



(Texto com revisão.)

O SR. PRESIDENTE (Jean Paul Prates. Bloco Parlamentar da Resistência Democrática/PT - RN. Fala da Presidência.) – Declaro aberta a 16ª Reunião da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática do Senado Federal da 3ª Sessão Legislativa Ordinária da 56ª Legislatura.

A presente reunião ocorre de modo semipresencial com a utilização do sistema de videoconferência adotado pelo Senado Federal e se destina à realização da terceira audiência pública com o objetivo de debater a implementação das redes móveis de quinta geração (5G) no País, os benefícios para os seus usuários, os desafios e as oportunidades da indústria 4.0, além de aprofundar questões relativas à segurança cibernética das redes que serão implementadas, em cumprimento ao Requerimento nº 16, de 2021, da CCT, de minha autoria, e ao Requerimento nº 17, de 2021, da CCT, de autoria do Senador Vanderlan Cardoso, visando a subsidiar a avaliação da política pública de implementação das redes móveis de quinta geração (5G) no exercício 2021.

O público interessado em participar da audiência pública poderá enviar perguntas e comentários pelo endereço www.senado.leg.br/ecidadania ou ligar para o telefone 0800-0612211. Já temos algumas perguntas aqui, que vou ler ao final.

Na nossa audiência de hoje, vamos debater dois temas muito importantes: a segurança das redes móveis 5G e a indústria 4.0.

Para você que está em casa nos assistindo, a indústria 4.0 ou a chamada quarta revolução industrial é uma expressão que engloba um amplo sistema de tecnologias avançadas, como inteligência artificial, robótica, internet das coisas, computação em nuvem, *big data*, realidade virtual, enfim, tecnologias que estão mudando as formas de produção e os modelos de negócios no Brasil e no mundo.

O foco da quarta revolução industrial é justamente a melhoria da eficiência e da produtividade dos processos. E o que tem a ver isso com 5G? A tecnologia das redes móveis de quinta geração vai permitir que todo esse sistema possa se integrar e atender à sociedade e às empresas com eficiência e agilidade.

Para isso, é importante que tenhamos confiança na proteção e segurança de todas essas tecnologias funcionando, sem que tragam prejuízos à soberania e à economia do País, aos dados dos cidadãos e ao funcionamento das empresas.

Imaginem o quanto essas tecnologias poderão beneficiar a melhoria da educação, da pesquisa, do desenvolvimento, da inovação, o quanto as empresas poderão aumentar sua capacidade produtiva!!

E qual a segurança que temos hoje? Os dados pessoais dos cidadãos e cidadãs, das empresas, seus planos de negócio, sua produção, seus dados estratégicos, a economia do País e das empresas, estarão todos protegidos?

Por isso também convidamos, aqui, especialistas em cibersegurança para que possam nos dar um panorama de como estamos hoje e de como será com a implantação da tecnologia 5G.

Vou aproveitar este momento para fazer algumas indagações, antecipar algumas perguntas, a fim de que nossos convidados possam responder durante suas apresentações.

Uma dúvida que temos diz respeito à Instrução Normativa GSI nº 4, editada em 26 de março de 2020, que dispõe sobre os requisitos mínimos de segurança cibernética que devem ser adotados no estabelecimento das redes 5G. À época da publicação desse



normativo, houve receio de que alguns fornecedores de equipamentos não pudessem implantar suas redes no Brasil.

Hoje, entre os principais fabricantes de equipamentos de telecomunicações, que, inclusive, estão aqui presentes na audiência, existe algum que não tenha se qualificado a fornecer seus equipamentos para as redes 5G no Brasil?

Outra questão diz respeito às obrigações dos licitantes vencedores da faixa de frequência em 3,5GHz, que prevê a implantação da rede privativa de comunicação da Administração Pública Federal, ao custo estimado de R\$1 bilhão. Uma vez que essa rede está fornecida por fornecedores privados, por prestadores de serviços privados, quais são as exigências que contribuirão para tornar as comunicações do Governo Federal mais seguras?

Por fim, tendo em vista que, embora a segurança cibernética seja componente essencial para as redes 5G, as vulnerabilidades das redes de comunicação podem permitir ataques criminosos nos mais diversos setores, que podem resultar em prejuízos incalculáveis para a economia do País e até para a segurança nacional.

O que se deve fazer para tornar as redes de comunicação mais seguras?

Como o Governo brasileiro busca defender o País e minimizar os efeitos dos ataques de uma possível guerra cibernética ou também de terrorismo cibernético?

Essas são algumas questões que nós já gostaríamos de deixar registradas e que podem ser respondidas por todos os convidados e convidadas.

Encontram-se presentes, no plenário da Comissão, os seguintes expositores: Victor Hugo da Silva Rosa, Coordenador-Geral de Gestão de Segurança da Informação, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR); Marcela Carvalho, Assessora Especial da Presidência da Agência Brasileira de Desenvolvimento Industrial (ABDI); Jacqueline Lopes, Diretora de Relações Institucionais da Ericsson para o Cone Sul da América Latina; Wilson Cardoso, Diretor de Tecnologia da Nokia América Latina.

Encontram-se presentes, por meio do sistema de videoconferência – e eu aproveito para saudá-los e desculpar-me pelo atraso –, os seguintes expositores: Renato da Fonseca, Superintendente de Desenvolvimento Industrial da Confederação Nacional da Indústria (CNI); Arthur Pereira Sabbat, Diretor do Conselho da Autoridade Nacional de Proteção de Dados (ANPD); Marcelo Motta, Diretor de Cyber Security da Huawei América Latina; Roberto Gallo, Diretor-Geral da Kryptus.

Agradeço, portanto, a presença de todos e de todas.

O Senador Vanderlan fez também um requerimento para esta audiência. Ele se encontra em voo, portanto justifico a ausência dele, que teria justamente a oportunidade aqui de falar. Certamente fará comentários se conseguir chegar ao destino a tempo; se não, obviamente em outras ocasiões, nesse trabalho contínuo que estamos fazendo aqui na fiscalização desta política.

Já, iniciando o nosso debate, gostaria de dividir nossa audiência em dois blocos, para ficar mais didática para os nossos espectadores. Primeiro, tratar da indústria 4.0 e, em seguida, da segurança cibernética. Sabemos que os temas são transversais, mas é apenas para ouvirmos, primeiro, os representantes das indústrias e, depois, tratarmos então da cibersegurança. Creio que assim fica mais fácil para o cidadão que está em casa, a cidadã, também entender e acompanhar esse processo.

Dessa forma convido, para sentar à Mesa, a Sra. Marcela Carvalho, que está aqui, presencialmente, e é Assessora Especial da Presidência da Agência Brasileira de Desenvolvimento Industrial (ABDI), para sua exposição, a quem já dirijo – aproveito para



dirigir – uma pergunta que eu também gostaria que o nosso próximo convidado da CNI respondesse, que é a seguinte.

Com a implantação da indústria 4.0 no Brasil, que se espera que o 5G permita, há uma expectativa de um aumento significativo da produtividade das atividades econômicas no País. Por outro lado, existe o risco de eliminação de postos de trabalho, elevando as taxas de desemprego – e isso nos preocupa muito. Por isso, quais são as estimativas mais recentes sobre os impactos sociais e econômicos esperados com a transformação do modelo de produção para a indústria 4.0? Como o poder público deve direcionar as suas políticas para a geração de emprego nesse contexto?

Agora, sim, por favor, a Sra. Marcela Carvalho, a quem concedo a palavra por dez minutos.

A SRA. MARCELA CARVALHO (Para expor.) – Bom dia a todos.

Senador Jean Paul, muito obrigada pelo convite.

Cumprimento todos os presentes, que estão nos assistindo aqui, presencialmente ou por meio da página do Senado no YouTube.

Bom, como os senhores sabem, a ABDI tem natureza de serviço social autônomo, ligada ao Ministério da Economia, por meio de um contrato de gestão, e nossa atuação hoje vai no sentido de acelerar – ou pelo menos induzir a aceleração – a transformação digital no setor produtivo nacional e também na indústria, principalmente na indústria, por meio da adoção e difusão de novas tecnologias, especialmente as tecnologias 4.0, que o Senador mencionou há pouco, ou quarta revolução industrial, que também é uma outra forma de se referir a essas tecnologias.

E de que forma fazemos isso? Bom, a ABDI hoje atua no sentido de tentar minimizar os riscos da adoção dessas tecnologias, ao fazer testes, projetos-piloto. E através desses projetos, a gente consegue ter informações acuradas de cases reais que depois são difundidas para todos os setores da economia. E, assim, a gente consegue demonstrar benefícios de uma adoção tecnológica, custos dessa adoção. Porque, veja bem, se o investimento em tecnologia é feito sem que se saiba quais os benefícios, quais os custos, erros e acertos, esse industrial, essa empresa pode optar por não fazer, por não ter essas informações. Então, a redução do risco é um alvo da nossa atuação.

E, por outro lado, a ABDI por vezes testa tecnologias para auxiliar no processo de regulamentação dessas tecnologias, com base em evidências de políticas públicas e no processo regulatório. Esse foi o caso das redes de 5G, mas as redes de aplicação privada 5G. Então, são casos que não foram abrangidos pelo leilão acontecido recentemente, mas as redes de dedicação privada, as redes privadas que podem ser implantadas aí pela indústria, comércio, varejo, enfim, logística, inúmeras aplicações.

Bom, dito isso, de que forma o 5G vai impactar, então, os nossos processos produtivos, não só no Brasil, mas no mundo? O 5G foi concebido especialmente para a conexão entre máquinas e equipamentos. Então, a gente costuma falar que não é mais um G, do 4G. Ele tem características muito específicas que fazem com que ele seja muito atraente para as aplicações industriais, de saúde, nas cidades e na educação. Então, onde o 5G se mostra mais disruptivo é exatamente nesses ambientes que eu mencionei. Por quê? Porque ele tem características muito especiais de confiabilidade da rede, de capacidade de transmissão de dados, de capacidade de ligar equipamentos à rede de forma quase que infinita, milhões de equipamentos ligados à rede, e com uma latência muito baixa. E a latência é exatamente o tempo de envio dos dados e a resposta desses dados. Então, se a gente fala de uma latência de um milissegundo, por exemplo, a gente está falando de respostas em tempo real, o que permite aplicações em telemedicina, por



exemplo, de uma cirurgia remota, e operação de um guindaste de forma remota; enfim, todas essas aplicações.

Na indústria, o que a gente espera, então, de uma aplicação de 5G é uma maior flexibilidade na planta industrial, versatilidade, redução de custos e também aumento de produtividade.

Então, Senador, imagine que a gente consiga, por exemplo, realizar a manutenção preventiva de máquinas, colocando ali um dispositivo de IoT *machine learning* para que a gente consiga, antes de o equipamento quebrar ou apresentar um defeito, fazer reparos que não sejam aqueles em que seja preciso parar a produção industrial para que a gente consiga fazê-lo. Isso traz produtividade. Tempo na produção, além de produtividade, é economia de custos e mais recursos para o industrial no fim do dia. Além disso, aplicações na logística e outras aplicações.

Então, a gente fala que o 5G é o grande habilitador disso tudo, porque ele é uma espécie de guarda-chuva que coloca embaixo dele essas tecnologias 4.0 e faz com que essas tecnologias mostrem a sua capacidade máxima de operação; então, é uma disruptão.

No caso da ABDI, a gente tem atuado na questão das redes privadas. Firmamos um Acordo de Cooperação Técnica com a Anatel (Agência Nacional de Telecomunicações) e, por meio desse ACT, a gente, a ABDI precisa testar o 5G em três ambientes: na indústria, no agronegócio e nas cidades, em cidades inteligentes. O primeiro piloto já aconteceu, já está em andamento. Trata-se de uma aplicação que fizemos na fábrica da Weg em Jaraguá do Sul, Santa Catarina, que é uma das fábricas mais automatizadas do grupo Weg. Aplicamos lá, colocamos duas redes distintas: uma rede que é operada por uma Telecom, uma operadora que é o que a gente chama de não *stand-alone* – a Ericsson, que está aqui presente, e a Claro fizeram essa rede para nós –; e a segunda rede é uma rede totalmente privada, uma rede que tem a característica de ser uma rede fechada para a indústria, que foi implantada pela Nokia, que também está aqui presente. Nós comparamos o desempenho dos casos de uso nessas duas redes, e o que se viu é que o 5G hoje, o que a gente tem de evolução tecnológica, que é o Release 15 do 3GPP, que é uma evolução da tecnologia, as características do 5G trouxeram velocidade em torno de 80% do limite teórico, que é exatamente o que já é necessário para várias aplicações, como por exemplo: robôs de inspeção, câmeras inteligentes, aplicação de realidade virtual para controle de qualidade nas fábricas. Então, estamos extremamente satisfeitos com os resultados.

E um resultado indireto desse teste é exatamente trazer luz ao setor produtivo nacional, as informações com relação a custos/benefícios – custo de implantação das redes – e onde essas redes podem ser melhor aplicadas, porque há casos em que um 4G resolve; então, como podemos aplicar da melhor forma possível com relação a custo/benefício.

Respondendo à pergunta do Senador – meu tempo está acabando –, eu menciono o seguinte: a gente sabe que o 5G deve adicionar... Há dados muito diferentes, em termos de valores, do que o 5G vai trazer em termos de mercado para os operadores 5G e para a indústria em termos de produtividade, eficiência etc. Por quê? Porque a gente tem todas essas estimativas com base nas aplicações que a gente já conhece hoje. Mas o grande barato do 5G é que existirão aplicações que a gente nem conhece. Então, por exemplo, o CEO da TIM menciona que a gente vai ter 23 bilhões adicionados em dez anos com a chegada do 5G na indústria e a criação de 200 mil novos empregos formais.



De fato, é uma estimativa, e a criação de empregos vai se dar com certeza, mas saberemos aproveitar esses empregos? A forma como isso vai acontecer vai depender exatamente das políticas públicas para treinamento e qualificação dos profissionais hoje que atuam nessas fábricas, de forma que eles consigam operar um mundo em que essa tecnologia é uma realidade, em que as tecnologias 4.0 são uma realidade.

Então, políticas públicas voltadas a treinamento e qualificação técnicos são extremamente necessárias neste momento. Enfim, haverá criação de empregos e haverá, sim, substituição de empregos. O que se diz no mundo inteiro é que o saldo será positivo, mas os governos precisam atuar no sentido de treinar seus funcionários, sua mão de obra, seus trabalhadores.

Eu acho que paro por aqui e fico à disposição para responder perguntas, Senador.

Obrigada mais uma vez.

O SR. PRESIDENTE (Jean Paul Prates. Bloco Parlamentar da Resistência Democrática/PT - RN) – Obrigado, Marcela. Excelente!

Isso, de fato, projeta não só a necessidade de a gente ter a consciência de formar pessoas, mas, como esses empregos, esses postos de trabalho são atividades novas que ainda não foram nem sequer concebidas – vão ser concebidas ao longo do tempo –, eu acho que o essencial aqui é que as escolas, lá na base, lá desde a formação básica mesmo, tenham acesso ao 5G ou pelo menos a um 4G de qualidade, enfim, universalizado, porque essas pessoas terão que, na sua infância e no seu estudo mais básico, já ter contato com a agilidade e o acesso à internet de qualidade, porque, senão, não adianta: nós vamos ter mais concentração e esses novos empregos irão sempre para as mesmas pessoas que vão estar concentradas nos lugares em que terão acesso desde pequenos e terão o hábito de atuar diante da indústria 4.0 e de toda essa cibernetica nova.

Então, novas funções são muito bem-vindas, com certeza vai haver transformação nas faixas de emprego, do trabalho, e nós temos sempre que precisar de mão de obra também para o trabalho que não está ligado à rede. Porque há coisas que... Por exemplo, para produzir alimentos, não se produz na web, não adianta. Levar coisas de um lado para o outro nunca vai ser... Ainda não chegamos ao ponto daquela desmaterialização de um lado para chegar ao outro lado, o da Jornada das Estrelas – nós não estamos nesse ponto. Então logística, agricultura, outras coisas, por mais mecanizadas que sejam, têm sempre um fator humano por trás. O conflito é esse e o conflito é mundial, não é, Marcela? Isso não é uma questão brasileira apenas. Mas a preocupação de nós estarmos na frente dos outros países e na frente de todos esses outros regimes com certeza nos assola, nós teremos que fazer face a isso.

Eu queria passar a palavra também, no mesmo tema, e aproveitar a presença do Renato da Fonseca, que é Superintendente de Desenvolvimento Industrial da CNI, para justamente dar prosseguimento, por dez minutos, a esse mesmo debate inicial.

Obrigado, Renato.

O SR. RENATO DA FONSECA (Para expor. *Por videoconferência.*) – Obrigado, Senador Jean Paul. Inicialmente, agradeço, em nome da Confederação Nacional da Indústria, o convite. Esse tema é importantíssimo para nós.

Muito boa a apresentação da Marcela. Vou usar várias coisas do que ela coletou.

Vou pedir licença para apresentar aqui algumas informações, para facilitar. Espero que vocês já estejam visualizando.

O SR. PRESIDENTE (Jean Paul Prates. Bloco Parlamentar da Resistência Democrática/PT - RN) – Está o.k. aqui.



O SR. RENATO DA FONSECA – O primeiro tópico, Senador, foi exatamente o que V. Exa. colocou em termos das revoluções industriais. Acho que isso é importante também na resposta do emprego.

Esse dado, esse gráfico aí, que é quase uma linha reta, mostra o PIB *per capita* do Reino Unido de 1270 a 2016. Ou seja, o mundo, a humanidade, passou um período grande da sua existência numa relação onde praticamente os fatores de produção eram fixos. Então, você tinha problemas de superpopulação, com doenças, às vezes resolvidos com guerras, busca por territórios. A partir do momento em que a gente tem a Revolução Industrial, ali no final do século XVIII, você percebe que essa curva começa a ter um crescimento do PIB *per capita* – é o PIB dividido pela população do Reino Unido – muito forte. Isso acontece no mundo todo.

A primeira com a mecanização. Motor a vapor; depois, a gente tem a energia elétrica, motor a combustão; o advento da organização da linha de produção, com as linhas de montagem. E aí, a segunda revolução industrial: veio o carro, o automóvel, ou seja, a cultura, a sociedade muda. A terceira revolução industrial veio ali na década de 70, com a automação, com chegada dos computadores, com robótica sendo introduzida na produção. Começa também uma mudança ímpar da sociedade.

Nós estamos hoje vivendo o que se chama de indústria 4.0, exatamente para se fazer referência à quarta revolução industrial. Acredito que vai ser confirmado esse nome, porque nós temos mudança não só no processo produtivo, mas na sociedade. A sociedade se digitalizou. E essa revolução é exatamente quando junta a questão digital com o físico, onde a gente mistura esses dois mundos. Isso muda o nosso padrão de vida.

Em termos da indústria, a gente tem, obviamente, um elevado ganho de produtividade, ou seja, a gente tem mais eficiência no processo produtivo. Não é apenas você estar com um robô – isso foi feito na década anterior –, mas é que você está ligando esse robô com sensores. Você está sabendo exatamente o que se passa, seja se uma máquina está aquecendo muito, seja se o ritmo de produção diminuiu em alguma etapa. E o sistema permite até conversas entre as próprias máquinas, ou seja, apenas com uma supervisão, e ele começa a se autorregular, evitando desperdício ou uma parada muito prolongada. A gente flexibiliza a linha de produção. A gente, alguns anos atrás, era quase que refém da padronização.

Há uma frase famosa do Henry Ford dizendo que qualquer um poderia escolher a cor do seu Ford, desde que fosse preta. Por quê? Porque era muito difícil ficar mudando a cor do veículo. Então, quando a gente tinha, na automobilística, algumas décadas atrás, a linha de produção de um determinado modelo, só se produzia aquele modelo. Hoje, não. Hoje, com a robotização, com a digitalização, com essa integração, a gente pode, numa mesma linha de produção, produzir modelos diferentes, produzir carros personalizados. Já é possível você escolher a cor do assento, a cor do carro, o tipo de painel, ou seja, como você faz isso no carro, você também faz isso no tênis, você faz isso em outros produtos. Então, a gente tem uma massificação da personalização, ou seja, é uma coisa que parece controversa, mas esse é um grande ganho.

E essa mistura do virtual com o real: você não faz mais um protótipo físico; você faz um protótipo virtual. O tempo de lançamento do produto é muito grande. O comissionamento de novas máquinas, quando você está expandindo a sua fábrica, é feito virtualmente primeiro, e depois a máquina entra e não perturba o fluxo de produção. No passado, se você colocava uma máquina nova, às vezes levava semanas para fazer o *setup* dessa máquina, para fazê-la funcionar com o resto da cadeia.



E novos modelos de negócios, ou seja, a gente tem novos modelos surgindo neste mundo.

Como isso está no Brasil?

A gente fez uma pesquisa em 2016 em que 48% das empresas utilizavam pelo menos uma tecnologia digital, de indústria 4.0. E acabamos de fazer uma pesquisa agora – vai ser divulgada nos próximos dias – que aponta 69% das empresas. Obviamente, o índice é muito mais concentrado, acima de 80%, de grandes empresas utilizando essas tecnologias.

Assim como em outros países, o uso inicial da digitalização é muito mais dentro do processo produtivo, com máquinas com sensores, com produção mais flexível. Então, apesar desse número maior de empresas utilizando a tecnologia digital, nós estamos ainda no início desse processo, de aproveitar essas oportunidades que a Marcela citou na sua apresentação. Metade das empresas, principalmente as pequenas e médias, utilizam no máximo até três tecnologias digitais das 18 que nós listamos nessa pesquisa. Então, é um processo que ainda está no seu início.

E qual é a dificuldade?

A gente tem uma dificuldade que é o baixo incentivo à inovação. O Congresso vem discutindo mais de uma vez a questão do FNDCT, que é um fundo para inovação, ou seja, apesar da crise, apesar da questão fiscal, a gente não pode menosprezar o impacto da inovação no crescimento, como a gente viu naquele gráfico inicial. Sem inovação, a gente não consegue voltar a crescer a taxas superiores a 2%, 3% ao ano, o que este País não faz há cerca de dez anos.

Falta de trabalhador qualificado. A questão educacional é importantíssima. O novo ensino médio é fundamental que seja implementado de fato – está nesse processo, nesse início de processo. Por quê? Hoje no Brasil, por exemplo, apenas 9% dos estudantes do ensino médio fazem, concomitantemente, a educação profissional. O que significa isso? A maioria dos alunos que termina o ensino médio são preparados para fazer o Enem, não são preparados para ir trabalhar. E cerca de 20% apenas conseguem chegar à universidade. O que esses outros 80% vão fazer? Eles vão ter que aprender uma profissão depois do ensino médio. Nos países europeus, mais da metade dos alunos do ensino médio fazem junto o ensino profissional, uma educação profissional. E isso é importante para já ir formando esses jovens, e obviamente uma educação profissional com a digitalização preparando para a 4.0, para que eles cheguem ao mercado de trabalho qualificados.

Nós temos o segundo problema que é o estoque, quantidade de trabalhadores. Com a maioria das pessoas aqui já formada, eu, vocês todos, a gente precisa se adaptar à tecnologia digital. O Senador citou a questão das crianças, a criança até é mais fácil; criança pega um celular e comece a mexer rapidamente. Eu, por exemplo, custei muito a usar várias das vantagens que o celular nos permite, ou seja, não é apenas um instrumento de falar. Eu tenho certeza de que há várias outras que eu não consigo, que eu não conheço, que eu não sei utilizar ainda. Então, essa capacitação da digitalização para trabalhar com as máquinas é importantíssima. A gente precisa fortalecer essa requalificação desses trabalhadores.

As próprias empresas têm pouco conhecimento – são novas tecnologias –, não têm conhecimento adequado do custo de implantação. Muitas acham que isso tem que ser implementado de maneira imediata em toda a empresa; isso não é verdade, isso pode ser feito gradualmente, dentro até do plano de revisão de manutenção de investimento das



empresas. E esse trabalho da ABDI e o trabalho da CNI de levar essa informação, de fazer esses testes é importantíssimo.

E há a infraestrutura, quando a gente cai na 5G. A Marcela ressaltou bem, a 5G é um novo mundo. Obviamente, os representantes das empresas vão ter mais informações técnicas muito melhores do que a minha, mas só para dar uma olhada entre as tecnologias que foram evoluindo da década de 80 até agora, a gente tem um salto, em relação à 4G, de uma velocidade de 1GB para 10GB – alguns estudos mostrando que o pico pode chegar a até 20GB –, e principalmente uma taxa de latência, ou seja, de resposta de demora, muito pequena.

Então, vou dar um exemplo fácil. Eu ainda sou do tempo em que... Uma vez eu tive que ir a São Paulo, a gente precisava de um mapa, a grande inovação era o Guia Quatro Rodas, que botou o mapa num livro. A gente ficava abrindo, mudando de página e dirigindo isso. Isso realmente muda para o Waze, muda para Google Maps. Só que às vezes também você está dirigindo e a resposta do Google Maps demora. Isso faz com que você perca aquela entrada. A 5G vai acabar com isso praticamente. Você vai dar mais segurança, e isso vai permitir que as empresas usem novas tecnologias, aumentem o seu investimento em digitalização e passem a regular a distância. Você confia num trator, num caminhão ou numa colheitadeira que vai funcionar a distância, usando as redes 5G e, com isso, a gente vai ter um ganho de produtividade muito grande.

Então, eu vou passar rapidamente, porque meu tempo está esgotado. Eu acho que a gente tem: as questões das leis municipais, isso provavelmente deve ser citado, mas a gente precisa do físico, das antenas para que o digital funcione; a questão de instalações próximas a fábricas, na agricultura, principalmente, chegando a esses lugares; o custo alto das redes privadas ainda; e, principalmente, a falta de conhecimento da empresa.

Eu queria... Desculpe estar passando um pouco do tempo, mas, em relação à pergunta de emprego, é importante ressaltar que, desde a primeira revolução industrial, esse medo da perda de emprego para as tecnologias existe e, cada vez que há essa mudança mais radical, ele aumenta.

Isso aconteceu no início da revolução industrial, aconteceu em 70 e está acontecendo agora, mas, quando a gente olha uma série longa de taxa de desemprego no Reino Unido, ela pouco muda desde o tempo pré-revolução industrial até agora, ou seja, no longo prazo novos empregos aparecem.

Mas o Senador colocou uma questão importantíssima: no curto prazo, há custo, sim. Quando a gente tira cortadores de cana e substitui por uma colheitadeira, segundo dados da própria CNA, são cem cortadores de cana, e a colheitadeira precisa de sete pessoas capacitadas. Como eu faço para realocar esses cem trabalhadores num País em que a maioria desses trabalhadores não tiveram uma educação adequada?

Então, o investimento em educação tanto para as crianças como para recolocação é importantíssimo e, obviamente, um programa de renda mínima também é essencial para receber essas pessoas. E até, em nosso caso, a gente vai poder usufruir da tecnologia e trabalhar menos no futuro.

Muito obrigado.

Desculpe-me por ter passado um pouco do tempo.

O SR. PRESIDENTE (Jean Paul Prates. Bloco Parlamentar da Resistência Democrática/PT - RN) – Não, sem problema, Renato.

Obrigado.

Eu até quero avisar a todos que essa campainha é automática. A gente coloca o tempo, então, quando ele se desculpou pelo atraso, tocou a campainha, mas não foi



proposital, é porque realmente há um tempo aqui. Aqueles que já vieram aqui várias vezes sabem que, quando a gente coloca o tempo, ela toca um minuto antes de terminar e, depois, aos 15 segundos. Então, para avisar a todos que quando tocar a campanha é apenas para nos ajudar a controlar o tempo. Quando a gente às vezes está falando e perde a noção.

De fato, Renato, só para fazer um contraponto ou, na verdade, corroborar, a nossa preocupação veio pelo fato de a faixa a qual estava acoplado o compromisso de investimento na conectividade nas escolas ter dado deserta. Praticamente, a faixa de 26GHz, que é – não sou especialista, mas segundo me dizem – uma faixa ainda de nova fronteira, inexplorada, inclusive tecnologicamente. Talvez os demais possam depois explicar isso. Colocaram o compromisso de conectividade nas escolas exatamente como contrapartida de uma faixa em que não houve interessados. Então, uma das preocupações que a gente tem aqui em relação ao leilão foi essa, porque, na verdade, a conectividade das escolas ficou em aberto por conta dessa questão da faixa ter sido... Em vez de colocar no 3,5GHz, colocou-se lá no 26GHz e ficou sem investidor, sem interessados.

Mas isso a gente pode discutir ao longo do tempo aqui da nossa audiência.

Eu queria, dando sequência ao segundo bloco da nossa audiência, convidar para que se junte a mim na Mesa, já que está presencial, o Sr. Victor Hugo da Silva Rosa, que é Coordenador-Geral da Gestão de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

Acrescento aqui um agradecimento à GSI pela presença de vocês aqui. Com certeza estamos todos aqui unidos num espírito de construção desta política e com muito otimismo em relação a ela.

E a quem eu também pergunto, já para ajudar um pouco no debate, referente ao voto divergente do Ministro Aroldo Cedraz, do TCU, ao analisar o edital de licitação de 5G daquele tribunal, entendendo que haveria a necessidade de licitação específica para contratação de uma rede privativa de comunicação da administração pública federal.

Como o senhor avalia que o Governo Federal poderia minimizar os efeitos, os riscos apresentados pelo Ministro Cedraz em seu voto divergente?

Por favor, Sr. Victor Hugo, claro, a sua exposição. Apenas aduzi essa pequena pergunta aqui para que a gente trate desse ponto em específico, já que a audiência justamente se dedica à análise e à fiscalização dessa política pública.

Obrigado.

Concedo a palavra, por dez minutos, com a tolerância que necessitar, como fiz com o orador anterior.

Obrigado.

O SR. VICTOR HUGO DA SILVA ROSA (Para expor.) – Bom dia a todos. Bom dia, Senador. Obrigado pelo convite; agradeço em nome do Ministro General Augusto Heleno.

A ideia é trazer – vou acabar respondendo aqui, no curso da apresentação – a questão de riscos relevantes. Então, o departamento de que eu faço parte lá, o Departamento de Segurança da Informação, é mais conhecido até pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo, que é a face mais visível operacional, e a equipe que coordeno é a equipe que trabalha com acordos, memorandos de entendimento internacional e normas.

Basicamente aqui, a apresentação vai abordar e perpassar a IN 4, que é uma das perguntas também. Então, a gente vai acabar respondendo essas questões. (Pausa.)



É interessante que as apresentações dos colegas que me antecederam, da ABDI, da Marcela, e do Renato, da CNI, foram interessantes, porque a gente não combinou, mas se encaixam aqui perfeitamente no que eu queria mostrar.

O primeiro eslaide é mais um histórico. O colega Renato apresentou também um histórico e a mudança de quebra de paradigma, que os dois apresentadores colocaram, que é o que nos preocupa na parte de segurança cibernética, que é um cuidado muito maior que a gente tem em relação às tecnologias que estão hoje aí.

Então, a gente teve praticamente um século de telefonia fixa convencional, desde a criação, a fundação da Bell Company, desde 1877, e houve aquelas décadas que foram do 1G ao 4G. A gente vê que, basicamente, a gente gira em cima de comunicação humana. Então, a grande quebra de paradigma é que agora vai ter uma comunicação máquina à máquina, M2M (Machine-to-Machine), e isso é a grande transformação.

Então, o que acontece? A gente costuma dizer que o celular são os grilhões modernos, ele dita nossa vida, nossa agenda está ali, nossa comunicação, diversos aplicativos e tudo o mais. Isso vai se aprofundar ainda mais, não só em relação a nós, como em relação a todo um processo da sociedade. A gente está falando de fábricas que vão conversar não necessariamente com seres humanos, mas entre si, inclusive com previsões de produção, previsões de logística e tudo o mais.

Então, a gente vai passar – e é uma experiência da humanidade – a estar imerso, como eu mostro lá, ao final... Vamos eu ver onde está o apontador *laser* aqui. Não aparece muito, mas é o quadro final que eu destaco lá, que é o novo paradigma: a gente vai estar imerso num grande sistema de automação, a gente vai fazer parte, a gente vai ser peça disso. Ao mesmo tempo em que a gente é o usuário, cliente desse sistema, a gente é peça dele, que ele vai usar para prever demandas, prever deslocamento de modais de transporte e tudo o mais. Então, o grau de criticidade que a comunicação, com o 5G, passará a ter é muito alto, muito alto! Então, principalmente a parte de produção e a parte de telemedicina.

Bom, quais são os fatores de risco? Desses fatores, eu citei algumas referências. A gente tem estudos aqui, nacionais também, mas há de órgãos, como a Enisa, que é de segurança cibernética da Comunidade Europeia; do Cisa, que é a norte-americana; citei da Otan também, e alguns outros, apenas para ter algumas referências. Mas são... Basicamente convergem os especialistas. Acho que a gente tem isso aí.

Eu dividi em três grandes blocos – para ficar fácil de entender – os fatores que o 5G traz que são inerentes a ele, e muitas coisas são benefícios do 5G, mas aquele benefício traz com ele um risco também. Então, eu dividi em características gerais da tecnologia 5G, características técnicas e de implementação da rede, que está muito relacionada às operadoras e aos fornecedores dela, aos contratados dela para implementar, e outros que é característica mercadológica, do mercado de equipamentos de rede que vão compor essas redes 5G.

Quanto às questões gerais de tecnologia, a gente tem aumento da superfície de ataque, porque isso aí é lugar comum, todos apontam para si. Ou seja, terá mais pontos por onde entrar os ataques.

A questão da comunicação máquina a máquina, massiva. Ou seja, ataques poderão estar ocorrendo e em evolução, e se de uma maneira dissuadida, dissimulada, poderá a ter até uma percepção tardia do ser humano, claro! Porque aí vai entrar muito a questão de uso de aprendizagem de máquina e inteligência artificial para tentar fazer frente a isso.

E a questão da comunicação ultrarrápida e altamente confiável, que é o que os colegas falaram. A baixa latência, ou seja, a resposta rápida. Ao mesmo tempo que isso é



um benefício, isso para um atacante... É um benefício para o usuário e para o atacante também é um benefício, ou seja... Eu digo o seguinte, no computador, lá em casa, ainda não chegou fibra ótica, onde eu estou morando, então, eu costumo dizer que um *hacker*, às vezes, vai desistir de me atacar, de tão lento que é. (*Risos.*)

Mas com o 5G essa coisa vai mudar. Será muito rápido mesmo.

Bom, isso aí é nas questões gerais da tecnologia. No relacionado às características técnicas e de implementação das redes, muito relacionado às operadoras, os palestrantes que estão aí que são de fabricantes sabem muito bem disso, que é a característica da arquitetura do 5G. Então, essa questão da virtualização da rede, o *software-defined networking*, a rede definida por *software*, traz realmente um risco junto, porque é até a questão de auditar a rede como está configurada.

A rede do 5G... É claro que isso já vinha acontecendo, o uso dessa rede configurada por *software* já vem acontecendo em *data centers*, já vem acontecendo desde o 3G, mais fortemente no 4G, mas agora será realmente massivo. No 5G, você terá uma rede que pode ser *mutatis mutandis*. Então, você tem aquelas configurações tradicionais. No *backhaul*, o que é equipamento de roteador, o que é um *gateway*, isso aí tudo vai poder se configurar, ou seja, haverá muitos equipamentos genéricos que podem ser configurados por *software*, inclusive remotamente. Então, existem preocupações, por exemplo, na Comunidade Europeia, a própria Enisa já fez normas em que há determinados tipos de equipamentos, determinados tipos de função que não podem ser feitas remotamente. Então, isso é uma coisa para a qual a gente precisa se atentar.

A questão da complexidade e flexibilidade na gestão e na orquestração de rede. Isso aí também é outra coisa. A rede pode ser fatiada, dividida em sub-redes. Então, ela pode ser configurada de maneira diferente. Por isso se deve ter um cuidado muito grande nas operadoras no implementar.

A questão das incompatibilidades e funcionalidades com sistemas antigos. Então, haverá uma herança. É a mesma coisa de a gente colocar um sistema numa casa, num prédio, supersofisticado, com a digital, mas o porteiro ainda, para quem não cadastrou, vai lá com a chave e abre. E não tem *log*, não sabe quem abriu. É praticamente isso.

Então, o 5G estará se conectando com sistemas legados em 4G e 3G. E tem que haver alguns cuidados de qual função que vai compatibilizar para não abrir esse tipo de possibilidade.

Outra coisa é a computação de borda. Exatamente por ter baixa latência, o 5G leva massivamente o processamento para a ponta, mais perto dos usuários. Então, isso aí associado com outro risco que está mais abaixo, que é o da cadeia de suprimento, vai ter peças, partes que podem ser supridas por diferentes subfornecedores do fornecedor, que às vezes é difícil de auditar ou por estar em outro país, ou por ser outro sistema, ou por ser muito diversificado. Então, na computação de borda, você pode ter equipamentos com um risco maior, com vulnerabilidade, instalados na ponta.

Eu somei ali a cultura das operadoras. Por quê? Até o 4G, ainda existe uma cultura de centralizações, ou seja, é um cuidado dos técnicos da operadora de fazer uma análise, de fazer uma auditoria naquele equipamento que está fazendo uma orquestração de maneira mais central. No 5G, isso aí vai estar distribuído mesmo. Então, você acaba dando um poder às pontas, que aí tem que cuidar. Então, hoje o modelo das operadoras já é realmente fazer um contratante...

(Soa a campainha.)



O SR. VICTOR HUGO DA SILVA ROSA – ... que vai fazer esse tipo de gestão por eles. Então, está muito contratual. Há uma preocupação muito grande na capacidade técnica das operadoras de poder criticar isso aí.

E as questões relacionadas ao mercado, que a gente vai bater, em que eu vou tentar correr aqui, é o que a gente frisou na IN 4, a auditabilidade da cadeia de suprimento associada a uma baixa capacidade nacional para auditar. Eu não digo no sentido, como os colegas colocaram, de implementar a função da rede – nisso aí a gente é bom, a gente tem condição do uso –, mas eu estou falando daquelas ameaças de *hardware*. As ameaças em *hardware* são poucos laboratórios internacionalmente que têm condição de depurar e descobrir. Nisso a gente tem uma baixa capacidade, esse é um problema.

Outra coisa é permissivos legais para violação de privacidade e segurança por alguns governos. Isso, no geral, tem alguns... Eu estou falando da parte pública, não estou falando da parte de inteligência ou outras coisas; eu estou entrando só no que é realmente público.

E há a questão da concentração do mercado de redes na mão de poucos ou pensar um fornecedor.

A gente fez a IN 1, e eu vou resumir isso aqui. Não vou entrar. Foi um grupo que participou, vários aqui envolvidos no assunto: o GSI coordenando, o então Mctic – ainda estavam comunicações com ele e a Anatel –, o MRE, a Segov, o CPQD também participou, para desenvolver a IN 4. Na IN 4, os requisitos mínimos de segurança foram fechados com esse grupo. A gente o verteu para a norma.

Mais adiante houve uma consulta pública na Anatel que criou a Resolução 740, porque, frise-se, a norma do GSI é para o Poder Executivo federal; ele não normatiza empresas reguladas, ele faz a regulação para quem vai regular. Então, ele fez uma norma para o Ministério das Comunicações – na época, o Mctic...

(Soa a campainha.)

O SR. VICTOR HUGO DA SILVA ROSA – ... e para a Anatel.

Bom, o que nos preocupa, eu vou para um ponto aqui de atenção – e foi capturado praticamente tudo dentro da norma da Anatel –, é a questão do inciso X do art. 5º da IN 4. Embora a diversidade esteja como princípio na Resolução 740 no que a gente colocou, ao que leva esse inciso, conforme ele está ali transrito? Ele leva as operadoras a terem que cuidar para que não mais do que a metade dos equipamentos instalados sejam de um mesmo fornecedor.

Em relação a uma pergunta que fizeram lá: não foi vedado – à época foi colocado isso em nota à imprensa e tudo mais, pela área de comunicação do GSI –, não se trabalhou em vedação, como alguns países trabalharam, a fornecedor, mas se trabalhou com uma preocupação de proteção da sociedade, com a questão do erro de modo comum e da falha de modo comum e com a questão de concentração de mercado, que é muito mais afeta a outros órgãos.

Então, o que se procurou fazer foi colocar o seguinte: nenhum fornecedor, independentemente de qual fornecedor, independentemente de qual país, poderia ter mais do que a metade dos equipamentos, para evitar o erro de falha comum. Se o projeto, se componentes-chaves naqueles produtos lá tiverem uma vulnerabilidade e forem explorados, isso não pode comprometer a rede inteira, por exemplo, em uma grande cidade. Imagine se São Paulo está apenas na mão de um fornecedor, se há uma vulnerabilidade que ele não consegue, em tempo, corrigir e sanar, toda a rede está comprometida.



Então, vai ficar a apresentação aqui. Eu coloco o que, no passado, no Brasil... Em termos de telefonia fixa, eram seis grandes fornecedores internacionais de seis países diferentes. Já na telefonia móvel, no 1G e no 2G, já começou a ir para três. No 5G, já há uma tendência, continua com três, mas com uma concentração maior em um. E, hoje, no Brasil, a gente tem uma tendência... Já está com 50% em um fabricante dominando praticamente o 3G e o 4G, com uma tendência de poder chegar a 100%, quiçá. Então, é mais essa preocupação com que a gente tem que ter cuidado aí na hora de implantar.

Outra pergunta que fizeram, Senador, se o senhor me permite responder, é se existiu algum fornecedor. Não, não foi nenhum. E o certame... Na realidade, não só a Anatel, como outras reguladoras no mundo inteiro se preocupam com a diversidade de operadoras. O equipamento que a operadora vai contratar fica por conta de quem vencer. Então, não há vedação, e o próprio edital não veda. Então, hoje, há uma diversidade, a despeito de ter havido lote vazio, infelizmente, nesse da educação, mas foram preenchidos os grandes centros. Os interesses econômicos acabaram sendo preenchidos, e houve diversidade, houve competição – esse é o viés que, em vários países, as reguladoras em telecomunicações adotam. Só que a camada de baixo, que é de equipamentos que vão ser colocados, está por conta de quem venceu os leilões. Então, eles é que vão escolher os equipamentos. Essa é uma atenção que a gente tem que ter.

É basicamente isso aí.

Desculpem-me por ter estourado o tempo aqui.

Muito obrigado pela oportunidade.

O SR. PRESIDENTE (Jean Paul Prates. Bloco Parlamentar da Resistência Democrática/PT - RN) – Obrigado, Victor Hugo. Sempre temos uma tolerância de um a dois minutos para que terminem. Muito obrigado pelo esclarecimento.

Quero, logo, sem mais delongas, passar a palavra ao Sr. Arthur Pereira Sabbat, que é Diretor do Conselho da Autoridade Nacional de Proteção de Dados (ANPD), a quem também já faço uma pergunta diretamente. Com a implantação das redes móveis de quinta geração, 5G, o tráfego de dados nas redes de telecomunicações deve aumentar de forma ainda mais acelerada. Como a ANPD está se preparando para os desafios trazidos justamente pela implantação do 5G?

Então, com a palavra o Sr. Arthur Pereira Sabbat, pela via remota.

O SR. ARTHUR PEREIRA SABBAT (Para expor. *Por videoconferência.*) – Muito obrigado, Exmo. Sr. Senador Jean Paul Prates.

Exmos. Srs. Senadores, senhoras e senhores, em nome do Diretor Presidente da Autoridade Nacional de Proteção de Dados, Waldemar Gonçalves Ortunho Júnior, eu agradeço o convite e a valiosa oportunidade.

Na qualidade de um dos diretores do Conselho Diretor da Autoridade, eu gostaria de voltar minha abordagem para o impacto do advento das redes 5G sobre a proteção de dados pessoais. Inclusive, vamos abordar também essa bem oportuna pergunta colocada pelo senhor, Senador, considerando os aspectos de segurança da informação e de segurança cibernética. E alguns desses aspectos, voltados à proteção de dados pessoais, já foram abordados pelo Dr. Victor Hugo, do GSI.

Bem, é importante ressaltar que as redes 5G, como já foi falado, trarão uma série de comodidades e de novas oportunidades à sociedade, em virtude de dois aspectos, entre todos, entre vários também, que proporcionarão: o primeiro é a elevada velocidade de conexão com baixíssima latência; o segundo, quase em decorrência desse, é a elevada quantidade de conexões simultâneas de alta qualidade e confiabilidade. Essas são, sem



dúvida, características disruptivas, mas que também exigirão que todos – poder público, setor privado, cidadãos, enfim, a sociedade – adquiram, em seu cotidiano e no seu *modus operandi*, no seu *modus vivendi*, conhecimentos e cultura em dois campos que estão intimamente relacionados e que estão muito em voga e crescendo de importância a cada dia, que é a segurança cibernética e a proteção de dados pessoais.

Um dos benefícios que se espera com a implantação das redes 5G é o uso eficaz de equipamentos de internet das coisas, tecnologia que podemos definir como a interconexão, por meio da internet, de dispositivos de computação incorporados em objetos do nosso uso cotidiano, o que permite a esses objetos enviar e receber dados em diferentes volumes.

A essência dessa tecnologia de internet das coisas – e aí vamos nos aprofundar no porquê da nossa preocupação com isso – é o potencial dessa tecnologia para conectar objetos utilitários comuns, aqueles utilizados no nosso dia a dia, à internet, do mesmo modo que outros dispositivos que hoje somente possuem sentido praticamente se ligados à rede, como computadores e *smartphones*. Portanto, constata-se que o 5G irá potencializar intensamente a internet das coisas.

A partir desse ponto, nesse contexto, eu gostaria de abordar alguns reflexos da implantação das redes 5G para a proteção de dados pessoais.

Primeiro, o aumento da quantidade de equipamentos conectados simultaneamente e na mesma região, como *smartphones*, computadores pessoais, dispositivos de internet das coisas, possibilitado exatamente pela rapidez de resposta dos recursos de 5G.

Segundo, o aumento da interação entre coisas, pessoas e plataformas e aplicações, pela facilidade e rapidez de conexão.

Terceiro, a implementação e ampliação do uso de dispositivos de internet das coisas em áreas diversas da nossa atividade humana, como consumo, saúde, serviços públicos, gestão urbana... Enfim, no dia a dia do cidadão.

O aumento também da coleta... E aí começam as nossas preocupações também: o aumento da coleta e das demais operações de tratamento de dados pessoais, uma vez que esses equipamentos de internet das coisas necessitam de variadas quantidades de dados pessoais para serem eficientes aos seus proprietários, para eles cumprirem com a finalidade a que eles se destinam, para oferecerem à comunidade a comodidade que ele se propõe a oferecer.

E também, como consequência dos aspectos anteriores, teremos um aumento vertiginoso do fluxo, do tráfego desses dados pessoais, o que demandará atenção tanto por parte da autoridade nacional de proteção de dados, mas também de fabricantes e distribuidores desses equipamentos, quanto de órgãos públicos e, com certeza, por parte dos cidadãos usuários, que são os titulares de dados. A Lei Geral de Proteção de Dados Pessoais foi feita para ele, para o cidadão, para nós, titulares de dados.

Também temos outro aspecto a considerar, o potencial aumento do impacto de ataques cibernéticos sobre instituições públicas e privadas, sobre o cidadão, enfim, uma vez que esses benefícios da tecnologia 5G, como foi abordado pelo Professor Víctor Hugo, também poderão ser explorados com o tempo por criminosos cibernéticos. O que nos serve em termos de comunidade também pode servir em termos de facilidade para realização de ataques cibernéticos se esses equipamentos não forem programados, configurados e não tiverem medidas adequadas e níveis adequados de segurança cibernética. Isso é questão de arquitetura de concepção.

Por fim, verificamos também esse aumento da importância da segurança cibernética e do zelo com a proteção de dados pessoais. Este é um tema que está grassando o



mundo com maior intensidade: a valoração da privacidade dos cidadãos, a importância que os governos têm de dar a essa proteção e à segurança dos dados do cidadão – tudo isso é muito interligado. Como disse, a segurança cibernética não existe sem a proteção de dados pessoais e vice-versa. Isso é uma realidade, é impossível separá-las.

Eu entendo que a segurança cibernética, portanto, é fundamental para uma adequada proteção de dados pessoais – nesse sentido que eu gostaria de colocar –, e isso se tornará mais evidente com a implantação das redes 5G. Daí a ser essencial que os princípios de segurança cibernéticos sejam considerados tanto pelas operadoras ao contratarem as empresas que irão instalar a infraestrutura das redes 5G voltadas à implementação da rede 5G especificamente quanto pelos fornecedores de equipamentos dessas redes ou que se utilizarão diretamente dos benefícios dessas redes, como é o caso dos dispositivos de internet das coisas.

Eu creio nesse sentido, portanto, que, com esse conceito de quantidade volumétrica de dados pessoais que passarão a trafegar na internet, aliado a numerosos dispositivos pessoais utilitários – de internet das coisas, inclusive –, a disseminação de conceitos e da cultura de segurança cibernética e da proteção de dados pessoais para a nossa sociedade é urgente e por que não dizer imprescindível, muito mais do que essencial.

Era o que eu tinha a dizer no momento, Senador.

Eu agradeço imensamente e continuo à disposição.

Se me permite, sobre a pergunta específica de V. Exa., quero dizer que a Autoridade Nacional de Proteção de Dados está se estruturando. Nós estamos concebendo, juntamente com o Governo Federal e com o apoio do Ministério da Economia, um projeto de lei para que nós alcancemos maior autonomia, inclusive autonomia administrativa, orçamentária, e que nós consigamos mais recursos, mais pessoal, porque nós precisamos nos fortalecer para fazer frente a toda essa realidade que se avizinha e que vai se agravar com o advento das redes 5G.

Era isso. Muito obrigado, Senador, pela oportunidade.

O SR. PRESIDENTE (Jean Paul Prates. Bloco Parlamentar da Resistência Democrática/PT - RN) – Obrigado, Arthur.

Por favor, conte desde já com o nosso apoio a essa pretensão legítima quanto à questão dos recursos para que todo esse processo funcione a contento e que a gente consiga, de fato, ter o controle adequado desse processo não só de implantação como de operacionalização a partir da sua implantação no Brasil.

Concedo a palavra, por dez minutos, aproveitando o acesso remoto, ao Sr. Roberto Gallo, Diretor-Geral da Kryptus.

Por favor, Roberto. Tem a palavra por dez minutos.

O SR. ROBERTO GALLO (Para expor. *Por videoconferência.*) – Bom dia, Senador Jean Paul. Muito obrigado pela oportunidade de contribuir com esta audiência.

Primeiro, quero saudar também o representante do GSI, perfeita a exposição. E, apesar de não muito, digamos assim, adjetivada, traz consigo sutilezas importantes do ponto de vista estratégico.

Vou compartilhar a minha tela aqui, se me permitem, no sentido de ilustrar um pouco mais a apresentação que faço.

Apenas, para aqueles que não me conhecem, basicamente vimos trabalhando na empresa já há quase duas décadas em importantes sistemas para o Estado brasileiro, entre os quais a urna eletrônica do TSE; a Infraestrutura de Chaves Públicas Brasileiras, incluindo a Autoridade Certificadora Raiz; as comunicações seguras das Forças Armadas; a segurança cibernética do Itamaraty; a tecnologia para emissão do seu passaporte pela



Casa da Moeda; e o Ato 77, que comentarei brevemente, da Anatel, que prevê a fiscalização e auditoria dos equipamentos de telecomunicações em geral. Portanto, Sr. Senador, tento dar aqui um contorno mais estratégico em minha palestra e muito menos tecnológico.

Bom, vivemos atualmente, senhores e senhoras, uma guerra de narrativas em torno de uma realidade muito importante. O 5G representa uma promessa de desenvolvimento econômico de US\$13,2 trilhões até o ano de 2035. Isso é dez vezes o PIB nacional. Uma única tecnologia – uma única tecnologia! – tem a capacidade de gerar dez vezes a riqueza do PIB brasileiro nos próximos 15 anos.

Essa geração de riquezas se espalha por diversas áreas da economia. De novo, segundo o Fórum Econômico Mundial, esses dois dados são do Fórum Econômico Mundial, várias áreas são tocadas pela riqueza gerada pelo emprego e pela própria venda da tecnologia 5G, não é? O 5G gera valor de duas maneiras: tanto no que ele habilita de novos negócios, mas também na própria infraestrutura. Vejam, no setor de manufatura, quase 5 trilhões são esperados; na área de comunicação e informação, outro 1,6 trilhão; no setor de comércio, 1,2 trilhão; e o setor público também – por que não? – é tocado por esse grande advento.

Decorre, entretanto, Senador, que tivemos o que o americano chama de momento Sputnik. Os mais novos certamente não lembram, mas, em um certo momento, os Estados Unidos, durante a era da corrida espacial, foram pegos de surpresa – nem havia a corrida espacial ainda – com os russos lançando um primeiro satélite. No imaginário americano, na cultura americana, o momento Sputnik é quando você é surpreendido por um avanço rápido e contundente do seu adversário ou da sua competição. Como reportado na época, na capa do *The New York Times*, ali se mostrava a pujança, naquele caso, do Governo comunista da União das Repúblicas Socialistas Soviéticas, e esse momento Sputnik se repetiu com o advento do 5G, esta é a realidade.

A concentração de mercado, notada pelo colega do GSI, insere-se dentro de um contexto grande, Presidente, Senador, em que existe um ecossistema, e o ecossistema 5G passa ou perpassa por diferentes tipos de indústrias. A mais importante delas obviamente está em torno das próprias infraestruturas de telecomunicação e dos aparelhos celulares ou dos *modems* celulares que ali se utilizam.

Acontece que, ainda que existam diversas camadas, diversas empresas, diversos negócios que geram valor e que giram em torno do 5G, a verdade é que o grande vencedor dessa corrida é a China. Vejam o número de patentes depositadas e garantidas – esse último dado é de fevereiro de 2020 – sobre tecnologia 5G. O grande habilitante está no Oriente. O Ocidente, em particular os Estados Unidos, perdeu essa corrida. Há ainda, obviamente, até 2020, uma importante posição dos países europeus, em particular dos escandinavos, com a Nokia e a Ericsson, mas essa é uma corrida ganha pela China. E, vejamos, é o que leva a uma guerra de narrativas muito importante. A partir do momento Sputnik, não havia outra oportunidade para o americano a não ser levar em conta aspectos políticos e geopolíticos estratégicos.

Esse aqui é o edifício sede da União Africana. Esse prédio, construído com recursos chineses, reportadamente teve os dados extraídos durante uma grande parte do tempo – isso é reportagem, não estou afirmando que é verdade, estou apenas trazendo a reportagem do *Le Monde Afrique*. A informação, a integralidade da informação dos servidores da União Africana era transferida durante a noite para Xangai. Esse tipo de ação, obviamente, muitas vezes está envolto em grandes pressões estratégicas



econômicas. Vários anos depois, quase sete anos depois, a União Africana voltou a comprar equipamentos da empresa chinesa teoricamente envolvida com aquele processo.

Isso tem levado – de forma desproporcional, na minha opinião, essa é uma opinião estritamente pessoal – a uma resistência contra, em particular, a fabricante chinesa Huawei. Esses dados aqui da Bloomberg, de forma gráfica, mostram os países onde em particular os equipamentos dessa companhia têm tido algum tipo de banimento ou resistência local dos governos. As cores não ajudam muito, mas se vê obviamente que Estados Unidos, Canadá, Reino Unido, Austrália, Japão, Índia e países escandinavos – Polônia – possuem algum tipo de restrição importante.

Mas como esse tipo de restrição apareceu? Ele emergiu basicamente de uma pressão internacional muito grande, principalmente do Governo americano, que sabe o que está fazendo, sabe a importância do assunto porque ele mesmo assim o faz. Esse eslaide aqui é um eslaide de marcação *top secret*, equivalente ao nosso ultrassecreto, da seção de inteligência de comunicações da NSA, que vazou a lista de maiores alianças tecnológicas, obviamente para atividade de segurança de comunicações, ali está escrito: "Commit". Há provedores de toda parte. Se os senhores se lembrarem, no começo do ano passado, saiu no *The Washington Post* um dos maiores escândalos, que eu diria, do século. É chamado de "o golpe de inteligência do século". Empresa sueca, com sede na Suíça, chamada Crypto AG. Descobriu-se que a empresa era uma copropriedade do serviço de inteligência norte-americano, a CIA, e da Alemanha Ocidental. Desde a década de 50, essa empresa distribuiu equipamentos com *backdoor* para mais de 120 países, inclusive o Brasil. Das informações vazadas, se identificaram 62 países clientes. Basta uma procura no portal da transparência que os senhores veem que nós, Brasil, fomos alvo também.

Senhores, senhoras, os países com um aparato de inteligência robusto, industrializados – e aqui estou falando de Estados Unidos, Reino Unido, Alemanha, China, Rússia –, usam seus serviços de inteligência, utilizam equipamentos de guerra cibernética para atingir seus objetivos comerciais, objetivos ideológicos, de todo tipo. A escolha entre provedor A, ou B, ou C obviamente tem que levar em conta esse tipo de situação, mas sabendo que é global. Por que é global esse problema? Pelos fundamentos. Esses fundamentos são fundamentos econômicos e até técnicos. (Pausa.)

Eu gostaria de usar mais dois ou três minutos, se me permite, Senador.

Bom, primeiro quero lembrar que estamos aí numa sociedade pós-industrial. Grupos, nações e países sempre lutaram, ao longo da história, por recursos: comida, água, pedras, fertilizante, petróleo, mas a realidade é que, do meio século para cá, o maior ativo é conhecimento e tecnologia. A diferença entre um celular de R\$1 mil e um de R\$15 mil é nada, senão o projeto. São os mesmos materiais que ali estão: silício, plástico, vidro, ouro, cobre. Entretanto, as técnicas que se utilizam para ganhar vantagem no terreno da informação, se obter conhecimento e tecnologia ou informações negadas são iguais para vários tipos de atividades, sejam elas benignas ou nocivas: prossecução legal, em que a capacidade de invadir um sistema é fundamental justamente para que se processe e prenda o criminoso; mobilização militar, quando na defesa é altamente positivo; espionagem; e até mesmo chantagem. Todos estão sujeitos aos mecanismos que estão embarcados nesse tipo de tecnologia, seja acidentalmente, o que eu vou comentar brevemente, seja de propósito.

Um homem público pode ser chantageado por uma opinião. E quantos homens públicos não estão vendendo essa palestra aqui? Espionagem pode atingir a indústria, pode atingir o Estado, pode atingir vários.



Outro fator importante é que, a despeito do que qualquer fabricante falar, existe um teorema fundamental da computação que diz que é impossível provar que um sistema é seguro. Não há o que se dizer. Há uma impossibilidade matemática para que isso ocorra. Isso faz com que as proteções, como vou explicar, já finalizando, não possam ser estritamente técnicas, elas têm que levar em conta processos e a lei. A lei tem que ser pesada para aqueles que abusam da confiança.

Outro aspecto importante – este é técnico, mas me permitam; gastarei aqui 30 segundos: existe uma impossibilidade técnica de se distinguirem *backdoors* de *bugs*. Veja, Microsoft, Apple investem literalmente dezenas ou centenas de bilhões em seus sistemas e, mesmo assim, possuem defeitos. Sabendo os senhores que é impossível eliminar defeitos e sabendo os senhores que é possível criar *backdoors* que são indistinguíveis de defeitos, conclui-se, por obviedade, que é impossível se eliminarem *backdoors*. Tanto é assim que existem até concursos aqui – e este é um concurso – de como se criar um *backdoor* que é indistinguível de um *bug*.

Na prática, já indo para o encaminhamento final aqui, diferentes estratégias são necessárias para que se busquem diferentes tipos de problemas de segurança. Claro, quando existe um defeito acidental – análise de projeto, análise do artefato sem código e o projeto ter alguma eficácia, óbvio, sem ser intencional –, isso já não é tão efetivo, por isso em amarelo, e não serve em nada para aqueles que estão, de fato, querendo colocar alguma coisa de forma oculta. A técnica não responde a tudo. Essa é a verdade.

O acompanhamento de processo, o desenvolvimento do sistema sob certificação cerrada, sob os olhos dos interesses nacionais avançam bastante aquilo que a gente é capaz de pegar, até o acidental oculto, eu diria assim, aquele *bug* que é acidental, mas é oculto.

Agora, o enquadramento legal é a última instância, com punição exemplar, para que se permita a segurança de fato e a confiabilidade de fato nas tecnologias que se empregam.

Já para o meu último eslaide, Senador, falo sobre caminhos que podemos tomar.

Primeiro, a gente precisa entender que a infraestrutura 5G não pode ser confiada para tudo, e não há declaração de fabricante ou sessão de *workshop* que se possa fazer que garanta que a segurança para itens críticos esteja lá, simplesmente porque é impossível. A gente precisa, portanto, ter uma estratégia de camadas: a segurança deve estar em outra camada, usando criptografia, técnicas cibernéticas, sob o controle nacional, se a aplicação assim demandar, uma aplicação de Estado ou uma aplicação crítica.

Outro caminho que vai ao encontro do exposto pelo 5G é se garantir a variabilidade dos provedores de internet, não dependendo de um único fornecedor, para que a gente tenha resiliência nas redes.

E mais: atualizar a criminalização para sabotagem e espionagem, explicitando infraestruturas críticas de telecomunicações – a nova Lei de Segurança Nacional regrediu, em minha opinião, nas proteções: descharacterizou-se o crime de espionagem fortemente ou o de sabotagem, inclusive –; ampliar as inspeções técnicas exploratórias nas infraestruturas e tecnologias nos moldes do Ato 77 da Anatel – seria um bom avanço, mas está infralegal –; multiplicar exercícios cibernéticos, como o Guardião Cibernético, levado pelo Exército Brasileiro; e, obviamente, investir em tecnologia nacional para a infraestrutura.

Quem sabe, assim, a gente consiga entrar na próxima onda da infraestrutura de 6G. Termino aqui a minha colaboração. Lamento os minutos a mais.



Muito obrigado.

O SR. PRESIDENTE (Jean Paul Prates. Bloco Parlamentar da Resistência Democrática/PT - RN) – Nós é que agradecemos, Roberto, e a todos vocês, pelas competentíssimas apresentações. Acho que quem está assistindo em casa... Estamos chegando na hora do almoço, mas, enfim, de todo jeito, nós temos bastante audiência, pelo que estamos vendo aqui nas perguntas recebidas pela internet, porque as apresentações são riquíssimas e o assunto, de fato, inspira muita curiosidade, além de serem muitos assuntos mesclados importantes: inovação, concentração de mercado, mercado em si, segurança, privacidade, enfim.

Vamos iniciar aqui a série final com as empresas. Temos aqui a Ericsson, a Nokia e a Huawei.

Eu queria convidar, para compor a mesa comigo aqui, a nossa próxima convidada, a Sra. Jacqueline Lopes, Diretora de Relações Institucionais da Ericsson para o Cone Sul da América Latina, para a sua exposição. Concedo a palavra por dez minutos.

Obrigado, Jacqueline.

A SRA. JACQUELINE LOPES (Para expor.) – Bom dia a todos!

Começo agradecendo ao Senador Jean Paul pelo convite.

Cumprimento todos os colegas aqui presentes e também os que participam conosco de forma remota.

Hoje eu trarei um pouco mais sobre essa tecnologia do 5G, a visão da indústria, começando um pouquinho aqui sobre a Ericsson. A Ericsson é pioneira do 5G em cinco continentes. Nesse aspecto global, nós já temos cerca de cem redes de 5G ativas em mais de 45 países e hoje também temos cerca de 150 contratos assinados em 5G. Somos também pioneiros em termos de padronização dessa tecnologia.

E no Brasil, como a Ericsson está? Já estamos aqui há quase cem anos instalados com uma fábrica em São José dos Campos e um centro de pesquisa e desenvolvimento localizado em Indaiatuba. Somos líderes de mercado aqui no País e, em abril deste ano, nós também lançamos a primeira linha de produção do 5G, no hemisfério sul; não apenas no Brasil, não apenas na América Latina, mas em todo o hemisfério sul. E, para que esse pioneirismo aconteça e continue ocorrendo, é fundamental o investimento em inovação. Por isso nós investimos também cerca de 100 milhões por ano, aqui no País, em aspectos de inovação local.

Complementando a discussão sobre a tecnologia do 5G, nós temos um estudo interno na Ericsson informando que, em 2030, o potencial de receitas, a partir da digitalização no País, deve totalizar R\$391 bilhões adicionais, dos quais 153 bilhões são relacionados ao 5G. Com isso nós percebemos a importância que essa tecnologia tem e, como já bastante debatido aqui hoje, no nosso painel, esse valor não traz benefício somente para o setor de telecomunicações; ele é transversal, ele é um vetor de transformação em diversos segmentos. Para ficar em alguns exemplos: a indústria, a saúde, a segurança pública, a educação. E esses setores, em geral, vão ter um aumento de conectividade, até 2030, entre 65% e 85%. Isso ressalta a transformação que nós já estamos vivendo aqui no País e que deve ser intensificada.

Por isso, nós consideramos o 5G a infraestrutura mais importante dos próximos anos, pelas suas características técnicas de alta velocidade, de ultraconfiabilidade, de baixíssima latência. E justamente essas características, aliadas às diferentes faixas de espectro que foram recentemente licitadas no leilão aqui no nosso País, permitem aplicações em diversos casos de uso nos mais diferentes setores.



Dentre eles, podemos trazer aqui três exemplos protagonizados pela Ericsson. O primeiro deles é um caso relacionado à telemedicina – a realização de uma ultrassonografia de forma remota que foi realizada em Minas Gerais, em parceria com um de nossos clientes. Esse é apenas um exemplo, mas é interessante notar, e a pandemia deixou isso muito claro para todos nós, a importância que nós temos do monitoramento – as consultas começam a ser realizadas em larga escala de forma remota, há o controle de doenças crônicas que oneram bastante o nosso sistema de saúde, melhoria da qualidade de vida da população e, com isso, nós podemos alavancar essa tecnologia para beneficiar toda a sociedade.

Isso não está restrito ao setor de saúde. Na parte de indústria 4.0, a ABDI e a CNI trouxeram vários exemplos aqui também. Inclusive, o caso que eu trago aqui é justamente o caso da WEG, que foi realizado em parceria com um de nossos clientes e também com a ABDI, e demonstra o benefício que isso vai ter para o setor produtivo. Existe um potencial aumento de produtividade de cerca de 25%, por exemplo, em aplicações de manutenção preditiva. Isso também contribui para aumentar a segurança da nossa indústria. E o aumento da competitividade vai contribuir para o desenvolvimento econômico.

Interessante ainda a gente considerar o caso do agronegócio. Aqui eu trouxe um exemplo em que nós tivemos uma aplicação em parceria com a São Martinho, também com um de nossos clientes. Houve recentemente também uma parceria com outro cliente, com a John Deere. No agronegócio, também os casos de uso são inúmeros. Podemos, por exemplo, monitorar a plantação, existem tratores conectados, o uso de defensivos agrícolas pode ser controlado por meio de inteligência artificial. Isso vai contribuir também para a competitividade no campo.

Vamos lembrar que a agricultura é um dos principais setores motores do PIB do nosso País. Também é um dos principais setores exportadores. Com isso, nós notamos que o 5G, aliado a todos os seus casos de uso, consegue impulsionar essa transformação e o aumento da competitividade nas mais diversas esferas e setores.

Ponto interessante: muitas pessoas se questionam se haveria benefícios adicionais. Em tempos de COP, eu adiciono mais um: não só essa inovação contribui para melhorar a competitividade, mas, ao mesmo tempo, embora o tráfego de dados aumente em quatro vezes por meio do 5G, a gente observa que o consumo energético permanece constante, ou seja, estamos deixando aqui de gastar energia e tornando a inovação sustentável não restrita ao setor de telecom e, sim, aplicável aos diversos segmentos da nossa indústria.

Inegável também dizer que, para a sociedade, existem vários outros aqui, por exemplo, a educação. Notamos que, no começo da pandemia, os cinco primeiros meses trouxeram um crescimento, que era esperado para o setor, de até dez anos. Isso vai permitir que as pessoas possam trabalhar de diversas regiões. Então, você observa um desenvolvimento econômico de toda a nossa sociedade.

Com esses benefícios e o alto valor em jogo trazido pelo 5G, existem também discussões inerentes sobre a questão de segurança cibernética. A Ericsson tem uma abordagem holística para segurança cibernética. Nós atuamos aqui em quatro camadas, quatro níveis, que são interdependentes. Primeiro, a parte de processo operacional: aqui nós estamos falando tanto do monitoramento, quanto das respostas aos ataques e possíveis ataques. Depois, no processo de *deployment*, a segurança das próprias redes, como elas podem trabalhar de forma segura. Em terceiro, a parte do desenvolvimento de produtos de fornecedores, ou seja, entendemos que isso é uma responsabilidade que envolve a cadeia do segmento; portanto, é importante que lá na ponta os fornecedores



também tenham produtos seguros, que vão chegar na outra ponta junto com os nossos clientes, que são as operadoras. E, por fim, o processo de padronização no setor de telecomunicações, para o qual nós contribuímos ativamente em nível nacional e também global.

Esse conjunto de quatro níveis interdependentes almeja justamente atender ao usuário final, para quem nós queremos proporcionar uma experiência mais adequada e segura, respeitando os aspectos de risco aqui de segurança cibernética.

Para que todas essas discussões avancem – e aqui estamos falando apenas do começo do 5G –, o diálogo entre o Governo, o mercado e a sociedade vai acelerar o desenvolvimento tecnológico do nosso País. Por isso, agradeço, mais uma vez, a oportunidade de continuarmos aqui dialogando com vários desses atores envolvidos na agenda de 5G, e fico à disposição para perguntas.

Muito obrigada.

O SR. PRESIDENTE (Jean Paul Prates. Bloco Parlamentar da Resistência Democrática/PT - RN) – Obrigado, Jacqueline. Exatamente seu eslaide final mostra o que nós estamos fazendo aqui: dialogar desde o início, desde a implantação, desde o processo de concepção da regulação, da realidade nova que vamos viver, e o Senado e esta CCT justamente representam a sociedade aqui discutindo com vocês do setor.

Concedo a palavra agora, por dez minutos, ao Sr. Wilson Cardoso, Diretor de Tecnologia da Nokia América Latina, para sua exposição, a quem também convidado para sentar-se e juntar-se aqui a nós, à Mesa.

Obrigado, Jacqueline.

E, enquanto você prepara a apresentação, queria rapidamente ler algumas perguntas que chegaram aqui – enquanto vocês colocam aí.

Maria Cecilia, do Rio de Janeiro: "Essa implementação seria acompanhada de projetos para ampliar o acesso à internet no País de uma forma geral?".

Elinadja Targino, de Alagoas, pergunta: "Como ocorrerá a implementação do 5G nas regiões mais longínquas, como Norte e Nordeste?".

Também aduzindo aqui pergunta no mesmo sentido Fernanda Moreira, de Minas Gerais: "Quais os lugares que irão fazer esta instalação [primeiramente]? Importante dar atenção para os lugares mais precários".

Marcelo Ceolin, do Rio Grande do Sul: "Quais as principais inovações trazidas com essa tecnologia?". Creio que temos tentado responder aqui, e estimulo o Marcelo a procurar também as duas outras audiências públicas que fizemos anteriormente, que trazem muita coisa a respeito disso; e as empresas aqui também trouxeram hoje bastantes respostas em relação a essa pergunta.

E a Joanna Silva, de Santa Catarina: "Quais os custos extras [que serão repassados para] o cidadão [...]?".

Sobre essas duas perguntas quanto ao alcance inicial e a questão dos custos extras estamos tratando justamente nessa sequência de três audiências públicas. Nesta também poderá ser tratada.

Portanto, temos aqui Wilson Cardoso, Diretor de Tecnologia da Nokia América Latina, com a palavra por dez minutos.

Obrigado.

O SR. WILSON CARDOSO (Para expor.) – Senador, boa tarde! Boa tarde a todos os presentes na plenária e a todos os que estão nos assistindo na internet.

Começando um pouco mais rápido, acho que todos se lembram da Nokia pelo passado de telefones. Nós não fabricamos mais telefones desde 2007, licenciamos uma



marca para uma empresa chamada HMD, que inclusive fornece telefones aqui no Brasil hoje.

Mas falando um pouco da nossa empresa no Brasil, temos 3 mil funcionários; nós temos escritórios em São Paulo, Rio de Janeiro e Curitiba; produção em São Paulo; parcerias com o Senai, com o Inatel e outras universidades do Brasil; e projeto de internet das coisas qualificada na chamada do BNDES, focado na agricultura e na indústria 4.0.

Um dos fatores que nós buscamos entender desde o começo – esse foi o estudo que nós fizemos logo após o começo da pandemia – foi entender o impacto econômico do 5G no Brasil. Esse estudo mostra esse impacto econômico de US\$1,2 trilhão nos próximos 15 anos, mostrados os diversos setores da economia que estão apresentados nesse eslaide. Equivale dizer que é um aumento de 1% do PIB nos próximos 15 anos à medida que nós vamos adotando o 5G nos diversos setores da economia. Claro, começa com o Governo com educação eletrônica, com a possibilidade de medicina remota, passando pela indústria, passando pelos serviços de agricultura e logística.

Nós temos de ter em consideração que é importante ter o 5G na fazenda para que nós tenhamos os benefícios já mostrados aqui, que nós tenhamos o 5G nas estradas para garantir que nossos corredores de logística garantam que a nossa soja, nosso produto agrícola chegue ao porto. É importante ter o 5G nos portos e ter todas as cadeias integradas de maneira que essa produtividade de 1% ao ano seja atingida.

Até existem algumas previsões de que, em 2030, nós vamos ter dois tipos de indústrias: as indústrias que estão conectadas por 5G e as que não existem.

Então, essa é perspectiva que nós temos de ter em consideração par o aumento da produtividade no Brasil nos próximos 15 anos.

Claro que, como já foi mostrado, estamos fazendo três coisas com o 5G. Estamos aumentando nossa superfície de contato, ou seja, nós podemos conectar milhões de dispositivos por quilômetros quadrados com muito mais velocidade e com uma latência muito mais baixa, como já foi explicado aqui e que é o tempo de resposta da rede.

A rede 5G pode ser uma rede segura, deve ser uma rede segura por todo o *design* que nós fazemos, mas nós vamos conectar muito mais dispositivos. Vamos ligar dispositivo de internet das coisas, vamos ligar dispositivos que vão manipular moedas eletrônicas novas nossas, vamos ligar as fazendas, vamos ligar *drones*, helicópteros, tudo isso vai ser ligado nessa rede. E semáforos! Agora, como nós vamos garantir que esses dispositivos são dispositivos seguros?

Uma pergunta que eu sempre faço para todo mundo, e aproveito esta plenária, é: quem já se preocupou em fazer atualização dos seus dispositivos de *wi-fi* na sua casa nos últimos dois anos? Esse dispositivo hoje na sua casa pode ser um instrumento de ataque à sua casa, e nós não nos preocupamos com os dispositivos. Então, um dos grandes problemas que nós podemos ter com o 5G – e esse é um fator fundamental – é que os dispositivos precisam ser mantidos, operados.

Claro, dentro da rede 5G, nós temos mecanismos para garantir o correto funcionamento desses dispositivos, porque, se o medidor de energia tiver que mandar uma informação para o ponto central da rede como um formato definido, e não mandar essas informações para esse ponto central na rede, mandar para outra localidade, automaticamente isso será alarmado e informado.

Então, o que nós podemos dizer? Com esse aumento da exposição, que já começou na era do 4G, e nós estamos evoluindo com a era 5G, nós estamos aumentando a quantidade de alertas de segurança que acontecem na rede, e é



fundamental nós termos pessoas treinadas, ferramentas de análise e possibilidades com auxílio de inteligência artificial para possibilitar aumentar a segurança dessa rede 5G.

Voltando um pouco ao passado, eu acho que, quando tudo começou, esse problema de geopolítica global – isso vem da *Bloomberg Businessweek*, desculpa fazer propaganda aqui, mas vem de um artigo de uma revista –, isso aconteceu em 2015, quando um componente, que está mostrado aí em cima de um dedo, atacou milhares de redes no mundo porque esse componente foi introduzido em placas de computadores. E, através desse componente, foram criadas portas que acessavam esses computadores e atingiam informações.

Cabe destacar, senhoras e senhores, que hoje um vírus de covid, que tem 125 nanômetros, possibilita a instalação de 30 transistores. Para as pessoas de cabelos mais grisalhos, como eu, a gente fazia, quando eu comecei o meu curso técnico, um rádio FM com dois transistores.

Então, é disso que nós estamos falando. É possível colocar dentro de um vírus hoje de covid 30 componentes que possibilitariam abrir um *backdoor*. Fazer verificação de todos esses componentes dentro de um equipamento hoje, seja o mais simples, o seu telefone celular, até o computador mais complexo, é impossível, é humanamente impossível porque nesses componentes hoje nós estamos chegando a bilhões de componentes por centímetro quadrado.

O que nós fizemos como primeiro ponto? Começamos a desenhar todos os nossos *chipsets* e manufaturá-los com fabricantes certificados de maneira que eles sejam seguros. E hoje, já pensando em 2022, 100% dos componentes críticos hoje garantimos que são de uma linha de produção segura.

O segundo ponto que nós temos que ver é a mudança desse ecossistema. Como já comentado aqui hoje, em uma rede 5G nós podemos fazer várias fatias dessa rede e conectar vários dispositivos. Então, eu posso ter uma fatia para a indústria automobilística, uma para a parte de segurança, outra para a parte hospitalar, e essas fatias são seguras por natureza. Mas a gente precisa imaginar o seguinte: à medida que eu vou da periferia da rede para a parte mais central da rede, mais e mais usuários podem ser afetados. Então, quando nós voltamos à apresentação do GSI, realmente, quando a gente vai para o núcleo da rede, nós podemos ver por esse eslaide que milhões de usuários podem ser atacados por uma pessoa só em um dado momento. E isso não é só o fator equipamento, mas é o fator humano, porque isso pode ser um técnico que, mal-intencionado, carrega um vírus no período de manutenção noturno. À medida que nós vamos mais para a esquerda do eslaide, nas torres, nas estações rádio base, nós temos menos usuários conectados, mas temos uma capacidade menor de ataque, uma exposição menor. Então, isso é um fator fundamental para entendermos o que nós estamos discutindo e o que nós estamos vendo.

Nós temos que imaginar também que muitos desses equipamentos, por exemplo, redes de fibra ópticas, estão nas nossas estradas, e é impossível supervisioná-las 24 horas por dia todo o ano.

Existem elementos de segurança da arquitetura de 5G que são definidos, padronizados mundialmente, e isso mitiga grande parte dos ataques possíveis, mas o elemento humano ainda continua. É claro, o que é que foi feito através do mundo, e nós somos partidários desses acordos? Por exemplo, na Europa criaram-se ferramentas de análise de segurança, de cibersegurança, para as redes 5G que são aplicadas a todos os Estados europeus. Cada Estado aumenta as suas particularidades de acordo com a Constituição Europeia, mas isso possibilita definir o seu conjunto de medidas para que os



fornecedores sejam, exatamente como colocado na apresentação anterior, culpados por riscos causados em infraestrutura de segurança do país. Esse é um dos pontos que nós colocamos.

Inclusive, semana retrasada o Governo finlandês assinou um acordo de cooperação de cibersegurança com o Governo brasileiro, garantindo uma total transparência de tudo que aconteça entre a Finlândia e o Brasil em termos de segurança, cibersegurança. Então, nós somos uma empresa finlandesa, e tudo que acontecer na Finlândia, em grande parte da rede da Finlândia – claro que é fornecida pela Nokia – será reportado automaticamente ao Governo brasileiro.

Existem outros tratados que foram feitos pela organização da defesa do Atlântico Norte, e assim nós podemos ter vários exemplos, através do mundo, da preocupação de segurança com a rede 5G.

Essa caixa de ferramentas da União Europeia cria medidas estratégicas e técnicas que não substituem umas às outras, mas a gravidade dos riscos depende da natureza do serviço e aplicação em causa. Ou seja, no fundo, os fabricantes e as operadoras são responsáveis pela segurança da rede, e é claro que eles também são parte integrante desse processo de segurança.

A segurança de uma rede 5G é baseada num triângulo de confiança e ética. Ela vai para a supervisão integrada da rede, de como essa rede se adapta a todo o crescimento – o 5G não é estático, ele vai evoluir nos próximos dez anos – e a escalabilidade dessa rede. E cabe destacar que nós, como empresa, fomos o único fornecedor de telecomunicações classificado como uma das empresas mais éticas em termos de fornecimento de equipamentos nos últimos anos.

E o nosso comprometimento é claro: nós protegemos as informações de nossos clientes como as nossas, somos transparentes em nossas práticas de segurança, incorporamos segurança em todos os nossos produtos e serviços, prontamente informaremos qualquer problema relacionado a produtos ou serviços e validamos independentemente nossas práticas de segurança. Esses são os compromissos de segurança da Nokia com o Brasil, e estamos abertos ao diálogo contínuo.

Muito obrigado, Senador.

O SR. PRESIDENTE (Jean Paul Prates. Bloco Parlamentar da Resistência Democrática/PT - RN) – Obrigado, Wilson.

Vamos à última, porém não menos importante, empresa das três.

Marcelo Motta, por favor, pelo acesso remoto. Está por aí?

O SR. MARCELO MOTTA – Com certeza, Senador.

O SR. PRESIDENTE (Jean Paul Prates. Bloco Parlamentar da Resistência Democrática/PT - RN) – Marcelo Motta é Diretor de Cyber Security da Huawei América Latina.

Bem-vindo, Marcelo. Por favor, a palavra é sua por dez minutos.

O SR. MARCELO MOTTA (Para expor. *Por videoconferência.*) – Muito obrigado, Senador, pela oportunidade. É um prazer enorme estar aqui hoje falando com o Senado, com os nossos colegas e com os ouvintes.

Eu tenho uma apresentação para compartilhar. (*Pausa.*)

Conseguem enxergar aí?

O SR. PRESIDENTE (Jean Paul Prates. Bloco Parlamentar da Resistência Democrática/PT - RN) – Pronto, já chegou. Está na tela.

O SR. MARCELO MOTTA – Perfeito.



Bom, apesar dessa minha carinha de chinês, eu sou Marcelo Motta, brasileiro, nascido em São Paulo. Estudei engenharia, fiz mestrado aqui no Brasil e, por mais de dez anos, fui professor na Escola de Engenharia Mauá. Ingressei na Huawei em 2002 e permaneci na Huawei do Brasil e América Latina até 2012, tendo, então, migrado as minhas atividades para a matriz da empresa em Shenzhen, onde atuava já nessa área de soluções e segurança cibernética.

Então, estou de volta aqui ao Brasil e vou começar falando um pouquinho, brevemente, a respeito da nossa empresa, para quem não conhece. Nós somos uma empresa global, estamos em mais de 170 países, fazemos parte da lista das maiores empresas do mundo, e basicamente o nosso progresso está conectado à inovação. Nós temos mundialmente mais de 197 mil funcionários, sendo mais da metade deles envolvidos em atividades de pesquisa e desenvolvimento, o que faz com que a gente tenha esses diversos títulos que eu aqui coloco: liderança em termos mundiais no que diz respeito à aplicação de patentes, por mais de cinco anos consecutivos, resultado de bilhões de dólares que investimos dentro dessa área, para poder inovar e trazer as melhores soluções aos nossos clientes.

A nossa base fica em Shenzhen. Somos uma empresa privada, 100% privada. Começamos a nossa operação em 1987.

Aqui são as áreas em que a gente atua. A gente oferece soluções de conectividade para as operadoras, sejam as grandes, sejam as pequenas, empresas, governos; dispositivos inteligentes também para os consumidores; e atuamos também na área de computação na nuvem.

No Brasil... Enganam-se aqueles que imaginam que a Huawei chegou aqui ao Brasil para atuar no mercado de 5G. Nós estamos aqui há mais de 23 anos e tivemos a oportunidade de participar de todo o processo de criação dessas infraestruturas de banda larga fixa e banda larga móvel no País, com muita cooperação com as grandes operadoras, com as pequenas operadoras, com o Governo brasileiro; na Copa do Mundo, nos Jogos Olímpicos. E somos pioneiros na introdução de novas tecnologias no País. Então, o que a gente está fazendo aqui no Brasil é justamente isto: infraestrutura de banda larga fixa e móvel; dispositivos inteligentes; computação na nuvem, atuando aí com as operadoras, com as empresas e também com o Governo brasileiro.

São mais de mil empregos diretos que hoje temos, 16 mil empregos indiretos, e temos dois centros de manufatura locais: um em Manaus; outro em Sorocaba, interior de São Paulo – basicamente, só para falar um pouquinho a respeito da nossa empresa.

Acho que já muito foi falado a respeito de 5G, a respeito da alta velocidade, quantidade de dispositivos que podem ser conectados à rede e o tempo rápido de resposta para essa tecnologia. Então, felizmente, esse leilão aconteceu e vai ajudar o Brasil a levar conectividade, a expandir banda larga fixa, a expandir banda larga móvel no País, atendendo escolas e residências e melhorando a infraestrutura de comunicação móvel do nosso País.

É importante ressaltar que eu fiz uma comparação entre Brasil e China, por exemplo, em que a gente tem aí uma densidade de estação rádio base, que são essas unidades, essas torres que dão cobertura de sinal. No Brasil, a gente tem uma densidade muito menor do que a densidade de estação rádio base que existe na China. Então, já no 4G existia um gap de torres e estações rádio base no nosso País. Então, esse é um problema que, provavelmente, a entrada do 5G no mercado vai ajudar a sanar para que a gente estenda a conectividade dentro do nosso Território aqui.



E o importante é o 5G dentro da indústria, que é o tópico aqui que a gente está tratando. A indústria brasileira perdeu produtividade na última década. E a gente tem aí, então, a oportunidade de usar a tecnologia 5G para trazer mais competitividade para a indústria brasileira.

E nós estamos aqui à disposição do Governo brasileiro e das operadoras para trazer essas tecnologias, para trazer a tecnologia 5G e as outras, toda a gama de produtos em que a gente atua. Na área de 5G, comprovadamente, existem aí experiências comerciais dentro desses diversos países que eu estou aqui colocando, em que os nossos parceiros, que usam os nossos produtos, oferecem aos seus clientes, oferecem às indústrias as maiores velocidades. Isso são dados públicos de redes comerciais.

E é importante também ressaltar que a gente vai trazer uma nova tecnologia. São altas taxas de dados. É importante a gente fazer isso com soluções que tenham desempenho e um consumo de energia otimizado, visto que isso certamente já fazia e hoje faz mais sentido ainda dentro do cenário em que a gente atua dentro do Brasil. Então, a gente está trazendo todo o resultado desse investimento em pesquisa e desenvolvimento para contribuir com o Brasil nessas áreas.

Nós fizemos um estudo junto com a Deloitte, e o impacto da introdução do 5G no País é um impacto muito relevante, de mais de 2,5%, ano a ano, por 15 anos consecutivos aqui no País. Então, isso contribuiria, em 15 anos, para um incremento de 40% no PIB brasileiro.

É importante também que o Brasil faça parte dessa cadeia de suprimentos global, beneficiando-se da economia de escala que existe. Como eu já disse, a gente atua em mais de 170 países. Isso faz com que, com mais competição, a gente consiga expandir a infraestrutura no País a bons preços para os consumidores, como já acontece no 4G, justamente na banda larga pré-paga, e eu estou falando aí justamente da parte mais baixa da população brasileira.

Então, o que nós fizemos? Nós pegamos o 5G, testamos com todas as grandes operadoras. Nós usamos o 5G no nosso centro de manufatura, no nosso *warehouse* em Sorocaba, o primeiro centro automatizado com 5G na América Latina. Tivemos ganhos expressivos de produtividade, mais de 25%, e reduzimos aí o tempo de um ciclo de produção de 17 para 7 horas. E é esse benefício que a gente quer levar para as outras áreas aqui no Brasil.

A gente também, em Sorocaba, está junto com a Prefeitura de Sorocaba, no Parque Tecnológico de Sorocaba, em uma iniciativa do Ministério da Ciência e Tecnologia, na criação de um centro de excelência para a indústria 4.0. A gente está junto nessa iniciativa também, levando o que a gente fez para esse centro para que isso possa também ser aprimorado e expandido para as indústrias no Brasil.

Também atuamos em diversas outras áreas, mineração, agricultura, sempre com ganhos bastante expressivos.

Nesse processo, a gente verificou que: conectividade é necessário? Sim. Agora, onde existem os maiores *gaps* para o Brasil poder usufruir dos benefícios da tecnologia? Está na capacitação da mão de obra, em você usar a conectividade para criar, por meio dela, aplicações inteligentes que façam uso do processamento de dados para você ter esses ganhos que aqui eu exponho.

Em relação à questão de segurança, as perdas estimadas aí com crime cibernético, somente em 2021, são da ordem de US\$6 trilhões – isso é maior do que o PIB do Japão, em 2021.



Isso não é um problema novo: tivemos aí históricos de vazamento de dados que deram origem à GDPR na Europa, depois à LGPD no Brasil; ataques de negação de serviço, que só crescem; ataques cibernéticos dentro do setor elétrico ou na infraestrutura hídrica; ataque na cadeia de suprimentos; *ransomware*. Então, vejam, isso já é uma realidade há muito tempo, e essa realidade também afeta as empresas aqui no Brasil, como, é público, aconteceu, por exemplo, recentemente, com a CVC, com a Renner, e aí existem também vários episódios de vazamentos de dados dentro do País. E nós estamos falando disso sem a introdução, ainda, da tecnologia 5G. Então, essas ameaças estão aqui presentes.

E como a Huawei enxerga o espaço cibernético?

Nós enxergamos o espaço cibernético quebrado em camadas. Você tem lá embaixo os dispositivos que fazem uso da rede, e essa rede provê conectividade. E você vai o quê? Esses dispositivos estão levando os dados para as nuvens, e esses dados que estão armazenados na nuvem vão ser usados pelos aplicativos. Então, se você tem o Facebook, você tem os seus dados lá na nuvem e você tem... Portanto, o Facebook é uma das aplicações; o WhatsApp é outra; o ViChat é outra, e assim sucessivamente. E essas diversas camadas a gente tem que proteger.

Então, a gente fala que: o espaço cibernético é maior do que, única e exclusivamente, as redes de telecomunicações; dois, é uma responsabilidade compartilhada.

Dentro da área de redes de telecomunicações, de forma específica, você tem o quê? O fornecedor do equipamento. Então, eu tenho que fornecer um equipamento seguro. A arquitetura dessa rede, a resiliência dessa rede, a redundância, na verdade, é uma responsabilidade da operadora. É ela que desenha a rede.

E aí você tem um terceiro aspecto, que é a operação. Eu posso ter o sistema mais seguro do mundo, a rede redundante e, por meios lícitos, a pessoa de operação vai, faz e acaba, pode comprometer a segurança da rede como um todo. Então, onde a gente atua? Nós fornecemos equipamentos de telecomunicações, de acordo com os padrões internacionais. Como vai ser montada essa rede, essa infraestrutura, como isso vai ser operado, a gente tem toda a colaboração com os nossos clientes, mas a geração dessa arquitetura e a operação acabam sendo responsabilidade dos nossos clientes.

Na área de telecom, isso não é uma responsabilidade nova das operadoras. As operadoras fornecem as redes – 2G, 3G, 4G, 4,5G –, as redes de banda larga fixa. E, quando aqueles ataques que a gente viu no eslaide anterior acontecem, qual operadora está envolvida? Então, o ponto é: eu não estou tirando a importância da questão de segurança cibernética para dentro do universo das redes de telecomunicações, mas nós temos que enxergar onde está o problema. A maior parte do problema está na camada de aplicação. Isso já existe única e exclusivamente hoje, já existe hoje! Então, o importante é a gente segmentar para poder endereçar bem esses problemas.

Nós atuamos em todas essas áreas e temos aí um investimento única e exclusivamente para a segurança cibernética, no ano passado, da ordem de US\$1,1 bilhão. Então, a gente tem trazido tecnologias avançadas para poder produzir os equipamentos da forma mais segura possível. Então, isso envolve todo o ciclo de vida do produto, não só o equipamento que eu entrego para o cliente, mas todo o *software* que vai ser colocado, que vai ser atualizado, como a gente vai entregar esse *software* para os clientes, por meio de processos com assinatura eletrônica, certificação de que o que vai rodar dentro de um equipamento é um *software* da Huawei, para justamente evitar que existam códigos maliciosos infiltrados por outros fornecedores. Isso é o que a gente



chama *trustworthiness*. E, somente nessa área, a gente está envolvido num projeto de mais de US\$2 bilhões, que começamos em 2019, para melhorar tudo isso, porque, visto que as ameaças aumentam, a forma como a gente produz o equipamento tem que continuar também progredindo.

Na área de dados, uma vez que existem os dados lá na camada de aplicação, é importante controlar quem vai ter acesso a dados, que esses dados sejam criptografados. Não é isso? E, se um *hacker* ainda assim invadir, é importante ter um mascaramento para que o *hacker* não consiga roubar toda a informação. Então, existem técnicas que a gente traz para as nossas soluções justamente para ajudar nesse processo de defesa.

Particularmente no que diz respeito às redes 5G, a rede em si, a segurança da tecnologia 5G se aprimorou em relação à tecnologia 4G. Então, certamente o quatro, a tecnologia 4G é mais segura que a tecnologia 3G também. Isso é por padrão. Eu trago, aqui no lado esquerdo, justamente essa comparação em diversos aspectos de que a tecnologia 5G é mais segura que a tecnologia 4G.

E aí existem várias formas de você olhar os equipamentos, olhar o processo de desenvolvimento para que você tenha o quê? Uma certificação externa para mostrar que você tem um processo de desenvolvimento seguro, que você tem um equipamento seguro que segue as normas e os padrões internacionais. Então, eu trago aqui o GSMA Nemas 3GPP, a especificação de segurança (Scas), e o Common Criteria, que é uma forma de avaliar equipamentos que está aí disponível no mercado desde 1994 e é largamente utilizado. Agora, isso não inibe os requisitos locais, como a Instrução Normativa nº 5, do GSI, a Resolução 740, da Anatel, e o Ato 77 também. Então, são todas iniciativas muito boas que a gente imagina para se certificar que a base, o fundamento dos equipamentos sejam seguros, mas não podemos esquecer das outras camadas também.

Dentro da empresa a gente tem aí todo um processo de governança em segurança cibernética. Somos mais de 3 mil profissionais dentro dessa área. Eu trabalhava no time global; hoje eu cuido da Huawei do Brasil e a Huawei América Latina. São mais de 12 áreas em que a gente atua.

Só mais um eslaide e eu estou terminando.

São mais de 12 áreas em que a gente atua, desde a definição de quais são os padrões que a gente vai usar a desenho da solução, com critérios de segurança e proteção de privacidade, já desde o começo do processo de desenvolvimento, seleção de parceiros – quem que vai fornecer *hardware*, quem que vai trabalhar conosco. A gente tem um processo de seleção para esses terceiros. Fechou o desenvolvimento, o time de pesquisa e desenvolvimento testa a solução. Antes de ir para o mercado, essa solução passa por um laboratório independente que vai testar essa solução antes que a gente autorize essa solução ser lançada no mercado.

Temos um time também que avalia as vulnerabilidades, quaisquer novas vulnerabilidades que possam aparecer na solução, para que a gente possa tratar e atender a todos os clientes, atualizar esses equipamentos para poder atender aos clientes.

E o mercado brasileiro nos conhece. Estamos aí de longa data no País. Nós temos, portanto, uma história aqui. Então, há algumas iniciativas dentro da qualificação de mão de obra, que a gente verificou que é um *gap*, mais especificamente instalação de fibra – a gente colocou um centro de capacitação profissional dentro dessa área.

Na área de segurança cibernética, inaugurei o nosso T-Center, o centro de transparência local aqui no Brasil, em julho deste ano. Representantes das grandes



operadoras, da Anatel, do GSI estiveram lá presentes. Temos, junto com o Inatel, a escola de engenharia aqui no Brasil... A gente patrocina um centro de cibersegurança que eles estão criando, justamente para que o Brasil consiga desenvolver cada vez mais a sua *expertise* dentro dessa área. E atuamos aí com uma vasta rede de universidades, promovendo educação *online*, compartilhando nossos conhecimentos, justamente para trazer todo esse conhecimento acumulado também aqui para o País.

E é basicamente isso que eu queria colocar, não é? A gente está aqui há mais de 23 anos. Prezamos por toda a transparência e cooperação com as operadoras e com o Governo. Não chegamos hoje aqui ao País. E é importante a gente fazer a distinção entre o que é uma notícia que aparece no jornal, a quantidade enorme de narrativas que se colocam presentes e, de fato, o que é a realidade. Não acho que nenhum cliente iria gostar de adquirir um equipamento que tivesse aí várias falhas de segurança, que fosse objeto de espionagem etc. Esses clientes testam a nossa solução, nos conhecem e confiam em nós. E o nosso objetivo é continuar contribuindo aí para o Brasil.

Agradeço a oportunidade e me coloco à disposição para as perguntas.

O SR. PRESIDENTE (Jean Paul Prates. Bloco Parlamentar da Resistência Democrática/PT - RN) – Perfeito, Marcelo. Muito obrigado.

Nós estamos – a quem assiste a nós – aqui, na Comissão de Ciência, Tecnologia, Inovação e Comunicação no Senado Federal justamente analisando e debatendo a implantação e a operação da tecnologia 5G, da indústria 4.0, como política pública sob a avaliação desta Comissão para este exercício.

Eu queria aproveitar e saudar o nosso Instituto Metrópole Digital, da Universidade Federal do Rio Grande do Norte, que tem participado das pesquisas e traz a inovação com cursos para os nossos estudantes lá do Rio Grande do Norte. Quero agradecer, inclusive, a parceria com a Huawei – o Marcelo está aqui presente –, que abriu aí cem vagas para estudantes do IMD, projeto 5G Training, no Rio Grande do Norte. Quero parabenizar obviamente a Universidade Federal do Rio Grande do Norte por estar protagonizando essa discussão e levando o nosso Estado do Rio Grande do Norte à ponta da inovação. Muita força aí para o Instituto Metrópole Digital!

Quero dizer, em relação aos trabalhos de todos os presentes, a todos que assistem a nós, que nós teremos agora, como próximos passos, a visita aos parques tecnológicos 5G das empresas que estão conosco aqui. Eu aproveito já para agradecer a vocês por nos receber na próxima semana, a cada uma das empresas, justamente para visitar os parques tecnológicos. Fazem parte do processo e do trabalho da Comissão essas visitas presenciais. No dia 1º de dezembro, teremos audiência com o Ministro das Comunicações; no dia três, imaginamos finalizar o processo de trabalho dessa avaliação, que é uma avaliação expedita, porém bastante concentrada, e por isso esse trabalho intenso – e essas apresentações que vocês trouxeram nos enriquecem muito –, e esperamos que até o dia 9 de dezembro tenhamos, portanto, a votação do nosso relatório final, contendo as recomendações – as análise, as recomendações e observações – desta Comissão do Senado a respeito dessa política pública.

Quero dizer também a quem está assistindo com interesse e que nos perguntam e a outros que obviamente de posse dessas apresentações também terão dúvidas... É sempre assim, não é? Quanto mais a gente conhece alguma coisa, mais a gente tem dúvidas sobre ela e mais tem interesse. Nós temos a intenção de fazer algo um pouco inovador aqui. Eu estava conversando com o Bennett e com a assessoria aqui, para colocar depois isso num *hotsite*, um *hotsite* simples, onde estarão o relatório final da Comissão, as apresentações de V. Sas. se nos autorizarem colocar lá – ou como



autorizarem colocar, porque às vezes o pessoal quer tirar um eslaide ou outro e tal; mas, como já foi apresentado publicamente, acho que não há problema –, e os *links* de todas as audiências em sequência. Para você que está em casa nos perguntando, por exemplo, sobre a implementação no Nordeste ou no Norte, isso já foi perguntado em audiências anteriores, e a gente já trabalhou esses questionamentos também juntamente com a discussão sobre o leilão. Então, ficaria ali tudo em sequência, e isso ficaria mais fácil para quem for pesquisar e se aprofundar sobre esse assunto, tanto gestores públicos, quanto interessados em geral, interessadas em geral, cidadãos, cidadãs, tudo isso compilado eletronicamente nesse *hotsite* acessível, com o registro de todo o nosso trabalho aqui, o processo de análise e as recomendações da política pública do 5G.

Queria agradecer ao Presidente Rodrigo Cunha, Presidente desta Comissão, pela deferência de estar presidindo esta análise. Queria também, pelo adiantado da hora, dizer que nós, claro, estamos extremamente satisfeitos – extremamente satisfeitos mesmo – com as informações e análises que vocês nos trouxeram hoje.

Eu vou saltar a sequência de palavras e de pronunciamentos finais, consultando aqui se há alguém em linha que tiver se inscrito. Acho que não há inscrições.

Tivemos a presença aqui registrada dos Senadores Vanderlan Cardoso, Paulo Rocha, Izalci Lucas, Rodrigo Cunha, Plínio Valério e Flávio Arns, membros desta Comissão.

Queria dar oportunidade, caso alguém queira, não insistindo absolutamente por questão das considerações de uns e de outros palestrantes aqui, para algum dos nossos convidados que gostaria de usar a palavra. Se quiserem, façam o sinal aqui conosco; senão, obviamente não é impositivo isso.

Eu queria saltar essa parte das considerações finais, agradecendo profundamente a cada um de vocês, desculpando-me evidentemente por um pequeno atraso, eventualmente algum estica aí das falas, mas acho que nós fizemos um compilado muito bom dessa questão da cibersegurança e do assunto que nós propusemos para esta terceira audiência pública na análise dessa política de 5G.

Portanto, quero agradecer a todos vocês, a todas vocês que nos trouxeram essas análises e dizer que às perguntas e aos esclarecimentos a própria Comissão está à disposição também para encaminhar outras respostas ou encaminhar as respostas dentro dos contextos das audiências que já tivemos; portanto, o nosso trabalho prosseguirá.

Não havendo, portanto, quem queira se pronunciar, acho que podemos considerar fechada mais esta audiência, agradecendo penhoradamente, mais uma vez, a todos que participaram dela e nos trouxeram essas suas apresentações, que muito contribuirão para a nossa análise e as nossas recomendações.

Muito obrigado a todos e boa tarde.

(Iniciada às 11 horas e 22 minutos, a reunião é encerrada às 13 horas e 30 minutos.)