Muito obrigada e um ótimo dia a todos.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado à Sra. Luana de Brito Tavares Diniz, fundadora e CEO do Instituto Nacional de Combate ao Cibercrime (INCC). Muito obrigado à senhora.

Eu passo a palavra, agora, à Patricia Peck. É assim? *(Pausa.)*

Com a palavra, Patricia.

A SRA. PATRICIA PECK (Para expor.) - Olá, boa tarde a todos.

Queria agradecer aqui, cumprimentando o Presidente da Mesa, o Senador Hermes, ao Senador Esperidião Amin, pelo convite, em especial, também aqui ao Senador Jorge Seif, ao Senador Marcos Pontes, à Senadora Damares e ao Senador Sergio Moro, por essa bancada tão representativa da pauta de cibersegurança no Brasil.

Agradeço também, de forma muito honrosa, ao Instituto Peck de Cidadania Digital, o qual represento, assim como ao Instituto Empoderar.

Eu tenho a oportunidade de trazer algumas sugestões. Vamos fazer a juntada depois, assim como os colegas. Hoje eu também integro o CNCiber; então acho que estamos bem representados aqui, e os colegas também já fizeram algumas falas.

Eu atuo, há 25 anos, com direito e tecnologia, com 57 livros publicados, e tenho o estudo do doutorado voltado para inteligência artificial e cibersegurança. Participo do Guardião Cibernético há anos e tenho até uma sugestão depois para a gente ter um Guardião Mulheres, porque eu acho que seria muito bom.

Eu vim aqui representar uma pauta que, além da pluralidade, é diversidade. E fico feliz com a participação da Luana, do INCC, de termos mulheres aqui nessa fala, porque a cibersegurança precisa também estimular mulheres em cibersegurança desde pequenininhas, para que elas também queiram participar disso.

Eu queria fazer esse primeiro comentário, aqui colocando algumas informações.

Deixe-me ver se eu consigo... Acho que ele não está indo. Você consegue passar para mim? *(Pausa.)* Ah, para cá! Acho que foi.

São algumas informações que são dados críticos, porque nós vivemos um apagão de cibersegurança no Brasil. Eu acredito que não existe soberania do Estado brasileiro se não for uma soberania digital e uma soberania quântica.

Aproveito a fala do Senador Marcos Pontes para reiterar que, além do medo que nós temos hoje no país, esta é uma pauta que beira o ciberterrorismo...

(Soa a campainha.)

A SRA. PATRICIA PECK - ... pensando naquilo que a gente tem que proteger do brasileiro.

Dito isso, eu queria acrescentar que a minuta do PL 4.752 e a minuta apresentada pelo CNCiber não são concorrentes, mas complementares, como já colocamos aqui. Temos vivido uma situação de falhas sistêmicas, e acredito, sim, como colocado pelo Senador Esperidião Amin, que nós temos que buscar uma lei boa, que seja aperfeiçoada ao longo do tempo. Não precisamos de uma lei perfeita, como não tivemos em outras ocasiões, como a própria LGPD, como um exemplo, que continua sendo algo que está amadurecendo.

Além disso, queria aproveitar para destacar para todos a importância que nós temos hoje de cooperação. Isso foi, inclusive, pergunta do João, de São Paulo, e eu digo: João, temos que cooperar, só assim a gente vai garantir mais segurança ao cidadão brasileiro.

E é um assunto que envolve educação, financiamento, políticas públicas... A questão trazida pelo Anderson...

(Soa a campainha.)

A SRA. PATRICIA PECK - ... do Rio Grande do Sul, também traz esse ponto.

Precisamos de uma rede central de alertas de ação imediata.

E a Giovanna, de Santa Catarina, perguntou como vamos ajudar as pequenas empresas. Temos que ter também uma atuação de indicação pelo Sistema S ou até um incentivo fiscal para que a gente possa realmente ter um Brasil com mais cibersegurança.

Definitivamente, esta proposta exige que nós possamos fomentar essa diversidade com uma harmonização regulatória, com apoio a PMEs, com proteção de inovação e inteligência artificial e, principalmente, com diversidade e educação.

E, falando dos públicos vulneráveis, como foi colocado aqui pelos demais colegas, eu estou entregando aqui em mãos, em seguida, aos Senadores, uma proposta para que a gente atualize o Estatuto do Idoso, para que, assim como a gente fez com o Estatuto da Criança, que virou o Estatuto da Criança Digital (ECA Digital), nós façamos o Estatuto do Idoso Digital, porque isso é uma necessidade preeminente para o Brasil. Nós sabemos que, hoje, ninguém a partir de 60 parece idoso, nós estamos tão bem conservados, mas, com toda certeza, o idoso...

(Soa a campainha.)

A SRA. PATRICIA PECK - ... precisa ser protegido também.

Muito obrigada.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado à Patricia Peck, que é Presidente do Instituto Peck de Cidadania Digital e Membra Titular do Instituto Empoderar. Muito obrigado.

Eu passo, agora, para Marta Helena... "Chuque"? É isso?

(Intervenção fora do microfone.)

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Diretora de Seguros Cibernéticos da Howden Brasil.

(Intervenção fora do microfone.)

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Com a palavra.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC. *Fora do microfone*.) - É do Rio Grande?

A SRA. MARTA HELENA SCHUH (Para expor.) - Gaúcha. Sim, do Rio Grande do Sul.

Exmos. Srs. Senadores, autoridades aqui presentes e demais membros desta Comissão, muito boa tarde.

Como profissional que acompanha diariamente as evoluções de cibersegurança e ameaças digitais no Brasil, é uma honra poder contribuir com este debate histórico do PL 4.752 e o anteprojeto da Lei de Cibersegurança.

O avanço desse marco regulatório estabelece um paradigma fundamental para o país: a transição da resposta reativa para uma cultura baseada em gestão de riscos, a resiliência digital e a corresponsabilização. No entanto, a eficácia de uma lei não se mede pelo rigor das suas exigências, mas pela capacidade real da sociedade em aderi-la. E é justamente nessa lacuna que o mercado segurador pode ajudar com as ações necessárias a essa implementação.

A minha contribuição aqui é estritamente técnica. Eu venho falar de um lugar em que há 11 anos eu atuo: na gestão de riscos no Brasil, que, consequentemente, impacta a ação financeira dos incidentes cibernéticos. Eu acredito que ambos os projetos têm algumas lacunas em que nós podemos contribuir de forma proativa e com dimensões que possam atingir o resultado requerido.

O primeiro é a viabilização econômica da inclusão digital, que muito foi falada aqui com os demais colegas. Acredito que o maior desafio regulatório certamente é o alto custo da implementação das estruturas operacionais, especialmente para as PMEs. E aqui o mercado segurador pode ser um facilitador econômico, especialmente para esse grupo de empresas, porque, além da proteção financeira diante de um incidente cibernético, nós do mercado segurador oferecemos, juntamente com a contratação da apólice, um arcabouço de ferramentas que possam ajudar na proteção e na inserção dessas pequenas e médias empresas na esteira de regulação e governança.

O segundo é a subscrição do risco com a indução de certificação proativa, é a certificação na prática. Isso porque, para a contratação de uma apólice, há pré-requisitos básicos em relação à governança, à segurança e às necessidades de resposta. Consequentemente, isso pode ser algo que venha a ser uma ferramenta complementar na supervisão indireta do Estado na relação em que haja o cumprimento da esfera da lei.

O terceiro é o apoio à resposta incidente e à resiliência nacional. A baixa maturidade técnica da média das indústrias brasileiras reflete-se especialmente no tempo de resposta e consequências que o incidente cibernético possa trazer. O seguro cibernético não se limita aos prejuízos financeiros. O seu maior valor público está justamente no fornecimento de respostas imediatas juntamente com o painel qualificado.

(Soa a campainha.)

A SRA. MARTA HELENA SCHUH - Nós somos parte interessadas no risco quando isso acontece. É nosso dever e nossa necessidade também mitigar as ações consequentes que possam ocorrer. E isso, então, funciona como uma extensão direta da capacidade de resposta do próprio Estado, minimizando os impactos econômicos e garantindo os serviços essenciais para a sociedade.

E, por último e não menos importante, a produção de inteligência e supervisão indireta. O mercado segurador é um dos maiores geradores de dados empíricos sobre a realidade cibernética. Nós coletamos métricas sobre a frequência e a severidade, os vetores de ataques e fazemos um monitoramento econômico e contínuo das ações que se desdobram diante de um incidente.

Para a sociedade e para o Estado, isso traz benefícios. Especialmente para o Estado, traduz-se numa maior eficiência regulatória, redução de custo na fiscalização e uma maior resiliência nacional. Para o setor privado, traz previsibilidade financeira, melhoria contínua da governança e uma *expertise* altamente especializada a um custo não oneroso. E para a

sociedade, a gente tenta trazer o menor impacto dos incidentes, maior continuidade nos serviços e confiança digital, além do elemento crítico para a economia da cidadania e do ambiente.

Então, senhores, os projetos legislativos em debate criam uma base de sistema moderna, mas dependem crucialmente de ferramentas de indução eficazes. Nós, do mercado de seguradores, podemos não ser, de forma isolada...

(Soa a campainha.)

A SRA. MARTA HELENA SCHUH - ... apenas um catalisador em relação à governança cibernética, mas integrar especialmente as estruturas do Sistema Nacional de Cibersegurança, o CNCiber e os ISACs, que estão sendo estruturados para o monitoramento.

Reconhecer o seguro cibernético como uma ferramenta estratégica na política pública pode reduzir as consequências econômicas de um incidente.

Fico à disposição.

E muito obrigada.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado, Sra. Marta Helena.

O SR. SERGIO MORO (Bloco Parlamentar Vanguarda/PL - PR. Para interpelar.) - Presidente, pela ordem aqui...

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Com a palavra, Senador.

O SR. SERGIO MORO (Bloco Parlamentar Vanguarda/PL - PR) - Aproveitando a exposição da Sra. Maria Helena...

(Intervenção fora do microfone.)

O SR. SERGIO MORO (Bloco Parlamentar Vanguarda/PL - PR) - Marta, perdão. Minha visão aqui está um pouco prejudicada.

Parabéns, primeiro, pela exposição.

E queria aproveitar a fala de V. Sa. para indagar: como é que está, dentro do mercado brasileiro, a disseminação do seguro cibernético? É um seguro exclusivo para esse... Ou normalmente é feita uma apólice mais ampla que inclui o risco cibernético? Como é? Se pudesse descrever um pouquinho para nós esse mercado...

A SRA. MARTA HELENA SCHUH (Para expor.) - Perfeito.

No Brasil, a adesão ainda é muito baixa, apesar de haver produtos para todas as esferas e indústrias. Então, hoje, é um produto estruturado unicamente para a proteção digital, inclui também a questão de fraudes, e não está inserido apenas para ações maliciosas oriundas de *hackers*. A gente tem visto também a questão de falhas sistêmicas que podem provocar desdobramentos equivalentes a uma ação maliciosa.

Se a gente comparar o mercado americano com o mercado brasileiro, hoje o mercado brasileiro tem cerca de R$300 milhões em prêmios emitidos no Brasil. No mercado americano, já são US$10 bilhões anuais, porque há, efetivamente, um incentivo à adesão para reduzir as consequências econômicas. E, como eu mencionei, não é só a transferência, mas traz todo um arcabouço que traz uma governança junto e ferramentas. Então, a gente trabalha com a sociedade como um todo, a gente trabalha com as empresas de tecnologia para introduzir novas ferramentas e, quando novas ameaças, novas tecnologias surgem, que possam trazer decorrências, a gente atualiza os nossos *frameworks* e as nossas necessidades de subscrição para que isso se reflita.

Então, converge muito bem com o que o Senador Esperidião Amin mencionou: que nós não podemos fazer uma estátua, que governança cibernética é algo contínuo. Nesses últimos 11 anos em que eu venho fazendo isso, a gente vê a evolução tanto das ameaças quanto as necessidades de as empresas se atualizarem em termos da sua governança e de implementação de novas ferramentas para o monitoramento disso.

A SRA. PATRICIA PECK (Para expor.) - Senador Moro, só um complemento.

Nós acompanhamos lá no escritório várias entidades que querem o seguro cibernético. O *checklist*, o questionário que você tem que responder para conseguir a apólice é bem longo, bem detalhado e dificilmente preenchível por pequenas e médias empresas. Então, grandes empresas até conseguem ter; mais da metade das empresas grandes que a gente conhece possuem. Inclusive, lá nós também temos um ótimo produto...

A SRA. MARTA HELENA SCHUH - Patricia, se me permite a palavra, nós estruturamos um produto com três perguntas, para PME...

A SRA. PATRICIA PECK - Está ótimo.

A SRA. MARTA HELENA SCHUH - ... e com acesso a partir de R$1 mil anuais, com essa esfera de proteção. Então, o mercado...

A SRA. PATRICIA PECK - Então, não tem desculpa mais! *(Risos.)*

A SRA. MARTA HELENA SCHUH - ... se atualizou em relação a isso; sim, era um dificultador até recentemente, mas nós avançamos com essa necessidade ao entender que as PMEs estão inseridas dentro das grandes empresas também como fornecedores e, consequentemente, isso se tornou necessário para que trouxéssemos um produto que refletisse a realidade delas.

A SRA. PATRICIA PECK - Excelente! Vou divulgar mais também.

A SRA. MARTA HELENA SCHUH - Por favor! *(Risos.)*

A SRA. PATRICIA PECK - Parabéns.

Aproveito para também fazer um agradecimento aqui especial ao Senador Mourão pelo convite do requerimento.

Obrigada.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado.

Eu vou passar agora para o Sr. Patrick Aron Rinski, Diretor-Executivo da Unidade 42 da Palo Alto Networks.

O SR. PATRICK ARON RINSKI (Para expor.) - Bom dia, Exmos. Senadores, demais autoridades, convidados, senhoras e senhores.

Cumprimento de forma especial os Senadores autores do projeto de lei e dos requerimentos que ensejam esta audiência pública, especialmente os Senadores Esperidião Amin, Jorge Seif, Chico Rodrigues, Astronauta Marcos Pontes, Damares e Sergio Moro. Faço um agradecimento especial ao Senador Hermes Klann pelo convite para participar deste debate superimportante.

Represento hoje a Palo Alto Networks, uma empresa global especializada em soluções de cibersegurança, e a sua Unidade 42, uma das organizações de inteligência de ameaças, consultoria e respostas a incidentes do mundo. Diariamente, processamos globalmente mais de 500 bilhões de eventos de segurança, traduzidos em 17PB provenientes de mais de 85 mil clientes, o que nos confere uma visibilidade sem precedentes sobre o comportamento dos adversários.

O Brasil atravessa um momento crítico de transformação digital, e esse projeto de lei representa um passo relevante para o fortalecimento da soberania digital brasileira. O desafio agora é assegurar que o futuro marco legal gere ganhos concretos de resiliência cibernética, evitando que a sua implementação se limite a requisitos formais de conformidade.

No campo da cibersegurança, a conformidade meramente estática pode criar uma falsa sensação de segurança: produz documentos e registros, mas nem sempre reduz riscos de forma efetiva. Se regulamentarem a segurança cibernética como algo lento e anual, estaremos indefesos diante de adversários que operam em milissegundos e já utilizam a inteligência artificial para mapear vulnerabilidades sem descanso.

Para que este projeto alcance sua real eficácia, a implementação da futura estrutura nacional de governança da cibersegurança, envolvendo o CNCiber e a autoridade nacional prevista no projeto, deve estar ancorada em resultados operacionais mensuráveis e em uma abordagem baseada em riscos.

As maiores potências do mundo já abandonaram esse modelo obsoleto de auditoria de papel, que atesta a segurança apenas no dia da inspeção. Hoje, o sucesso é medido...

(Soa a campainha.)

O SR. PATRICK ARON RINSKI - ... pela capacidade de detectar, conter e remediar ameaças em tempo real.

O Brasil já deve observar o que está funcionando globalmente.

Na União Europeia, marcos como o NIS2 e o Dora indicam uma tendência clara: a segurança cibernética deve ser tratada como uma gestão contínua de risco, com *report* tempestivo de incidentes e atenção especial a terceiros e prestadores críticos. Lá, a lei exige a gestão contínua de riscos de terceiros e trata o relato de incidentes não como uma burocracia, mas como uma ferramenta de defesa ativa.

Nos Estados Unidos, a abordagem já tem avançado para a maior responsabilidade executiva, uso de métricas dinâmicas e adoção de referências como o *framework* do Nist Cybersecurity. No Reino Unido, observa-se uma abordagem baseada em resultados, com menor ênfase em prescrever tecnologias específicas e maior foco em limites de riscos, falhas operacionais

e proteção da inovação. O padrão deixou de ser apenas perguntar se uma violação ocorreu. A pergunta central passou a ser o quão rapidamente ela foi detectada, contida e remediada.

Nossa legislação deve ser neutra em tecnologia, focando em resultados operacionais em vez de exigir apenas a conformidade estática. Precisamos instituir a cultura da visibilidade contínua, monitorar o ambiente digital 24 horas por dia, como um sistema de radar que nunca desliga e não apenas um documento que se assine uma vez por ano.

A América Latina enfrenta desafios relevantes na identificação precoce de ameaças e na capacidade da detecção de ambientes críticos. Em muitos casos, os invasores conseguem permanecer por longos períodos em redes críticas antes de serem detectados, acumulando informações e ampliando o potencial de dano. Precisamos de indicadores objetivos, como os tradicionais MTTD e MTTR, tempos médios de detecção e tempos médios de resposta, além da eficácia da interrupção desses ataques.

O compartilhamento de inteligência entre instituições públicas e privadas deve ser automatizado e contínuo. Se um banco ou órgão governamental sofre um ataque, os indicadores desse ataque devem ser compartilhados de forma segura, automatizada e tempestiva, para que outros sistemas possam reforçar suas defesas antes de serem atingidos.

O projeto deve transformar os centros de detecção e resposta a incidentes e centros de compartilhamento de informações...

(Soa a campainha.)

O SR. PATRICK ARON RINSKI - ... em um verdadeiro sistema imunológico nacional. A futura autoridade nacional pode e deve exercer um papel que vá além da fiscalização, atuando também como instância de coordenação, orientação técnica, integração entre Governo, setor privado, academia e sociedade.

Devemos exigir protocolos de compartilhamento de dados que sejam legíveis por máquina. Diante do volume e da velocidade das ameaças, processos exclusivamente manuais tendem a ser insuficientes. A definição de infraestrutura crítica deve ser dinâmica e baseada em risco sistêmico, não apenas o que é essencial hoje, mas também aquilo cuja interrupção possa gerar impactos relevantes na cadeia.

O projeto pode estimular diretrizes técnicas modernas sem engessar tecnologias específicas. Em primeiro lugar, precisamos modernizar a identidade. Mecanismos tradicionais de autenticação, como aqueles baseados exclusivamente em SMS, já se mostram insuficientes diante de ataques mais sofisticados. Precisamos migrar para a gestão contínua de postura de identidade.

Em segundo lugar, a contenção deve ser automatizada.

(Soa a campainha.)

O SR. PATRICK ARON RINSKI - Em determinados cenários, sistemas de segurança devem estar aptos a isolar ativos comprometidos de forma totalmente automatizada e supervisionada, reduzindo assim o risco de propagação do ataque.

Por fim, também será necessário avançar em mecanismos de proteção específicos para sistemas de inteligência artificial, capazes de monitorar o comportamento de modelos, identificar usos indevidos e interromper fluxos maliciosos em tempo real.

Srs. Senadores e convidados da CCT, termino com uma analogia simples: o nosso espaço aéreo nacional é protegido por radares e caças que agem de forma instantânea. Se uma aeronave hostil invade nosso território, não esperamos meses para agir. A defesa é imediata, porque o risco é existencial. O domínio digital exige, dessa mesma maneira, a urgência. Ao adotar métrica baseada em resultados, investir em contenção automatizada e promover uma governança verdadeiramente adaptativa, o Brasil poderá avançar de uma postura predominante reativa para uma estratégia mais preventiva, coordenada e resiliente.

A autoridade nacional de cibersegurança...

(Soa a campainha.)

O SR. PATRICK ARON RINSKI - ... deve reconhecer que a infraestrutura crítica dependerá cada vez mais de sistemas autônomos de inteligência artificial e de identidades de máquina e tecnologias criptográficas que podem permanecer operacionais por décadas.

Não estaremos aprovando apenas uma lei, estamos construindo a espinha dorsal de uma nação digital resiliente, capaz de prosperar sem medo.

Agradeço novamente o convite desta Comissão e coloco a Palo Alto Networks à disposição para contribuir tecnicamente com o aperfeiçoamento desse marco legal da cibersegurança e com a futura regulamentação.

Muito obrigado.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado ao Patrick.

Eu vou passar a palavra agora ao Rodrigo Marinho, CEO do Instituto Livre Mercado.

O SR. RODRIGO MARINHO (Para expor.) - Senhoras e senhores, boa tarde. É um prazer falar aqui.

Senador Hermes Klann, demais Senadores e grandes e queridos amigos que estão compondo a mesa, é um prazer e um privilégio estar aqui.

A fala do senhor e do Senador Seif, Senador Esperidião, foi muito relevante em dizer que há uma estátua. O projeto de lei aprovado sobre a lei de inteligência artificial aqui foi feito antes de existir ChatGPT, Claude e IA Generativa de forma geral. Então é para ter muito, muito cuidado em fazer projetos que avancem tremendamente na iniciativa privada, que não é o caso do projeto que foi apresentado pelo Senador Esperidião Amin e por demais membros da Frente Parlamentar. É um projeto excelente, é principiológico, traz base, permite avanço, permite que haja um nível de regulação infralegal melhor, permite que haja adesão voluntária dos entes subnacionais. Ou seja, Senador Moro, caso Governador, consiga chegar lá e criar o que ele pensa como centro de cibersegurança do Paraná, ele poderá trazer inovações que não são centralizadas em Brasília, que é sempre um risco temerário, até porque Brasília não tem a mínima ideia do que é o Amazonas, não tem a mínima ideia do que é o Paraná, nem a mínima ideia do que é Santa Catarina, são lugares absolutamente diferentes e que precisam ser tratados dessa forma. Ela usa padrões nacionais - o projeto de lei original -, traz transparência e traz todos os pontos relacionados a isso.

Eu confesso que, como liberal, tenho muito medo de criação de novas entidades estatais. Tenho um receio imenso. Temos poucas agências reguladoras, né? Temos imensas agências reguladoras. Aqui, em 2019, foi criada a Autoridade Nacional de Proteção de Dados, com a seguinte fala, Senador Esperidião: "não será transformada em agência reguladora porque não terá custo". Adivinhem o que aconteceu agora este ano? A Autoridade Nacional de Proteção de Dados virou a Agência Nacional de Proteção de Dados e agora passará a ter custo, entidade, base, briga por recurso, briga por receita, porque infelizmente recursos são escassos. Infelizmente, mas é um dado da realidade: recursos são escassos, necessidades são infinitas.

(Soa a campainha.)

O SR. RODRIGO MARINHO - Isso acontece hoje e acontecerá amanhã. A economia não vai conseguir mudar por conta disso e é muito temerário trazer uma nova entidade para criar algo num Estado já gigantesco que nós temos na realidade brasileira.

A minuta... O que me preocupa mais... Eu confesso que a minuta original tem pontos de interação, mas esse diálogo eu já tenho feito com o Diego, com o Seif, com o Esperidião; e o Instituto Livre Mercado tem sugestões de melhoramento, Senador Hermes Klann, para o texto, mas eu me preocupo com alguns temas apresentados. E eu acho que vou ser voz dissonante aqui sobre a minuta do CNCiber. Acho que fui feliz em dizer que estamos no Brasil e vamos usar, Senador Esperidião, a expressão brasileira.

Problema 1: classificação ampla de infraestruturas digitais como serviços essenciais. Isso pode aumentar custos, com risco de sobreposição à Ensic e Plansic já existentes. Eu confesso que tenho muito medo, toda vez que eu vejo segurança nacional e soberania nacional. Na década de 80, nós criamos uma lei de informática em nome da segurança nacional e no Brasil...

(Soa a campainha.)

O SR. RODRIGO MARINHO - ... foi a década do atraso. Para vocês terem uma ideia, importar computador era descaminho.

Há um livro muito interessante sobre o Banco Garantia, *Sonho Grand*e, em que se diz que tinha um computador para apresentar para fiscalização e um computador para operar. Não é isso que nós queremos para a realidade brasileira.

Soberania tecnológica aqui tem que ser definida de forma mais clara. É temerário, é perigoso, é sempre um termo aberto. Norma de controle aberto é sempre algo que pode ter risco de preferência, que é outra coisa que causa muito receio. Se a gente vai dar preferência sempre a entidades nacionais, nós prejudicamos criação de *know-how*, criação de novos produtos e concorrência de fato. Para que os produtos nacionais... A WEG, no estado de vocês, é um exemplo de uma empresa nacional que disputa no planeta Terra - não porque tem benefício setorial, mas porque é boa, porque ela funciona. E a WEG é uma referência no planeta por ser uma das melhores em motor elétrico. É exatamente a ampla concorrência que permite isso.

Problema 3: enquadramento automático de nuvem e extensão a fornecedores diretos e indiretos. O nível de regulação é enorme - para o pequeno, para o grande, para o médio. A preocupação trazida pela Marta e pela Patricia foi clara: o

pequeno vai ser retirado desse mercado se for apresentado dessa forma. Nós vamos afastar aqueles pequenos *players* - e aqui eu estou me limitando, Senador Seif, à proposta, à minuta do CNCiber.

Problemas cautelares amplos, multas a rodo... Isso é sempre temerário. Para a iniciativa privada, é sempre perigoso, principalmente quando é relacionado a bloqueio de tráfego, desconexão por até 72 horas...

(Soa a campainha.)

O SR. RODRIGO MARINHO - Isso exige, óbvio, um devido processo legal, uma chamada - quem vai se defender, como vai se dar isso, qual é a forma disso -, até porque há um receio sempre, sempre de censura. Já vimos isso acontecer em alguns momentos. Há um receio sempre de censura.

E, por fim, a obrigação de Etir própria gera custo elevado. Já existem modelos setoriais compartilhados que podem trabalhar.

Acho que esses são os pontos centrais. Se a gente for definir soberania digital, tem que amarrar e não pode deixar isso para o infralegal. É preciso dizer exatamente o que é, porque, óbvio, tem que ser uma definição de Estado, e não uma definição de governo.

A nossa proposta é saber claramente onde os dados estão armazenados - nós temos que ter consciência de onde estão armazenados -, quem pode acessá-los, qual o controle granular disso.

Na semana passada, todo o Brasil, grande parte do Brasil, recebeu uma mensagem... Defesa Civil, segurança nacional, tudo ali envolvido, Senador Marcos Pontes. E nós descobrimos que há dois anos a senha não era trocada. Não precisa ter uma grande coisa de cibersegurança, não, amigo; é trocar a senha, é ter um processo para trocar a senha. Não precisa de lei para isso, não. Isso é o básico. Se eu estou pensando em cibersegurança no Brasil e eu tenho um canal de comunicação efetivo para grandes desastres...

(Soa a campainha.)

O SR. RODRIGO MARINHO - A nossa vizinha Venezuela acabou de viver um desastre; todos os sentimentos e orações para que tenha o mínimo de mortes possível na Venezuela.

Você viu o que aconteceu no momento em que a senha não foi trocada.

Criptografia, obviamente para não ler sem autorização - é muito feliz a parte de criptografia quântica trazida -, resiliência operacional, ou seja, camadas para poder funcionar.

É óbvio que o projeto é necessário para o Brasil. E, no momento, nós estamos discutindo diversos projetos, seja na Câmara, seja no Senado.

O de *data center* é um projeto fundamental ao país e está parado no Senado Federal. Ele é fundamental. Nós temos a oportunidade de liderar esse mercado, e esse projeto não anda. Existe um projeto apresentado na Câmara hoje de *digital market act*, de criar um local que vai servir para censura dentro do Cade. É isso que está sendo criado na Câmara dos Deputados. Tem um projeto de stablecoin muito positivo sendo votado. Tem um projeto, que está aqui na Casa, de segregação patrimonial em bitcoin que precisa avançar.

(Soa a campainha.)

O SR. RODRIGO MARINHO - Tem um projeto pronto para ser votado de infraestrutura de mercado financeiro, que abre novas bolsas, novas possibilidades, que também está dentro do mercado digital na interoperabilidade.

Então, há vários avanços, o Brasil precisa fazer acontecer e evitar que haja um retrocesso. O cuidado central é sempre ter muito cuidado de não se tornar uma estátua. Repito, a lei de IA do Brasil, a lei de IA no Senado, foi aprovada antes de ter IA generativa. Então, a gente tem que ter muito cuidado, porque a inovação não para.

E é aquela história: nós podemos participar, nós podemos estar à frente, mas a gente tem que estar participando do mercado para que isso aconteça. Se a gente só faz a segurança, soberania nacional... A gente já tem precedente no Brasil, quem viveu a década de 80 sabe que foi um atraso absurdo que este país viveu.

O SR. ASTRONAUTA MARCOS PONTES (Bloco Parlamentar Vanguarda/PL - SP. Pela ordem.) - Sr. Presidente, pela ordem. Eu só gostaria de fazer um comentário, somando àquilo que eu falei inicialmente, e à palavra do Rodrigo também, que já vem participando de muitas audiências públicas aqui. Esse ponto vem corroborar, vem somar àquilo que eu falei: a necessidade de um trabalho que seja interligado e muito amplo. Não vai resolver só com uma agência, com uma... Isso não resolve. Precisa ser uma coisa interligada, um sistema para trabalhar junto.

Inclusive, falou da parte de educação, da inclusão, né? Foi falado aqui, se eu não me engano, pela Patricia também, sobre a inclusão, da necessidade de incluir não só, como se falou, as mulheres, mas também falo dos idosos. Eu tenho um projeto

de lei, se eu não me engano, é o 3.167, de 2023, que está lá na Câmara, para a inclusão digital para idosos. Mas isso também precisa ser um trabalho sistêmico, um trabalho sistêmico feito de uma forma muito cautelosa, como foi colocado aqui, porque senão você prejudica certos sistemas.

É igual a reforma tributária, tem que ser feito de uma forma muito cautelosa, muito bem-feita, senão alguns sistemas, algumas partes do sistema vão ser prejudicadas. O Redata está aqui parado - eu tenho falado disso já faz um bom tempo -, ele está aqui estacionado, e a gente está perdendo dinheiro para o país, literalmente é isso - não dá para colocar de outra forma -, a gente está perdendo dinheiro. Ele precisa andar para a frente. Quanto à infraestrutura do país - também foi chamada a atenção -, a gente precisa ter essa infraestrutura funcionando.

Eu lembro quando nós fizemos lá - eu era Ministro das Comunicações - a primeira preparação para o leilão de 5G, teve toda uma preocupação com a China, com os produtos das empresas chinesas, mas tem que se levar em conta que, se nós temos uma proteção técnica adequada - e isso se precisa ter -, não tem que ter esse tipo de receio, tem que trabalhar para o país, tem que trabalhar para render para o país aqui. E o setor privado é aquele que provê esses recursos, que provê emprego, etc. Não pode haver essa separação de nós contra eles. Isso não existe em lugar nenhum em que dá certo.

Só para ressaltar isso que a gente vive falando aqui, na Inteligência Artificial nós falamos muitas vezes isto: essas leis têm que ser feitas de uma forma que favoreça o país - favoreça o país -, sem medo de atacar aquilo que precisa ser atacado e de se fazer a coisa correta.

Obrigado.

O SR. PRESIDENTE (Arlindo Chinaglia. Bloco/PT - SP) - Obrigado, Senador. Obrigado ao Rodrigo Marinho.

Agora nós vamos passar a palavra ao Vinícius Malacco Ferreira, Gerente de Subscrição de Linhas Financeiras na Tokio Marine Seguradora. Remotamente, óbvio.

O SR. VINÍCIUS MALACCO FERREIRA (Para expor. *Por videoconferência*.) - Bom dia a todos e muito obrigado pelo convite.

Gostaria só de fazer uma observação inicial de que a minha fala é feita em caráter pessoal e técnico, como especialista em seguros contra riscos cibernéticos, e não representa necessariamente a opinião do meu empregador. Eu participo deste debate a convite da FenSeg, cuja subpermissão de linhas financeiras eu integro.

Eu concordo plenamente com o que foi dito pelo Senador Jorge Seif e reforçado pelo Senador Marcos Pontes, de que a preocupação com cibersegurança é absolutamente necessária, mas ela não pode se transformar em um obstáculo ao progresso tecnológico, à inovação e à digitalização da economia.

É justamente nesse espaço que eu acho que esse pedido de riscos cibernéticos pode exercer um papel muito relevante de dar suporte e segurança a esse desenvolvimento tecnológico. Ele não substitui o investimento em segurança da informação, governança, prevenção à resposta a incidentes, mas oferece uma camada adicional de proteção e previsibilidade para que empresas, entidades públicas e operadores de serviços relevantes possam inovar com mais segurança. Em outras palavras, o seguro pode ajudar a dar conforto econômico e operacional ao desenvolvimento tecnológico, porque contribui para a resposta a incidentes, para a recomposição de perdas, para a retomada das atividades e para a preservação da continuidade de serviços essenciais.

No caso dos riscos cibernéticos, especialmente em setores críticos, serviços essenciais e operadores de importância sistêmica, eventuais ataques podem gerar impactos econômicos, sociais, operacionais e institucionais que ultrapassam a organização afetada.

Por isso, mecanismos de mitigação e transferência de riscos, como o seguro, podem ser aliados importantes de uma agenda de inovação responsável.

Muito obrigado pelo espaço.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC) - Presidente, o senhor me concede um pequeno espaço?

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Sempre, Senador Amin.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Aliança/PP - SC. Pela ordem.) - Em primeiro lugar, eu quero cumprimentá-lo pela condução democrática, aberta, liberal da coleta de sugestões. Quero cumprimentar todos os que se deslocaram até esta reunião, alguns de fora do país - não é isso, Belisario? - e que têm sido parceiros, ao longo do tempo, na construção de uma ideia básica, que é o que foi apresentado.

Como eu sou o signatário do projeto, quero mais uma vez dizer que longe de mim a pretensão de ser o autor dele, mas alguém tinha que apresentá-lo, e o Presidente da frente parlamentar subscreveu. Mas foi um projeto fruto de muitas

contribuições, que agora estão sendo replicadas, corrigidas ou enriquecidas. E caberá ao Relator, com a ajuda da nossa consultoria, fazer o trabalho legislativo, legiferante, fazer a lei, com todas as cautelas que foram aqui realçadas.

Eu repito: os mais críticos ao projeto de lei reconhecem que ele não engessa, ele não bloqueia o dinamismo da criatividade, da inovação, que anda galopando pelo mundo afora. Todos os relatos aqui mostram que o galope, se é que não... O galope é muito lento para expressar. A velocidade com que se contesta, se disputa, se apresenta o certo, o atual é inédita na história da humanidade. Inteligência artificial, segurança cibernética, ataque cibernético, quer dizer, esse conjunto, mais a computação quântica, significa uma velocidade como nunca houve no mundo, em matéria de discussão do que é atual para a vida que nós estamos a viver.

Então, eu queria cumprimentá-lo, cumprimentar as contribuições e fazer votos a ambos - uma vez que o Senador Hermes representa aqui o mesmo mandato que o do Senador Jorge Seif - de que este relatório possa, em breve, ser entregue. Nós temos um ano atípico, um ano de eleição, mas seria muito importante que ele evoluísse para uma aprovação em Comissões do Senado e pudesse, sem nenhuma preocupação, começar a ser apreciado na Câmara dos Deputados, como ocorre com outros projetos. Neste caso, a Frente Parlamentar de Defesa Cibernética, no marco legal, teve um papel extraordinário, e o número de Senadores que por aqui passaram demonstra isso.

Eu vou ter que me ausentar. O senhor vai ter que dar a conclusão da reunião, com a certeza de que nós cumprimos o dever democrático de abrir este espaço. O Senador Seif e o senhor têm todos os elementos para um parecer atualizado, e eu, como Relator, participo desse enriquecimento de texto, com a convicção de que nós estamos cumprindo o dever de nos manter atualizados.

Muito obrigado.

O SR. JORGE SEIF JÚNIOR - Pela ordem, Sr. Presidente.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado, Senador Amin.

Senador Seif.

O SR. JORGE SEIF JÚNIOR - Senhoras e senhores, quero reiterar o agradecimento já feito pelo Senador Esperidião Amin.

Pelo nível das entidades aqui representadas, sejam públicas ou privadas, nós temos a convicção da importância do tema para a nossa nação, para as empresas, para o desenvolvimento econômico e, acima de tudo, para a proteção do cidadão brasileiro.

Eu quero deixar aqui consignado com as senhoras e senhores e peço urgência no envio do material posto aqui pelas senhoras e pelos senhores. O *e-mail* é o seguinte: cct@senado.leg.br - CCT é a abreviação de Comissão de Ciência e Tecnologia.

Quero fazer aos senhores também uma observação: esta frente parlamentar foi criada, como já foi dito aqui, com convidados interessados, que foi recorde com relação a qualquer outra frente parlamentar já criada no Brasil, e também as autoridades aqui, representando as senhoras e senhores, liderados pelo Senador Esperidião Amin, Senador Sergio Moro, Senador Astronauta, Senadora Damares, Senador Hermes Klann e também o Senador Jorge Seif, este que vos fala. Vejam a seriedade com que nós estamos tratando o assunto. Vocês se deslocarem de suas residências, de suas empresas e até de locais fora do Brasil mostra também a preocupação das senhoras e senhores.

E o nosso compromisso, enquanto Relatores desse projeto, eu e o Senador Hermes Klann, é que nós vamos nos debruçar, junto com a nossa consultoria aqui da Comissão, junto com o jurídico do nosso Senado, e também observando... Eu confesso aos senhores que eu estou pessoalmente, particularmente, trabalhando nos textos e buscando conciliação nas diversas sugestões que nós recebemos, tanto nas viagens que nós fizemos, para dentro e fora do Brasil, com as entidades que nós temos conversado, com as empresas, que têm total liberdade, com os órgãos de governo, Exército, Abin e outras entidades governamentais. Nós temos, assim, nos debruçado com muita responsabilidade, com muito cuidado também - o Rodrigo Marinho também fez observações importantíssimas. Nós temos, assim, nos dedicado para fazer uma legislação contemplativa com todas as preocupações que as senhoras e os senhores já demonstraram aqui, e muitas delas, inclusive, são recorrentes, e muitos dos comentários aqui das senhoras e senhores se sobrepõem, mostrando que é uma preocupação não só de um setor, não só de uma entidade, não só de uma empresa, mas da maioria das senhoras e senhores.

Então, repito: cct@senado.leg.br. Apressem-se, porque o Brasil tem pressa, os senhores têm pressa, e, acima de tudo, a população brasileira tem pressa de que nós apresentemos esse relatório. Muitas vezes o processo legislativo é um pouco lento, diante das necessidades e desafios e das preocupações que todos nós temos, enquanto cidadãos, brasileiros ou não, de empresas e de instituições.

Então, muito obrigado, de coração, em nome do Senado da República, em nome do instituto de cibersegurança, de segurança cibernética. Quero agradecer as contribuições, o deslocamento das senhoras e senhores, as contribuições, importantes contribuições dos diversos setores para que nós façamos, ou melhor, cheguemos a uma legislação que contemple, acima de tudo, o nosso Brasil de forma moderna, sem ser engessada, mas dinâmica, e ouvindo, especialmente num processo completamente democrático, ouvindo todas as senhoras e senhores, e os contemplando nessa legislação.

Muito obrigado.

O SR. PRESIDENTE (Hermes Klann. Bloco Parlamentar Vanguarda/PL - SC) - Muito obrigado, Senador Seif.

Só quero comunicar que, por meio do e-Cidadania, recebemos de cidadãos algumas manifestações, que estarão disponíveis no *site* da Comissão, no Portal do Senado.

Senhoras e senhores, encerramos esta audiência pública com a certeza de que o debate de hoje cumpriu seu propósito. As exposições e os diferentes pontos de vista apresentados enriquecem a análise do Projeto de Lei 4.752, de 2025, e contribuirão para a construção de um relatório tecnicamente consistente, equilibrado e atento às demandas da sociedade. A cibersegurança deixou de ser um desafio apenas tecnológico: ela é uma questão de soberania, de proteção das instituições, da economia, das empresas e, sobretudo, dos cidadãos brasileiros.

Como Relator da matéria, recebo com muita responsabilidade todas as contribuições aqui apresentadas, que serão cuidadosamente avaliadas durante a elaboração do parecer.

Agradeço aos convidados pela disponibilidade, aos Senadores presentes, às equipes técnicas e a todos que acompanharam esta audiência. Muito obrigado a todos.

Nada havendo a tratar, agradeço a presença de todos, e declaro encerrada a presente reunião. *(Palmas.)*

(Iniciada às 11 horas e 11 minutos, a reunião é encerrada às 13 horas e 32 minutos.)