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

REUNIÃO
15/12/2021 - 19ª - Comissão de Ciência, Tecnologia, Inovação e Informática

O SR. PRESIDENTE (Carlos Viana. PSD - MG. Fala da Presidência.) - Meu bom-dia a todos os senhores e também a todas as senhoras telespectadoras que nos acompanharão pela TV Senado, pelo nosso sistema de mídia social do Senado e também pela Rádio Senado. A todos o meu agradecimento por terem aceitado o nosso convite.

Declaro aberta a 19ª 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 e se destina à realização de audiência pública com o objetivo de debater o vazamento de dados pessoais de mais de 220 milhões de brasileiros - uma denúncia grave que foi feita pela imprensa e, a nosso ver, não investigada ou esclarecida da maneira correta -, em cumprimento ao Requerimento nº 1, de 2021, de minha autoria.

Você que nos acompanha pelas redes sociais e tem interesse em participar desta audiência pública poderá enviar perguntas ou comentários pelo www.senado.leg.br/ecidadania ou ligar para 0800 061 2211. Vou repetir: 0800 061 2211

Desde já, quero dar as boas-vindas àqueles que já se prontificaram. A Ana Cristina, de Pernambuco, já enviou a sua pergunta - muito obrigado, Ana -; também o Josue Rodrigues, do Rio Grande do Sul - obrigado, Josue -; o Rodrigo Silva, de Sergipe; a Raissa Siqueira, do Rio de Janeiro; e o Marcos Ribetti, do Espírito Santo. Obrigado a vocês desde já.

Então, você que quer participar e se informar mais sobre essa questão...

Também temos o Erick Faria, das minhas Minas Gerais - muito obrigado -, e o Jefferson Venancio, da querida Bahia, nosso Estado vizinho como o Espírito Santo.

Obrigado a vocês todos que estão participando. Enviem as suas perguntas. Eu vou repetir: www.senado.leg.br/ecidadania ou ligar para 0800 061 2211. Acessando o *site* do Senado, você terá todas as informações.

Esta audiência também agora vem em bom momento, uma vez que o País vem sofrendo, tendo notícias de uma série de ataques cibernéticos a dados essenciais, especialmente sobre a vacinação. Desde o último dia 10, nós temos uma série de tentativas de invasão, que conseguiram retirar do ar os dados do Conect SUS sobre a questão das vacinas. Ontem, também um novo ataque ao Ministério da Saúde - a rede interna foi desligada. Outros órgãos do Governo, também da área de segurança, como Polícia Rodoviária Federal, outros órgãos ligados à segurança, a Controladoria-Geral da União, a Enap (Escola Nacional de Administração Pública) e o Instituto Federal do Paraná sofreram ataques. Isso nos leva a discutir com muito mais seriedade.

O Brasil já avançou na questão da criação da Autoridade Nacional de Proteção de Dados, mas, para que se tenha uma clareza do que nós estamos tratando, as ameaças aos países não serão mais clássicas como no passado, de 1939 a 1945, com as guerras com grande movimento de soldados, de carros de combate e de aviões; as guerras serão de dados. Hoje, no mundo todo... Vamos falar aqui do recorte do Brasil: as nossas hidrelétricas, por exemplo, são todas elas automatizadas, e o Operador Nacional do Sistema controla a distribuição de energia elétrica em todo o País por meio de dados e de computadores.

Os aeroportos de todo o mundo, e não fora os brasileiros, também são controlados por dados, e o Sistema Nacional é quem faz toda a segurança de voos, aproximação, decolagem e controle, naturalmente, dos quesitos de segurança. Uma

possível guerra futura digital, naturalmente, pode criar confusões nos sistemas de defesa internos de um país e pode gerar, inclusive, uma defesa muito menor. Isso, é claro, nós estamos trabalhando aqui de forma hipotética, mas não de forma distante. Vejam, por exemplo, os dados do Conecte SUS, as vacinas que os brasileiros terão de apresentar, a comprovação para os que viajam, os que fazem turismo, os que moram, os estrangeiros que querem sair do país e se vacinaram por aqui. Esses dados são fundamentais para que nós tenhamos acesso e livre trânsito. É um dado de segurança individual.

São pontos importantes que nós precisamos discutir: se o Brasil está preparado e se nós brasileiros estamos, de fato, protegidos.

A suspeita, a denúncia do vazamento de 220 milhões de dados de brasileiros e estrangeiros é algo muito grave. Esses dados estão sendo usados de que maneira? Quem conseguiu ter acesso? De que maneira isso teria ocorrido? Quais foram as medidas tomadas, posteriormente, para que nós possamos evitar que, no futuro, tenhamos novos ataques?

Eu quero agradecer desde já as presenças, por videoconferência, do Procurador da República de Minas Gerais, Dr. Carlos Bruno Ferreira da Silva - meu muito obrigado -; Dr. Waldemar Gonçalves Ortunho Júnior, que é o Diretor-Presidente da Autoridade Nacional de Proteção de Dados, de cuja sessão para votação e sabatina eu tive a oportunidade de participar; Patrícia Peck Pinheiro, que é Presidente da Comissão Especial de Privacidade e Proteção de Dados da seccional de São Paulo da Ordem dos Advogados do Brasil; e Emílio Simoni, que é o Executivo-Chefe de Segurança da empresa PSafe, que vai nos falar sobre essa questão da manipulação e controle dos dados pela rede privada em nosso País.

Os nossos convidados terão, inicialmente, 15 minutos para a sua fala, e, posteriormente, nós abriremos o debate para as respostas das perguntas.

Por necessidade de outro compromisso, agradecendo mais uma vez ao Procurador da República Carlos Bruno Ferreira da Silva, concedo a ele a palavra por 15 minutos para o pronunciamento.

Dr. Carlos Bruno, meu bom dia ao senhor e muito obrigado mais uma vez.

O SR. CARLOS BRUNO FERREIRA DA SILVA (Para expor. *Por videoconferência*.) - Não, Senador, eu que, em primeiro lugar, quero dar muito bom dia ao senhor e a todos os que nos veem, neste momento, pela TV Justiça. Queria saudar o Dr. Waldemar, que faz um trabalho brilhante na ANPD, e a minha colega, Dra. Patrícia, que atua em proteção de dados na OAB.

Confesso que fico muito feliz com o convite. Peço desculpas de estar, inclusive, aqui no CNJ. Eu também sou titular de um ofício ambiental da Procuradoria da República de Minas Gerais e sou responsável pelos acordos de Brumadinho e de Mariana. E estamos, neste momento, aqui no CNJ, negociando a repactuação do acordo de Mariana, que é um acordo importantíssimo para o nosso Estado de Minas Gerais, Senador. Então, por isso, não posso, infelizmente, estar aí na companhia do senhor no Senado, apesar de estar fisicamente bem próximo - hoje não estou em Belo Horizonte, estou aqui em Brasília -, mas não poderia deixar de atender a esse convite para audiência pública.

Confesso que fico muito feliz que um Senador do meu Estado, como o senhor, traga esse tema, se preocupe com esse tema. Eu também saúdo o Dr. Emílio e peço desculpas de não ter falado, inicialmente, no seu nome. Fico muito feliz que um Senador do nosso Estado, do meu Estado se preocupe com esse tema. É um tema que eu me preocupo há muito anos. Fiz o meu doutorado, em Sevilha, já pensando em proteção de dados, e fico ainda mais feliz, Senador, com a sua fala inicial.

A nossa fala como palestrante é uma fala relativamente curta, mas a sua fala inicial já me ajuda muito, porque, além da motivação inicial da preocupação com essa *(Falha no áudio.)*

...milhões de dados, diretamente, dados de CPF, de nomes, dados de carros que, apesar de não ficar muito claro de onde foi a fonte do roubo desses dados, já deixa mais ou menos claro que são fontes públicas. Os dados de veículos são dados privativos do Denatran, do Detran, e já permitem alguns encaminhamentos, mas esse gancho que o senhor faz com os ataques ao Ministério da Saúde torna ainda mais claro o que eu pretendo falar na minha fala.

Há dois problemas separados quando há roubo de dados: há um problema de quem rouba os dados, e isso é um problema criminal, a Polícia Federal tem inúmeros bons estudos para se verificar quem rouba esses dados; mas há um problema tipicamente cível e administrativo, um problema que já foi abordado em várias leis de proteção de dados e, felizmente, no Brasil, a gente pode dizer, neste momento, que é abordado também pela nossa Lei Geral de Proteção de Dados, como eu vou mostrar.

É um problema que afeta não diretamente quem rouba os dados, mas, sim, quem guardou esses dados. Há obrigações dos titulares de banco de dados, obrigações que são muito sérias. Não há dúvida de que a gente está num processo de cultura da proteção de dados no Brasil, a lei é relativamente nova, a possibilidade de punição e de aplicação de sanções pela ANPD é mais nova ainda. A ANPD é um órgão recente, é um órgão que faz um trabalho brilhante, mas vem num

caminho ainda de se estruturar e é um órgão, como eu vou mostrar, fundamental para fixar a competência federal nesses casos de proteção de dados.

Eu acho que é muito provável que a gente vá seguir a jurisprudência da telefonia, em que os temas mais individuais são trabalhados na competência estadual e os temas que têm atuação da Anatel são trabalhados na competência federal, mas, realmente, esse gancho do senhor eu achei fundamental.

Ah, eu estou sem compartilhamento de tela. Eu já mandei a apresentação para vocês, eu vou seguir, aqui, a minha apresentação. Eu já autorizo, neste momento, o Senado que disponibilize a minha apresentação, para que nossos telespectadores possam ter acesso a isso.

Então, a primeira coisa que eu quero falar neste tempo curto em que eu vou estar falando - já passando para a próxima tela, a primeira tela é a minha apresentação -, é mostrar... Peço que passe para o próximo eslaide, se for possível, é mostrar que, na realidade, vazamentos de dados ocorrem no Brasil frequentemente.

Na realidade, esta minha apresentação é uma apresentação que eu adapto para este momento no Senado, mas é uma apresentação que eu já fiz no começo do ano, e não era a primeira vez que se vazaram dados no Brasil. Inclusive, houve uma sensação eu acho que, na sociedade, mas também no Ministério Público, que, inclusive, nos meses anteriores à entrada em vigor da possibilidade de sanções pela ANPD, houve até um aumento de vazamento de dados no Brasil, curiosamente houve esse aumento de vazamento de dados.

De alguma forma, até essas quadrilhas que já dominam dados... Eu me lembro que, quando eu falava de proteção de dados, inclusive dentro do MPF, ótimos procuradores falavam para mim assim: "Não, Bruno, mas se for na Praça da Sé, já estão lá vendendo todos os nossos dados, isso não é um tema para a gente discutir." E eu falava assim: exatamente por isso é um tema para discutir. Não é porque os nossos dados já estão em comercialização... E, no Espírito Santo, quando eu fui Procurador Criminal, eu entrei, inclusive, com algumas ações contra empresas que vendiam dados, entendendo que isso já era, na época, crime pelo Código Penal, especialmente porque essas empresas vendiam também dados bancários, dados que acessavam através do Serasa, mas não é porque nossos dados já estão na rua que isso não se torna um problema.

Peço que passe para o próximo eslaide, por favor.

Mas, no Brasil, a gente tem um pouco a sensação de que os problemas são só nossos. E outra coisa que eu também quero mostrar é que os problemas não são só nossos. Estou comentando um vazamento de dados da Adobe que é de 2013, vazamento de dados da rede de hotéis Marriott que é de 2018, vazamento de dados de servidores de internet de 2017, 2019.

Peço que passe para o próximo eslaide, por favor.

A diferença nesses países é que esses vazamentos de dados têm resposta, esses vazamentos de dados têm consequências. Então, dou um exemplo: a rede Marriott foi punida pela autoridade de proteção de dados do Reino Unido, que é uma ótima autoridade de proteção de dados, em 18 milhões de libras. A Adobe, lá em 2013... E vocês reparem que as punições vão aumentando com o passar do tempo. Há uma sensação, também mundial, claro, além da questão do dano, que é importante, do nível de vazamento, mas é um avanço mundial na compreensão de que vazamentos de dados são muito, muito sérios. Então, a Adobe é punida nos Estados Unidos, que tem uma legislação um pouco mais compreensiva com o vazamento de dados, diferentemente da legislação europeia, que é muito rigorosa quanto a isso...

(Intervenção fora do microfone.)

O SR. CARLOS BRUNO FERREIRA DA SILVA (*Por videoconferência*.) - Perdão, é que a reunião está aqui do lado.

A Adobe foi punida em US$1 milhão. Mas vocês reparem que a rede Marriott já é punida no Reino Unido em 18 milhões de libras, a Telecom já é punida na Alemanha em 10 milhões de euros, e a Equifax é punida no valor de US$700 milhões, e todas essas punições são alcançáveis no Brasil.

Pode passar, por favor, para o próximo eslaide.

Então, com o objetivo de acelerar a nossa apresentação - pode passar para o próximo eslaide, por favor - e permitir, inclusive, o debate, permitir eventuais dúvidas - vou dar meus contatos ao final - pelos nossos telespectadores, eu digo para vocês que toda base de Constituição e legislativa para haver proteção de dados já há no Brasil. Demorou muito - mas, felizmente, aconteceu - para o STF reconhecer a proteção de dados como direito fundamental, mas o STF, na Adin 6.387, reconhece a proteção de dados como direito fundamental e já temos uma LGPD, desde 2018, que já reconhece todos os critérios de proteção de dados que existem na legislação europeia.

Por favor, pode passar para o próximo eslaide.

Além disso, a ideia de vazamento de dados não é uma ideia unívoca. Na realidade, quando a gente fala em vazamento de dados, a gente fala de diferentes fatores. O primeiro é o que as empresas de informática fazem sempre conosco, que é pegar nossos dados e vendê-los.

A ANPD está fazendo um estudo muito bom, um estudo brilhante, relativo à nova política de privacidade do WhatsApp, uma política de privacidade que já foi punida na Europa, ela está fazendo um estudo muito sério em parceria da ANPD com o Senacom e o Ministério Público Federal. E, nesse aspecto, eu estou envolvido através da 3ª Câmara e do GT de Proteção de Dados e também do Cade, já com problema também de concorrência relativo a esse tipo de utilização, nesse caso, pelo WhatsApp, que foi uma utilização já punida na Europa. Além disso, existem empresas de mineração de dados, que buscam na internet dados pessoais para vender às pessoas. Eu também, no meu ofício, aí meu ofício de direito de cidadão, em Belo Horizonte, eu tenho um procedimento sobre essa liberação de dados. Há situações de vazamento de dados a partir de bancos de dados, que é um pouco o foco das notícias que motivaram esse convite do nosso querido Senador Carlos Viana, de Minas Gerais, e há também as quadrilhas que roubam dados, que se aproveitam de mandar *spam* em que as pessoas cliquem para que, com isso, possam roubar esses dados, que é outra forma de pegar dados de pessoas.

Por favor, o próximo eslaide.

Nisso entra um ponto que para mim é essencial na nossa conversa: o controlador de dados também tem obrigações na proteção de dados; a obrigação não é somente de verificar quem roubou os dados. Quem controla os dados, quem tem banco de dados de terceiros tem uma obrigação enorme de segurança e de prever privacidade como um conceito dentro do seu sistema e como parâmetro inicial do seu sistema. Os dados têm que ser recolhidos da forma mínima possível, e esses dados recolhidos da forma mínima possível têm que ser mantidos com segurança e a não manutenção disso com segurança causa punições e causa responsabilidade civil para o controlador. Isso está em todas as legislações, está no GDPR e está na nossa legislação, na nossa Lei Geral de Proteção de Dados. E esse dever de segurança é derivado de uma decisão do Tribunal Constitucional alemão de 2018.

Por favor, pode passar para o próximo eslaide.

O controlador é obrigado, e isso está na nossa lei, já cito aqui a LGPD, art. 48 da LGPD, a partir do momento em que se refira um incidente de segurança que possa acarretar risco ou dano relevante aos titulares, é obrigado a comunicar à autoridade nacional. Então, isso é uma obrigação do controlador de dados. Espero, por exemplo, que, nesses vazamentos que ocorreram na Polícia Rodoviária Federal e no Ministério da Saúde, os órgãos públicos federais já tenham feito isso ao MPD. Isso é fundamental porque, quanto antes se descobre o vazamento de dados, antes se têm condições de reprimir o vazamento de dados e diminuir os danos aos titulares, e isso evidentemente deve ser levado em conta quando a autoridade nacional determinar soluções.

Por favor, o próximo eslaide.

E essas sanções também já estão previstas na nossa lei, no art. 52, sanções que vão da advertência, multa simples, multa diária, publicização da infração, bloqueio de dados até, num nível mais alto, eliminação dos dados pessoais. A lei também, no seu §1º, já cria todos os critérios para publicação dessa sanção para o MPD, deixando claro que houve uma prorrogação de vigência em relação à aplicação das sanções, mas, desde 1º de agosto de 2021, a autoridade nacional já pode aplicar essas sanções.

Próximo eslaide, por favor.

Por fim, ressalto que, no art. 42 da nossa lei, fala-se em responsabilidade e ressarcimento de danos. Então, além da punição administrativa, cabe ao controlador de dados também uma ação de conscientização. E essa ação pode e deve ser feita coletivamente, por meio do Ministério Público Estadual e do Ministério Público Federal. No caso do Ministério Público Federal, não tenho dúvida de que se deve seguir a jurisprudência do Superior Tribunal de Justiça, que é uma jurisprudência baseada na telefonia, mas que se aplica tranquilamente à proteção de dados, em que o critério de ser competência jurisdicional federal ou estadual, e consequentemente competência de atribuição para ação civil pública do Ministério Público Federal ou do Ministério Público Estadual, é ação da MPD. Então eu tenho, no meu ofício de Direito do cidadão em Minas Gerais, vários procedimentos aferindo regularidade de proteção de dados, por exemplo, na área de farmacêuticas, na área de farmácias. Como eu falei, estou verificando a questão do reconhecimento facial do Aeroporto de Confins, estou verificando essas empresas de mineração de dados, mas sempre tomo como critério essencial a atuação, e a atuação tem sido, até este momento, muito feliz, com a presença do Dr. Valdemar, brilhante por parte da MPD, a atuação da nossa MPD, porque entendo que esse é o grande critério de fixação da competência federal.

Por favor, passe o meu último eslaide. Por favor.

Com isso, já faço o meu agradecimento a vocês, deixo o meu e-mail do MPF, meu e-mail funcional, deixo o meu contato no Twitter, local em que eu tento divulgar tanto o trabalho ambiental do Ministério Público Federal, quanto essas atuações e as questões relevantes de proteção de dados.

Agradeço enormemente a oportunidade, peço desculpas por hoje estar premido por um outro compromisso também muito importante para a sociedade brasileira e para a sociedade mineira. E por fim, agradeço enormemente a oportunidade, agradeço o convite e estou aberto a eventuais perguntas futuras. Infelizmente não vou poder ficar ao longo da nossa audiência pública, mas estou aberto a perguntas futuras no meu *e-mail* e por meio do Twitter.

E estou aberto a convites e, mais uma vez, saúdo enormemente o Senador Carlos Viana, do nosso Estado de Minas Gerais, pela iniciativa e por essa preocupação com esse tema tão importante para a sociedade brasileira.

Muito obrigado.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Obrigado, Dr. Carlos Bruno, Procurador da República em Minas Gerais.

Eu acredito que pela exposição que o senhor fez, nós tenhamos respondido aqui à pergunta do Rodrigo Silva, de Sergipe: "Quais mecanismos legais já aprovados na legislação penal ou propostas para punição adequada, visto que são dados sensíveis de pessoas?" O senhor concorda? O senhor quer acrescentar alguma coisa ao Rodrigo Silva, de Sergipe, Dr. Carlos? *(Pausa.)*

O áudio, por favor. *(Pausa.)*

Ok.

O SR. CARLOS BRUNO FERREIRA DA SILVA (Para expor. *Por videoconferência*.) - Senador, acho a pergunta muito boa do nosso telespectador, mas digo para o senhor: já há meios na nossa legislação. Os meios, claro, sempre podem ser melhorados.

Do ponto de vista cível, a nossa legislação é muito boa. A atuação do Congresso Nacional, na feitura da Lei Geral de Proteção de Dados, foi uma atuação brilhante. A nossa lei reproduz quase *ipsis litteris* a legislação europeia, que é o que há de mais moderno sobre o assunto. Então não tenho a menor dúvida de que nós temos todas as condições, no Brasil, para atuação administrativa e cível.

E digo também que acho que do ponto de vista penal, a legislação penal já fala em direito a sigilo há muito tempo. Há já normas que punem criminalmente esses casos há muito tempo, desde o nosso Código Penal, que é bastante antigo.

Eu não tenho dúvida de que com a verificação da proteção de dados, se criam novas hipóteses de sigilo, mas não tenho dúvida, e vários colegas do GT de Crimes Cibernéticos, do MPF, colegas da Polícia Federal têm feito manifestações para a melhora da nossa legislação processual penal e da legislação penal.

Há uma proposta, que também está no Parlamento, de adesão no Brasil à Convenção de Budapeste, que eu acho que seria essencial para que se melhore a repressão penal nesses casos, mas eu não tenho dúvida de que nós já temos condições de fazer essa repressão penal e que há muitas boas propostas dentro do Congresso Nacional, que ainda podem melhorar ainda mais a repressão penal, tanto do ponto de vista material, quanto do ponto de vista processual. Se fosse destacar um ponto específico, diria que a aprovação da Convenção de Budapeste, que é uma convenção importantíssima na repressão de crimes cibernéticos, que me parece essencial, que seja feita pelo Congresso Nacional.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Muito obrigado, Dr. Carlos, Convenção de Budapeste... Vou anotar essas sugestões aqui. Agradeço a presença. O Dr. Bruno deixou, inclusive, os contatos dele de *e-mail* e tenho a clareza que poderá responder a todos.

Um bom trabalho e façamos um bom acordo em Mariana, Dr. Carlos, porque a reparação por Brumadinho - eu posso dizer para o senhor, com muita alegria e com muita humildade - nasceu aqui no Senado. Nós, na CPI que fizemos aqui, em que eu fui Relator, ao final, eu coloquei que a empresa Vale não devia apenas indenizações materiais e humanas, a Vale devia uma reparação ao Estado de Minas Gerais e ao Brasil pela imagem que ela nos deixou por conta do crime ambiental. A força tarefa do Ministério Público abraçou essa ideia. Nós conseguimos um acordo, que hoje é muito importante. E Mariana, pela dimensão que teve, por abarcar Minas, Espírito Santo, inclusive até parte da Bahia, esse acordo de reparação à imagem do nosso País também é muito bem-vindo, para que a gente possa dizer claramente a essas empresas que nós concordamos que elas tenham liberdade de trabalho, que elas são muito bem-vindas, mas que elas têm responsabilidades com relação ao meio ambiente e à legislação brasileira.

Muito obrigado, Dr. Carlos. Parabéns pelo trabalho.

Eu convido aqui a Dra. Patrícia Peck Pinheiro, que é Presidente da Comissão Especial de Privacidade e Proteção de Dados da Seccional de São Paulo da Ordem dos Advogados do Brasil, para que possa fazer a exposição.

Dra. Patrícia, mais uma vez, o meu bom-dia.

Muito obrigado à senhora pela presença.

A SRA. PATRÍCIA PECK PINHEIRO (Para expor. *Por videoconferência*.) - Bom dia, Senador. Agradeço a oportunidade de estar aqui na audiência pública e também vou pedir para compartilhar alguns eslaides.

Acredito que vou complementar a fala do colega, do Dr. Carlos Bruno, em alguns aspectos. Parabenizo a iniciativa. É um tema de extrema relevância e, se eu puder compartilhar aqui a minha tela... Obrigada, já vi que foi autorizado compartilhar a tela. Já passo rapidamente à apresentação dentro do tempo de 15 minutos.

Então, primeiramente para contextualizar, o Brasil sofre hoje um apagão de segurança digital. Acho que esse é um dos pontos mais preocupantes. O ano de 2021 é o ano da nossa insegurança cibernética e é um ponto de atenção, de preocupação com o cidadão brasileiro. O que podemos fazer? Por que chegamos a esse ponto? Lembro muito bem de, em 2019, estar num evento na Espanha, a convite e indicada pelo Governo brasileiro, e que a temática já era esta: como vamos trabalhar melhor nossa frente de segurança cibernética?

Se vivemos numa sociedade digital que depende tanto de uma infraestrutura de telecomunicações e tecnologia, temos que garantir ao cidadão o exercício dos seus direitos digitais e, nessa frente, estão segurança, privacidade, já que o exercício da própria liberdade depende disso.

Então, hoje, todo cidadão brasileiro é um cidadão que reúne um conjunto de dados pessoais, e dados pessoais sensíveis, como foi bem colocado aqui. Se isso for vazado e exposto, a primeira coisa que pode acontecer com cada um de nós é um furto de identidade - *identity theft* -, ou seja, outra pessoa pode conseguir ser você por aí. Foi o que mais aconteceu neste ano: um aumento vertiginoso da fraude eletrônica. Isso, com toda certeza, aumenta o custo Brasil, gera um aumento, um efeito em juros. Como nós podemos recuperar a identidade desse indivíduo? Como podemos recuperar a confiabilidade das informações? Se você reunir hoje o nome de uma pessoa, o CPF, o último número de telefone celular, o endereço residencial e mais alguma informação que tiver sido exposta, como vimos - informações, às vezes, relacionadas ou ao âmbito de trabalho, ou de saúde -, você consegue fazer um cartão de crédito, abrir uma conta, até cadastrar-se em um partido político ou fazer outros cadastros que são estabelecidos.

Então, o Brasil virou alvo número um de ameaças cibernéticas, considerando outros países, como esse gráfico apresenta, e também de ataques de sequestro de dados. Esse é um ponto de atenção que eu gostaria de colocar aqui na audiência do Senado.

Como foi bem colocado pelo Dr. Carlos Bruno, nós já temos, sim, um marco legal de proteção de dados pessoais, temos um tratamento para âmbito administrativo e civil, mas vamos refletir: será que nossa legislação, do ponto de vista criminal, já ataca bem o problema do sequestro de dados pessoais, tamanho o impacto danoso social que essa prática realiza? Nós não temos essa tipificação específica. Então, talvez seja necessária uma reflexão, como já tem sido feito por outros países. A administração Biden, nos Estados Unidos, reuniu uma série de países para debater como poderia haver uma penalização maior e um rigor maior para o combate ao sequestro de dados, até porque isso afeta soberania nacional, segurança nacional.

Então, nós vimos aqui que o aumento de ataques de sequestro de dados no Brasil foi extremamente elevado, sendo o Brasil destaque frente ao mundo. Somos alvo! O Brasil é alvo por seu porte, por seu tamanho, mas também pelo quê? Pela falta do dever de casa, nos últimos anos, com segurança cibernética e porque a pandemia nos fez estar mais virtualizados. Estamos trabalhando mais com uso de recursos remotos, com uso de recursos de mobilidade e com uso de recursos de nuvem, que são alguns dos indicadores que podem ter permitido essa escala de insegurança digital.

Logicamente, isso já foi apresentado. Estamos aqui diante de um contexto de um ano de megavazamentos. E o que isso trouxe? O medo da população. O brasileiro tem medo, está com medo por conta do comprometimento das suas informações. E o que podemos fazer a respeito? Não pode haver paralisia. Tem que haver investigação e tem que haver a reação em cima da investigação. O que evita que o raio caia duas vezes no mesmo lugar? Como evitar que aconteça de novo? Como fortalecer nossas medidas de proteção?

Sabemos - eu já fazia atuação na parte de segurança cibernética há muitos anos, inclusive em colaboração com várias entidades públicas - que mesmo na área militar, que nós precisamos garantir também uma linha de defesa, que é o cidadão. Então estava também faltando uma campanha pública educativa à população de como se proteger. Se hoje passa um bandido e leva o celular de uma pessoa, rapidamente também consegue muitas informações e, a partir dali, consegue acessar informações das instituições.

Logicamente precisamos que as investigações evoluam, mas, principalmente precisamos de orçamento. Investir em segurança de informação exige recurso. Não conseguimos ter o ambiente mais seguro sem tecnologia, processos e pessoas - são as três frentes de atuação que precisam ser prioritárias.

Só rapidamente para um esclarecimento aqui, já que estamos em uma audiência, inclusive com os próprios cidadãos: o vazamento envolve, normalmente, um acesso indevido a dados, que podem ser tanto coletados, compartilhados ou divulgados na internet. Quando acontece um sequestro de dados, significa que ele fica obstruído. Muitas vezes, ele pode ficar bloqueado para acesso da própria instituição, o que gera uma barreira para a continuidade da operação. Você precisa fazer uma recuperação daquela base de dados. A violação de dados, então, ocorre quando a instituição sofre um incidente de segurança e ela tem responsabilidade pela proteção daqueles dados, como a legislação mesmo hoje já impõe - muito bem colocado pelo Dr. Carlos Bruno -, e essa violação resulta, então, em algum comprometimento de confidencialidade, de disponibilidade ou de integridade.

Os prejuízos são enormes, porque, além de você correr o risco da exposição daquela informação, você também tem uma paralisia do serviço público de atender ao cidadão enquanto você não puder gerar recuperação dos sistemas de forma confiável. Normalmente, uma das medidas de proteção é fechar a porta; se eu estou sob ataque, temos que bloquear acessos para todos, até que a gente possa disponibilizar novamente o ambiente.

Então, um vazamento pode ser originado de várias formas por ação ou por omissão: eu posso ter códigos maliciosos; posso ter senhas fracas ou senhas vazadas; posso ter ação de pessoas internas, que estão sendo facilitadores para que alguém de fora consiga acessar; posso ter também um furto de equipamento; um erro; uma negligência; não ter feito um *backup;* um ataque direcionado; ou erro de configurações.

Agora o mais importante: por que somos tão vulneráveis? Estamos atrasados no cumprimento da LGPD, uma lei completamente vigente e, quando olhamos o plano de implementação das instituições - isso já foi uma mensagem colocada pelo próprio TCU aos entes públicos -, ainda estamos num programa de conformidade, ainda precisamos alcançar essa conformidade, ainda temos um dever de casa a fazer, não fizemos todo o dever de casa, precisamos também ter uma política pública que priorize a proteção de dados. Como vamos dar subsídios, ferramentas, equipes, orçamento para viabilizar o cumprimento da legislação? A lei foi feita, a lei foi promulgada, a lei está vigente, nós temos que auxiliar as instituições a colocar em prática o que a lei determina.

Desde 2016, está pendente, em implementação efetiva, a Estratégia Nacional de Segurança Cibernética; avançamos, em 2020, com o Decreto 10.222, que criou o E-Ciber, e pouquíssimo em 2021, com a implementação mesmo da nossa Política Nacional de Segurança Cibernética, que é essencial e anda de mãos dadas com a legislação de proteção de dados e implementação em nível federal. Tem que haver, sim, temos que ter penas mais severas para crimes cibernéticos nesse nível, como o de ataque para sequestro de dados e vazamento de informações de proporções catastróficas. Isso, em outros países, vem sendo estudado para elevar para uma gravidade no mesmo nível de ciberterrorismo. Precisamos de uma força-tarefa dedicada ao combate ao crime organizado digital, porque alguém precisa pegar o bandido também - é lógico que a gente prepara o preventivo, as proteções, mas, se há alguém atacando a todos, e não formos atrás de quem está atacando, efetivamente nós temos o próximo ataque acontecendo amanhã, depois de amanhã, na próxima semana, isso não vai parar -, e da realização de uma campanha pública educativa efetiva à população, porque esse cidadão mais esclarecido também se protege mais, também faz a denúncia, também consegue ser aquele que olha e identifica a atividade suspeita para poder reportar a um canal da força-tarefa e colaborar para que a gente possa ter efetividade em prender quem está realizando esses ataques.

Já foi passada essa parte da fundamentação legal pelo meu colega Dr. Carlos Bruno. Então, eu vou passar rapidamente. A legislação já tem a previsão efetiva na parte cível e no compromisso de que instituições públicas e privadas devem cumprir com a lei, devem reportar à ANPD. A ANPD vem fazendo um trabalho excepcional, mas também precisa de recurso; também precisa de orçamento; precisa estar posicionada como órgão central de fiscalização e interpretação da legislação; precisa ganhar mais espaço em 2022, para efetivamente realizar o quê? A ANPD precisa efetivamente realizar a fiscalização.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Dra. Patrícia...

A SRA. PATRÍCIA PECK PINHEIRO (*Por videoconferência*.) - Sim, vou fechar.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Dra. Patrícia, só vou interrompê-la um minuto, só um segundo. É porque a tela não está tendo uma sequência, o controle está com a senhora. Então, a senhora está falando, e a apresentação não está seguindo.

A SRA. PATRÍCIA PECK PINHEIRO (*Por videoconferência*.) - Ah, não? Então, espere aí. Deixe-me ver por que não passou, me desculpe.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Isso.

A sua exposição está excepcional, muito clara; uma leitura muito abrangente e profunda do que estamos...

Isso. Aí, sim.

A SRA. PATRÍCIA PECK PINHEIRO (*Por videoconferência*.) - Essa tela aqui, agora, apareceu?

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Isso, agora, sim.

A senhora tem o controle, pode dar sequência. Perdoe-me a interrupção.

A SRA. PATRÍCIA PECK PINHEIRO (*Por videoconferência*.) - Ah, sim, que pena. Achei que estava mudando a tela, mas muito obrigada, Senador. Nós aqui no remoto temos essa problemática de não saber de tudo que está se passando.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Olha, doutora, há um termo que não faz parte da Língua Portuguesa ainda, mas que nós precisamos colocar no dicionário que é a "solucionática". *(Risos.)*

A SRA. PATRÍCIA PECK PINHEIRO (*Por videoconferência*.) - Concordo, concordo!

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - A problemática nós temos; agora, é a "solucionática".

A SRA. PATRÍCIA PECK PINHEIRO (*Por videoconferência*.) - A "solucionática", concordo.

Aqui, temos aquela tela resumo, fazendo o nosso dever de casa, com algumas sugestões importantes.

E, passando, então, essa parte que seria o embasamento legal já previsto pela Lei de Proteção de Dados, que já requer e exige que as instituições estejam em conformidade, mas precisamos auxiliá-las a ficarem em conformidade. A lei já trouxe a exigência. A questão agora é o plano de ação e o que eu quero comentar como conclusão da minha fala, viabilizarmos principalmente a fiscalização. E é uma fiscalização orientativa, pró-ativa, que pega pela mão e ajuda as instituições dentro de um ciclo de monitoramento, para iniciar em janeiro.

Logicamente, agora também temos o Conselho Nacional de Proteção de Dados, constituído com os conselheiros titulares, para também apoiar um trabalho evolutivo da legislação junto com a autoridade e também com relação ao trabalho educativo. Temos uma lei nova que ainda precisa ser muito mais orientada, precisa de um plano de ação para conseguir ser concluída a sua implementação e a fiscalização, porque isso vai apoiar para que a gente consiga ter visibilidade do grau de maturidade dos programas de proteção de dados que estão ainda em implementação nas diversas instituições públicas e privadas, mas devemos já ter um olhar para os setores críticos. Então, precisamos olhar para os setores críticos - saúde, água, energia, financeiro, nuclear, transporte, telecomunicações e a própria administração pública - a serem priorizados, para termos aí um caminhar para 2022, de forma a conseguir alcançar um estágio de segurança digital do Brasil que possa proteger mais o cidadão.

Então, eu concluo aqui a minha fala. Agradeço a oportunidade. Já deixei esse material também, foi enviado para ser compartilhado para todos. Fico à disposição para responder dúvidas aqui de todos.

Muito obrigada.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Dra. Patrícia, muito obrigado pela gentileza.

Gostaria de saber se a senhora disponibilizaria essa apresentação para os nossos telespectadores e telespectadoras interessados em acompanhar. Nós temos vários profissionais da área de tecnologia da informação que estão agora conectados e que têm enviado aqui, inclusive, as suas sugestões e as perguntas. Se a senhora nos permitir, há até um *e-mail* da senhora, por exemplo, aquela primeira apresentação. Não é isso? Nós temos o contato, se a senhora permitir, e as pessoas solicitarem essa apresentação.

A SRA. PATRÍCIA PECK PINHEIRO (*Por videoconferência*.) - Sim, perfeito, Senador, claro. Está autorizado, sim, compartilhe.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Está bem. Então, já está disponibilizado na página aqui? *(Pausa.)*

Está ótimo.

Então, já está disponibilizado àqueles que quiserem acessar informações da Dra. Patrícia, inclusive eu. Há algumas exposições ali que podem embasar um trabalho nosso aqui no Senado de ampliação. Por exemplo, quanto à essa questão inclusive que foi sugerida pelo Dr. Carlos, da Convenção de Budapeste, se cabe ao Congresso, então é dever nosso já buscarmos uma solução para que seja aprovado o mais rápido possível. E, dentro do que a senhora colocou, para a ampliação e a modernização da legislação brasileira, e nós contamos com o apoio da OAB no sentido de também colaborar.

Muito obrigado, Dra. Patrícia, pela exposição.

Eu convido o Dr. Waldemar Gonçalves Ortunho Junior, que é Diretor-Presidente da Autoridade Nacional de Proteção de Dados, que tem hoje a responsabilidade, uma grande responsabilidade, pelo que as senhoras e os senhores estão

acompanhando, num novo tempo. É interessante, Dr. Waldemar, que, quando nós falamos... Eu fiz a abertura aqui da nossa audiência pública citando os grandes e vários efeitos do vazamento de informações e dos ataques cibernéticos. Começa de uma maneira simples em que, por exemplo, um aposentado do INSS tem seus dados vazados e começa a ter a vida infernizada por ofertas de crédito consignado. É um problema sério.

Eu mesmo já me deparei, antes da minha vinda para o Senado, com empresas especializadas em fornecer dados das pessoas aposentadas do INSS. Esses dados vêm de algum lugar. E a legislação brasileira hoje dá conta de punir, inclusive, servidores públicos que facilitem o vazamento.

Mas nós vamos subindo... A escala de ameaças é muito grande. Eu citei aqui, de forma hipotética, mas importante, que hoje o conceito no mundo não é um conceito de guerra; o conceito é de defesa. Como os países já têm suas fronteiras delimitadas... O Brasil, por exemplo, é um País que não tem nenhum tipo de problema fronteiriço. A nossa relação com os vizinhos é muito pacífica há séculos. Mas, no mundo, os dados hoje valem muito dinheiro. A questão não está mais nas terras, mas está nas informações, que podem ser sequestradas e que valem muito dinheiro para as quadrilhas especializadas no exterior. E essas ameaças vão desde aquelas feitas no âmbito particular, como disse a Dra. Patrícia, como o roubo de um celular, como o fato de uma pessoa se passar por qualquer um de nós e fazer compras no cartão de crédito, a ameaças a aeroportos, no controle das informações, a ameaças ao sistema de controle aéreo nacional, a ameaças na questão da distribuição de energia e de vacinas.

Então, Dr. Waldemar, nós estamos diante de um novo tempo. Eu diria, quando muitas pessoas dizem que o mundo vai acabar, que o mundo acaba todas as vezes que nós somos desafiados a nos modernizar e a viver uma nova etapa.

A palavra está com o senhor, por favor, Dr. Waldemar.

O SR. WALDEMAR GONÇALVES ORTUNHO JUNIOR (Para expor. *Por videoconferência*.) - Bom dia, Senador! Inicialmente, eu gostaria de agradecer a oportunidade de a ANPD mostrar o seu trabalho. Quero parabenizá-lo por trazer este tema importantíssimo ao debate.

Desde o momento em que saiu a nomeação da ANPD, a divulgação de vazamentos foi cada vez maior, mais incisiva, com megavazamentos. O vazamento de 220 milhões de dados pessoais é, praticamente, o de toda a nossa população brasileira. Essa é uma preocupação não apenas da ANPD, do Senado, do Governo; acho que é uma preocupação extremamente elevada de todos os brasileiros. É uma invasão da nossa privacidade, é uma exposição dos nossos dados, o que nos afeta de forma bastante direta, o que é preocupante.

A Lei Geral de Proteção de Dados, na sua aprovação, já traz uma tranquilidade. Como o nosso amigo Carlos Bruno expôs, é uma lei bastante moderna, de bastante complexidade. São 65 artigos que ainda têm que ser analisados pelas empresas. Nós estamos em um processo educativo, em um processo de mudança de cultura necessário para o País. Eu acho que não só os setores, mas os próprios titulares de dados têm que entender quais são os seus direitos, quais são os riscos que eles correm normalmente quando disponibilizam dados sem analisar por que a empresa está pedindo aquilo. O próprio procurador citou que hoje a nossa ideia de minimização é importante. É importantíssimo nós buscarmos essa cultura em termos de proteção de dados.

Se nós analisarmos... No dia 19 de janeiro, quando a ANPD tomou conhecimento através da imprensa do grande vazamento, através até da descoberta pelo laboratório da PSafe, mesmo com uma estrutura precária - na época, nós não tínhamos nem 20 servidores -, nós já entendemos que tinha que haver uma ação conjunta. A ANPD não vai conseguir mudar esse cenário de forma isolada. Então, nós já notificamos a Polícia Federal, para dar início à apuração. E já articulamos com o NIC.br, com o CERT.br, com os diversos setores do Governo, para que, com sua *expertise*, possam nos ajudar a determinar quem são os controladores que, por algum motivo, deixaram que esses dados fossem vazados. Firmo bem a responsabilidade do controlador de dados. Ela é importantíssima. Quando ele assume os dados de um titular, a responsabilidade pelo sigilo e pela manutenção passa a ser toda do nosso controlador.

Sabemos que é um caminho longo esse de cultura, mas é algo que vamos ter que percorrer.

A ANPD tem um caráter hoje de normatizar e de fiscalizar. Então nós somos reguladores, nós somos fiscais. Sempre nós buscamos, com as melhores técnicas, com as técnicas mais modernas... Já que somos um órgão que mal completamos um ano, tivemos, então, a vantagem de buscar o que há de mais moderno e de colher todos os bons exemplos de outras agências reguladoras e - por que não? - das autoridades de outros países. Então, nós nos aproximamos de outras autoridades, vimos quais eram os procedimentos, selecionamos o que era mais adequado à Autoridade e passamos a atuar no nosso cenário nacional.

Quero deixar claro que, no setor privado, no setor público, nós temos o mesmo tratamento em termos de fiscalização ou em termos de sancionamento. A única diferença é que não faz sentido uma punição pecuniária ao setor público, porque

isso significaria tirar de um bolso para colocar em outro. Mas o tratamento tem sido bastante incisivo e bastante pontual em cima de todas as denúncias, de todos os comunicados de vazamentos que a Autoridade tem recebido.

Quando do caso típico que nós tivemos em maio, quando se divulgou o compartilhamento de dados entre o Facebook e a empresa WhatsApp, nós entendemos que não era apenas a ANPD que deveria atuar nesse caso, montamos o que chamamos de "quarteto", juntando a ANPD com o Ministério Público, com a Senacon e com o Cade, e passamos a atuar de forma conjunta. Acredito que todos foram unânimes em ver que os resultados foram melhores para todas as partes, para os quatro órgãos, para os titulares de dados e para as próprias empresas, porque, vamos dizer, era uma conversa única, e não precisávamos ficar repetindo a mesma conversa com os órgãos.

Então, essa forma de atuação, em que nós passamos a estabelecer acordos de cooperação técnica que agilizam essas ações, mostrou-se bastante eficiente e foi a nossa prática desde então. Temos utilizado esses acordos para, em qualquer vazamento, agilizar essa comunicação, agilizar, vamos dizer, as medidas mitigadoras de qualquer vazamento. Eu lembro que, em qualquer vazamento, o controlador, pela Lei Geral, comunica à Autoridade, entra em contato com os titulares de dados afetados.

Então, são regras já estabelecidas na própria lei, e é encargo da ANPD fiscalizar o cumprimento dessas regras. Então, em todos os casos que nós recebemos, nós estabelecemos um início de processo. Em função desse processo, passamos a abrir esse diálogo com a empresa, pois nós temos que ter as informações necessárias para tomar as nossas medidas quanto à aplicação ou não de sancionamento, sabendo qual o nível de comprometimento que a empresa teve nos diversos casos.

Lembramos que invasão sempre vai ocorrer. Se nós melhoramos a nossa tecnologia para a proteção, o criminoso também melhora a sua tecnologia de ataque. Preocupa-nos, no próximo ano, com a entrada do 5G, a velocidade... Tudo que vai ocorrer em termos de compartilhamento de dados, de transmissão de dados, vai ser acelerado de uma forma extremamente elevada. Então, com o 5G, ações em que levávamos horas, vamos executá-las em minutos. Essa parte é boa para nós, mas também o é para o cibercriminoso, pois, rapidamente, ele consegue copiar e extrair informações, de forma ilícita, de bancos de dados.

Vemos que é bastante importante essa conversa com o setor. Os setores têm que montar guias de boas práticas. Muitos ataques, muitos vazamentos são direcionados por falta de uma política eficaz de segurança. O controlador tem que entender a sua responsabilidade quando um dado é vazado. A ANPD vai atuar em cima do controlador. É importante o controlador usar dessa política boa de governança, mas também investir em tecnologia. Um dado que tem o seu vazamento, mas que estava criptografado, anonimizado ou pseudoanonimizado... Essas são técnicas que fazem com que o dado se torne inútil ao invasor, por ele estar de uma forma não clara. Isso são importantes medidas que até inibem esses ataques.

Então é muito importante que os diversos setores vistam essa camisa de proteção de dados e não façam planos só para atender algo que está na LGPD, algo que foi colocado em algum guia de orientação da Autoridade Nacional de Proteção de Dados. Tem que ser entendido que os dados estão sob sua responsabilidade e ele vai responder por qualquer incidente de dados.

Nós vemos extremamente importante o envolvimento da sociedade e do Governo em medidas que dificultem esses incidentes de dados, em medidas mitigadoras. Então, como efetivar? Detectar e identificar rapidamente qualquer atividade de incidente de dados; desenvolver estratégias de investigação e resposta; estabelecer canais de comunicação cada vez mais confiável; fornecer aviso prévio à sociedade e a comunidades afetadas - então, o titular tem que saber que os seus dados tiveram algum tipo de incidente -; fornecer e notificar instituições e comunidades de segurança sobre potenciais problemas; efetivar uma resposta coordenada à atividade. Então são diversas ações que nós vemos como ações que vão minimizar o incidente de dado e vão mitigar riscos.

É importantíssimo que o controlador, que não tinha essa preocupação antes da entrada em vigor da Lei Geral de Proteção de Dados, onde ele sempre queria ter cada vez mais dados para, de alguma forma, comercializar e ganhar dinheiro com este bem preciosíssimo que nós temos hoje que são os dados pessoais... Hoje menos é mais. Então é importante que a empresa, que os setores, que os órgãos tenham apenas aqueles dados que lhes serão necessários. Aquilo que não é necessário deve ser eliminado e não deve ser, inclusive, coletado.

Senador, essa é a mensagem que nós deixamos, esse é o trabalho que a autoridade vem exercendo neste um ano. Esperamos que, no próximo ano, já consigamos alterar a nossa natureza jurídica para uma autarquia independente. Isso nos dará celeridade na nossa atuação, isso nos dará uma forma de aumentar a nossa robustez física para o grande encargo que nós temos do tamanho do Brasil.

Eu lembro que, quando nós olhamos diversas agências de regulação no Brasil, essas agências têm um foco, seja na área de saúde, seja na área de energia, seja na área de educação. A nossa autoridade tem uma visão bastante transversal, uma missão bastante transversal, em que qualquer cidadão, quando sua digital, sua face é recolhida por uma farmácia, por exemplo,

ele já aciona a autoridade se sentindo de uma forma molestado. Então, esse é o nosso trabalho. Nós temos uma estrutura pequena, porém atuante. Temos coletado sempre isso através de pesquisas, através do nosso canal de comunicação, em nossa ouvidoria, no nosso *site*, anpd.gov.br.

E nos colocamos à disposição, Senador, para qualquer questionamento. E os nossos contatos estão já autorizados a serem liberados para receber qualquer tipo de indagação, de questionamento, de sugestão.

Muito obrigado pela oportunidade de a ANPD expor o seu trabalho nessa área tão importante no momento nacional.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Muito obrigado ao Dr. Waldemar Gonçalves Ortunho Junior, que é o Diretor-Presidente da Autoridade Nacional de Proteção de Dados.

Mas, Dr. Ortunho, antes de passarmos a palavra ao nosso técnico, o Sr. Emilio Simoni... É "Simôni" ou Simoni? Aí ele vai nos dizer com clareza qual é a... Eu acredito que é do italiano e deve ser "Simôni", não é? Mas é isso mesmo?

(Intervenção fora do microfone.)

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Então, *grazie mille!* Não errei aqui, não é? *(Risos.)*

Mas eu gostaria que o senhor, Dr. Waldemar, respondesse a uma pergunta lá do Jefferson Venâncio, da Bahia. Ele pergunta assim: "Senador Carlos Viana, eu gostaria de entender o que está acontecendo no País sobre esse assunto. No meu aparelho celular tem ocorrido certa invasão de informações". O que está acontecendo, Dr. Waldemar? O senhor concorda com a Dra. Patrícia? Ela abriu aqui a exposição dela de uma maneira excepcional, dizendo que 2021 é o ano do apagão de dados no Brasil. O senhor concorda com isso? O que está acontecendo? É a pergunta do Jefferson Venâncio, da Bahia.

O SR. WALDEMAR GONÇALVES ORTUNHO JUNIOR (Para expor. *Por videoconferência*.) - Algo que nós temos que trabalhar de uma forma bastante focada é como estão sendo feitos esses compartilhamentos. Se nós olharmos a nossa Lei Geral de Proteção de Dados, hoje o grande diferencial da nossa lei são bases legais. Então, é o que nós temos sempre questionado às empresas: baseado em que você está compartilhando dados. Foi o primeiro caso aí, do WhatsApp e do Facebook, quando eles falaram em compartilhamento. Aí nós fomos buscar qual é a base legal que eles estavam utilizando, se era consentimento, legítimo interesse ou algo do tipo.

Então, na área de telefonia, a própria Anatel já tem algumas novidades, como o Não Me Perturbe, mas, de forma geral, em qualquer compartilhamento de dados o cidadão tem que ter autorizado ou ter, de alguma forma, consciência disso. Aquela parte que nós falamos que é muito importante, Senador, de educação, ela é exatamente para isto: quando o cidadão entra em algum *site* que tem uma palavra "aceitar", ele não busca ainda aquela... o que ele está aceitando. Ele simplesmente, por pressa e comodismo, aceita, e depois ele vai ver que não devia ter aceitado de uma forma tão rápida assim. É essa cultura.

Nós estamos buscando, através desses diversos acordos de cooperação... Lançando cartilhas... Então, com a Senacon já lançamos cartilhas, já lançamos com o NIC.br. Já estamos numa fase... O ano que vem é um ano eleitoral, então, com o TSE, nós firmamos um acordo em que nós estamos produzindo cartilhas, juntamente com o TSE, para partidos, coligações, eleitores, candidatos. Então, acho que é extremamente importante.

E uma outra ação que nós estamos fazendo, por exemplo, é junto ao MEC. Nós entendemos que isso aqui é um problema que acontece cada vez mais cedo na nossa vida. Então, queremos entrar nas escolas, desde os primeiros anos, mostrando ao estudante o risco que ele tem quando ele compartilha, a responsabilidade que ele tem com seus dados pessoais, que é algo extremamente importante, de extremo valor e em que todas as empresas estão de olho e voltadas a isso.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Muito obrigado, Dr. Waldemar.

Eu passo a palavra, então, agora...

Primeiro, quero agradecer também a todas as perguntas que estão chegando aqui, da Elisa Valadão, de Minas Gerais; Lílian Chagas, do Rio de Janeiro; Daniella Carvalho, aqui de Goiás; William Silva, do Distrito Federal. Nós vamos buscar respondê-las após a nossa última participação, e eu convido você que está acompanhando a mandar a sua pergunta pelo www.senado.leg.br/ecidadania - "leg" de Legislativo -ou ligar para o 0800-0612211. A sua participação é importante.

Passo, agora, para a exposição do Emilio Simoni, Executivo-Chefe de Segurança da PSafe, a empresa que, inclusive, denunciou o vazamento de dados dos brasileiros em 220 milhões, pelo menos o que foi divulgado.

Emilio, um bom dia a você.

Eu já abro com uma pergunta que eu gostaria que você incluísse na sua apresentação: tivemos, realmente, o vazamento de 220 milhões de dados de brasileiros, individuais, e estrangeiros? Como isso ocorreu? E, naturalmente, esses dados já foram mapeados, estão sendo usados de alguma maneira?

A sua exposição, por favor.

Muito obrigado, Emilio.

O SR. EMILIO SIMONI (Para expor. *Por videoconferência*.) - Bom dia, Senador. Bom dia a todos.

Queria começar aqui, agradecendo pela oportunidade de falar numa mesa tão bem gabaritada. Todos os companheiros aqui hoje falaram brilhantemente, previamente, de forma que vai ser um grande desafio agora expor alguma informação nova, e parabenizar também pela iniciativa, afinal, tão importante ou mais do que a tecnologia é a conscientização, esse movimento de informar as pessoas.

Com relação aos vazamentos, infelizmente, aconteceu. A PSafe o identificou no início do ano, por um dos nossos sistemas de indexação. A gente monitora 24 horas por dia vários fóruns de cibercriminosos, onde esses dados são comercializados, vendidos. Também monitoramos redes sociais, dados indexados por *sites* de busca, e aí, no início do ano, a gente identificou uma oferta de venda desses dados de 220 milhões de brasileiros, além de dados de veículos, dados de empresas, e um dos nossos pesquisadores que estavam infiltrados nesses fóruns iniciou uma conversa com esse cibercriminoso, passando-se por um possível comprador, para que ele pudesse fornecer amostras do que ele estava alegando que seria vendido. Assim que a gente recebeu essas amostras, a gente verificou a veracidade delas e, de bate-pronto, notificamos a ANPD. Tivemos algumas interações, inclusive, com o Dr. Waldemar e com outros profissionais da ANPD, que atuaram prontamente na investigação.

A partir desse momento, esse caso teve uma grande repercussão, de forma que o cibercriminoso ficou preocupado com as ações da lei em cima disso e acabou se afastando desse cenário de cibercrime e parou de responder nossos pesquisadores, parou de anunciar a venda, mas esses dados foram expostos. Eles forneceram o que a gente chama de *samples*, que são exemplos, amostras do conteúdo vazado, que continham dados completos das pessoas: nome, parentesco, situação financeira, enfim, uma série de informações extremamente graves, porque esses dados podem ser utilizados para outros golpes, de que eu vou falar daqui a pouco numa apresentação, embasando tudo em que esses dados podem ser utilizados.

E tivemos, depois, outros grandes vazamentos, que foram alertados também pela PSafe, e outros em abril, com dados que, supostamente, vieram de operadoras. Esses dados também foram pegos por pessoas infiltradas nesses fóruns de cibercrime.

Agora, mais recentemente, nosso sistema de indexação identificou um *site* na internet onde um cibercriminoso agregou os dados de vários serviços de *streaming* e telefonia numa base única e utilizava isso para consultar por nome, por CPF, por telefone, por endereço e, provavelmente, isso era utilizado num painel de consulta, que é um serviço que o cibercriminoso vende para outros cibercriminosos, em que as pessoas interessadas procuram por pessoas com um perfil específico - ou uma renda alta, ou um grau de instrução, ou eles passam CPF ou nomes para receberem informações completas.

Então, resumindo a minha resposta, infelizmente, sim, houve o vazamento e ele é muito, muito grave.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Emilio, primeiro, seria interessante também nós explicarmos como a PSafe trabalha. Como vocês se organizam nessa questão de proteção de dados, quer dizer, vocês trabalham para as empresas, vocês fazem uma segurança, vamos dizer, privada desses dados do sistema?

Por favor, coloque para a gente entender com clareza qual é o trabalho da empresa.

O SR. EMILIO SIMONI (*Por videoconferência*.) - Certo.

A PSafe é uma empresa nacional, é uma empresa brasileira. Hoje, a PSafe é a proteção *mobile* mais usada no Brasil para celulares Android, IOS. Então, a gente tem uma vertical, que é um produto para pessoa final, é um antivírus gratuito. Qualquer um pode entrar no Google Play, na Apple Store e baixá-lo sem custo nenhum, e ele passa a proteger o seu celular. E a gente tem uma vertical corporativa, pela qual a gente leva tecnologia de ponta para as empresas que querem soluções contra incidentes de cibersegurança.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Sim.

O SR. EMILIO SIMONI (*Por videoconferência*.) - Isso tudo, baseados muito mais no cenário brasileiro e com um valor mais acessível do que empresas estrangeiras, que hoje chegam cobrando em dólar, tornando inacessível para os consumidores nacionais.

O SR. PRESIDENTE(Carlos Viana. PSD - MG) - O.k.

Agora, você nos colocou, então, que o vazamento existiu, mas que quem estava disposto a vender, ao ser denunciado, pelo menos, de que esses vazamentos haviam acontecido e que os dados estariam disponíveis, a partir disso, houve uma retração, não houve a comercialização dos dados. É isso?

O SR. EMILIO SIMONI (*Por videoconferência*.) - Houve a comercialização, eles estavam sendo vendidos há um bom tempo pelo cibercriminoso, pela quantia de US$30 mil à época, e isso ficou sendo ofertado num *site* da *deep web* e, depois, na *web* normal, em que qualquer um poderia ter acesso se a pessoa conhecesse esses fóruns de venda de dados, de cibercrime.

A gente não sabe dizer quantas vendas ele efetivou. A gente sabe que ele teve contato com várias pessoas. E ele nos mandou alguns exemplos de dados, pelos quais foi possível confirmar a veracidade desses dados, mas não foi possível afirmar com certeza qual foi a fonte.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Dr. Waldemar, eu tenho aqui uma pergunta da Ana Cristina, lá de Pernambuco, que diz o seguinte: "Quem vazou os dados de milhões de brasileiros?". *(Pausa.)*

Vamos abrir o áudio, por favor, do Dr. Waldemar. *(Pausa.)*

O.k.

O SR. WALDEMAR GONÇALVES ORTUNHO JÚNIOR (Para expor. *Por videoconferência*.) - Opa! Está aberto.

Nós acionamos, no primeiro momento, a Polícia Federal; pedimos também à PSafe. A Polícia Federal chegou a dois criminosos, um de Uberlândia, outro de Petrolina. Teve uma apreensão de 4TB de dados, que ainda estão sendo periciados.

A nossa ação sempre vai ser no controlador. Então, nós temos que ter... Quem possibilitou esse vazamento?

Sempre, para a ANPD... O nosso poder sempre é na área administrativa, a área penal seria com a Polícia Federal. Então, nós estamos aguardando a conclusão desse inquérito, que pode levar a uma resposta ou não. Nós acreditamos que, pelo volume, esta coleta é resultado de anos e de diversos vazamentos. Então, acreditamos que haverá alguma dificuldade em se obter esses nomes. Mas é um encargo que nós estamos aguardando ser concluído.

O Brasil, eu acho que precisa de um centro de tratamento de dados, um centro que consiga antecipar... A ANPD, como autoridade, vai resguardar o direito do cidadão, mas ela não tem esta missão de impedir o vazamento de dados. É algo que eu afirmo com certeza que sempre vai ocorrer; sempre nós temos que ter ferramentas que mitiguem esses impactos de incidentes de dados, com uma atuação bastante próxima aos diversos setores, com ferramentas cada vez mais úteis. Mas quem vazou os dados? É uma pergunta para a qual nós ainda estamos sem respostas.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Dra. Patrícia, tenho aqui uma pergunta... Na verdade, é uma exposição, um posicionamento da Daniella Carvalho, de Goiás. Ela diz o seguinte: "Esse tipo de ocorrência demonstra a completa ausência de atividade fiscalizadora e eficácia da LGPD".

A senhora concorda, Dra. Patrícia?

A SRA. PATRÍCIA PECK PINHEIRO (Para expor. *Por videoconferência*.) - Olá, Daniella. Obrigada pelo questionamento.

Nós já temos, sim, várias iniciativas de fiscalização da LGPD pela própria ANPD e também pelos convênios realizados pela ANPD com a Senacon e com outros órgãos, não é? Vimos aí a atuação já do Ministério Público e do Idec.

É o suficiente o que já está sendo realizado? Não, não é o suficiente. O Brasil é imenso, não é? E nós temos uma legislação recém-iniciada, vigente, em que foi permitida a aplicação de multas de agosto para cá. Então, o que a gente observa desse contexto todo é que precisamos investir mais para alcançar um nível maior, fiscalizatório, mas existe um passo antes. Vamos fiscalizar, vamos identificar o grau de desconformidade com relação à legislação.

Mas aí eu volto ao ponto que eu já comentei: a política pública para apoiar as instituições para estarem em conformidade. Como vamos conseguir viabilizar também uma atuação de combate a essas quadrilhas? Então, de um lado, é como eu ajudo a implementar o plano de conformidade a partir da identificação, na fiscalização, dos *gaps*, o que está faltando, e, do outro, é também como vamos atrás efetivamente dessas quadrilhas para que elas não sintam que está tão fácil assim, atacar e cair no mato e sumir, e depois nada acontece, que é essa necessidade de identificação desses infratores, provavelmente com uma força especial, uma força-tarefa criada, dedicada, com foco de atenção e com um orçamento apropriado para tanto.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Obrigado, Dra. Patrícia.

Emilio, você tem uma apresentação numa sequência, não é isso? Eu pergunto se gostaria de continuar, por favor, a exposição.

O SR. EMILIO SIMONI (*Por videoconferência*.) - Gostaria. Vou compartilhar a minha tela aqui.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Pois não, perfeitamente.

O SR. EMILIO SIMONI (*Por videoconferência*.) - Todos estão vendo minha tela?

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Sim.

O SR. EMILIO SIMONI (Para expor. *Por videoconferência*.) - Certo.

Então vou focar um pouco nesses últimos dois anos, que foi um período em que, junto com a pandemia que nós tivemos, veio a ciberpandemia, que foi um crescimento muito grande, desproporcional de ciberataques, em parte pelos cibercriminosos brasileiros serem muito oportunistas e aproveitarem o momento; por outro lado, as pessoas sendo forçadas a trabalhar em *home office*, onde, muitas vezes, elas não têm o mesmo nível de proteção que elas teriam na sua empresa, não têm a proteção de perímetro equivalente à que elas teriam no seu trabalho no dia a dia.

Vou falar um pouco de algumas notícias do tema, que já foi muito bem abordado pelos companheiros que falaram previamente. Então vou passar rapidamente.

A PSafe, através da sua indexação, identificou este ano três grandes megavazamentos. O primeiro deles foi em janeiro, em um fórum de cibercriminosos, onde foi anunciada a venda de uma base com dados de 223 milhões de brasileiros, 40 milhões de CNPJs, além de informações de veículos. Um mês depois, um dos nossos perfis infiltrados identificou um outro cibercriminoso vendendo dados que supostamente eram de operadoras de telefonia, duas operadoras de telefonia, que também continham dados pessoais, dados de endereço, perfil de telefone, perfil de conta, dados de contato. E agora, há menos tempo, nosso sistema identificou um *site* na internet, também através da indexação contínua, um *site* que permitia consultar nome, telefone, CPF, endereço. E por trás desse *site*, a gente identificou que havia uma base de dados da maioria das operadoras brasileiras - pelo menos o nome das bases era o nome das operadoras - e de duas empresas de *streaming* de TV, de forma que retornavam dados extremamente ricos em informação.

Fora essa questão, a gente percebeu que os cibercriminosos vêm criando bases enriquecidas que não são de uma única fonte. Eles vêm cada vez mais acumulando informações dos brasileiros e vendendo isso através de painéis de consulta, que são serviços do cibercrime, em que eles vendem consulta como se fosse, por exemplo, uma consulta de crédito de uma empresa, que é vendido hoje. Eles vendem consultas informativas, em que eles recebem o nome de uma pessoa, um CPF, ou um telefone, ou um perfil socioeconômico, e eles retornam essas informações para a pessoa que quer consultar.

O movimento que a nossa área de inteligência percebeu aqui na PSafe é que muitos vazamentos não vêm de hoje, eles vêm de dois, três anos atrás. E o cibercriminoso, percebendo que ia entrar em vigor a legislação com multas com relação ao vazamento de dados, a incidentes, ficou guardando esses dados vazados que eles conseguiram em anos anteriores para este ano, com a lei entrando em vigor e ele tendo um poder de barganha muito maior com relação à extorsão das empresas. Então, eles contactavam empresas, mostravam que estavam de posse desses dados que foram obtidos recentemente, ou então algum tempo atrás, solicitando o pagamento de valores altíssimos para que esses dados não fossem divulgados, não fossem vendidos ou divulgados de forma gratuita, gerando, assim, prejuízo para a empresa. Isso apareceu muito forte este ano, mas os dados já são acumulados há pelo menos dois anos.

Falando de vazamento de dados de forma mais geral, como foi exposto previamente, isso não é algo específico do Brasil; isso é uma crise mundial de vazamento de dados. Está havendo uma atividade muito grande de cibercriminosos.

Hoje a gente sabe que os dados são o novo petróleo, são o novo ouro, porque os dados têm um valor intrínseco muito grande. E de onde é que vem esse valor? Hoje, de posse dos seus dados pessoais, o cibercriminoso pode pegar um empréstimo no seu nome, pode abrir uma conta digital, pode tentar clonar o seu WhatsApp e se passar por você. Imagina ele instalar um número de WhatsApp com a sua foto, um número novo. Ele sabe quem são seus parentes, então ele cadastra um parente seu e contacta-o falando que é você. Ele vai provar que é você, falando coisas que normalmente só você saberia, como seu endereço, quem são seus parentes, onde ele está, e aí vai simular uma situação de emergência, pedindo pagamento de conta ou empréstimo. Então esses dados, essa abundância de dados é um prato cheio para o cibercriminoso aplicar golpes.

A PSafe vem indexando esses dados que são ofertados por cibercriminosos ou são disponibilizados em fóruns de criminosos, redes sociais, em várias fontes da internet já há alguns anos. Quando a gente pega algo em que a gente consegue identificar a fonte, em que há alguns indícios, a gente contacta a ANPD para informar o que foi identificado. A gente também contacta as pessoas impactadas, as empresas impactadas, quando a gente tem um indício de qual é a fonte, um indício seguro da fonte para dizer.

E depois, quando a gente vê que esse vazamento está impactando a população brasileira de forma geral, a gente acaba criando um relatório de impacto e fornecendo esse relatório para que os veículos possam conscientizar a população. É daí que vêm essas notícias falando de vazamento de 220 milhões, vazamento de 110 milhões. O mais recente tinha dados de mais de uma fonte, do mesmo CPF, chegando a 400 milhões de informações.

Quando a gente fala de dados indexados pela PSafe hoje, é a maior base mundial de dados indexados de vazamento de dados, que seriam um *e-mail* e algo anexado a esse *e-mail*, ou uma senha, ou um *hash* de senha, ou outros dados de localizações que podem estar atrelados a esse *e-mail*, sendo que, desses dados todos, mais de 1 bilhão são de empresas ou população brasileira, são dados que têm um domínio .br atrelado a eles. Então, esse é um impacto que afeta diretamente a população brasileira.

Quando a gente fala em prejuízo, quando a gente mapeia um pouco mais os ataques, aqui no Brasil, além de haver uma diversidade e uma quantidade de ataques muito grande, o que torna o nosso combate ao cibercrime um grande desafio é que o brasileiro tem uma criatividade excepcional, e assim como isso é utilizado para o bem, isso acaba sendo também utilizado para o mal. Então, a gente tem roubos de identidade, a gente tem ataques de *ransomware*, que geraram, nos últimos anos, mais de US$6 trilhões de prejuízo, o que é maior do que o PIB de muitos países hoje.

Ataques direcionados a empresa brasileira cresceram 60% no último ano. Baseado nas empresas que acessaram nosso sistema de consulta de dados vazados, a gente sabe que quatro em cada cinco empresas que checaram por dados vazados, infelizmente, tiveram dados vazados. Isso não quer dizer que a empresa em si teve uma vulnerabilidade. Muitas vezes, o colaborador utiliza o *e-mail* corporativo para se registrar em serviços de terceiros, e acaba que esse serviço de terceiro é comprometido, e a mesma senha que ele utilizou ali é a mesma senha que ele usa na VPN, no *webmail*. Então, o reaproveitamento de senha é um grande problema hoje que a gente enfrenta, e isso acaba abrindo brecha para o cibercriminoso.

A gente já teve previamente citados os casos que envolveram o Governo esta semana, em que a quadrilha responsável pela invasão comentou que foram utilizados usuários e senhas expostos na internet. Então, é realmente importante esse monitoramento, essa conscientização, saber o que foi vazado, o que está ativamente funcionando, logando na "infra" das empresas, para que possam ser tomadas medidas como alteração de senha, utilização de segundo fator de autenticação, que é algo extremamente importante.

Falando um pouco mais da diversidade de golpes, a gente tem o tratamento de dados, a engenharia social, que abarca muitos ataques, ataques de *malware*, espionagem industrial, *call center* falso, que é um golpe que nasceu no Brasil, assim como clonagem de WhatsApp, que nasceu no Brasil também e é um golpe muito focado no Brasil. Há sequestro de mídias sociais, chantagens, ataque de "sextorção", que é um golpe muito covarde, é um golpe que tem um peso muito grande na vítima, assim como perfis falsos, que criam uma dependência sentimental na vítima, golpes de falsa vaga de emprego; são golpes extremamente perversos. Golpes focados em IOT vão crescer de forma exponencial no ano que vem, com o advento do 5G, assim como outros golpes em cima de cartão de crédito, etc.

E os golpes, quando a gente fala de Brasil, têm muitos canais. Ao contrário do que a gente vê fora do Brasil, em que os golpes chegam via *e-mail*, via SMS, aqui, no Brasil, a gente também tem uma diversidade. E é muito comum, aqui, no Brasil, os roubos e golpes virem via redes sociais.

O cibercriminoso sabe qual é o perfil de vítima que tem maior propensão a cair no golpe. Então, ele não vai mandar um golpe para alguém que trabalhe com TI, por exemplo. Ele vai numa rede social, ele cria um perfil falso, ele utiliza mecanismos de propaganda incentivada para levar o golpe a pessoas que ele sabe que vão cair. Aí você pode customizar qual é o público alvo da sua propaganda. Na verdade, essa propaganda é um *site* falso de banco, é uma falsa premiação, é um *site* falso de *e-commerce*, principalmente na época de *black friday*. Este ano, por exemplo, a gente teve um crescimento de mais de 10% no número de golpes se comparados à *black friday* do ano anterior, que já teve também um crescimento muito grande.

Se eu pudesse aqui falar de algumas dicas rápidas, seria: não existe jantar gratuito. Desconfie do que chega prometendo algo que é bom demais para ser verdade: um celular que custa R$5 mil numa loja, chegou um *link* prometendo por R $500; uma televisão de 60 polegadas chegando por R$500; ou fala para você compartilhar com dez amigos que você vai receber gratuito.

Isto também é algo interessante, que nasceu no Brasil, em 2016: o cibercriminoso utilizar a vítima como vetor de disseminação de golpe. Então, chega um golpe para a vítima via rede social ou via aplicativo de mensagem ou *link* falando para vítima: você vai ganhar uma TV, uma vaga de emprego, mas, para isso, você tem que mandar esse *link* para 10 pessoas ou para 5 grupos, etc. Então, você imagina como esse golpe cresce: eles mandam esse golpe, inicialmente, para 10 pessoas, que passam para 100, que passam para 10 mil, 100 mil. Daí que surgem esses números que muitas vezes a PSafe fala na mídia: golpe de vaga de emprego, houve 300 mil bloqueios; golpe envolvendo *black friday*, com 100 mil bloqueios.

Ano passado, a gente teve um golpe recorde, que foram golpes que prometiam a liberação do auxílio emergencial. Foram golpes oportunistas, aproveitando o momento do brasileiro, em abril, em março, que chegaram a 20 milhões de bloqueios. É um número assustador. É um tipo de golpe que chegava para as vítimas prometendo liberar o auxílio emergencial, sendo

que o Brasil já estava em crise naquele momento com relação a muitas pessoas em situação de vulnerabilidade. A pessoa, achando que iria liberar o auxílio emergencial, pegava aquele *link* malicioso e mandava para 10 pessoas, colocava seus dados pessoais como CPF, endereço, parentesco, etc. Então, acabava ainda caindo em outros golpes, e, no final, a gente teve golpes com números estratosféricos, chegando a 20 milhões de bloqueios.

Falando um pouco mais deste ano, o que a gente tem hoje é a ciberpandemia de *ransomware*. São ataques de *ransomware* acontecendo cada vez mais. Por que esses ataques de *ransomware* têm crescido tanto? Um dos fortes motivos foi porque as quadrilhas que desenvolvem *ransomware* perceberam que existe um modelo de negócio muito mais lucrativo. Então, eles fizeram o que a gente chama *business plan*, fizeram um grande negócio que é o de *ransomware as a service*.

Até dois anos atrás, o desenvolvedor do *ransomware* se preocupava em espalhar aquela ameaça, mandava para a vítima, mandava via *e-mail*. Hoje, ele tem um sistema de afiliado. Então, o programador, a equipe de pesquisa que cria o *ransomware* não se preocupa mais em distribuir o *ransomware*.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Emilio...

O SR. EMILIO SIMONI (*Por videoconferência*.) - Sim?

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Vou interrompê-lo só um instantinho.

Para quem não é da área, quem não acompanha, eu gostaria que você dissesse o que é um *ransomware*. Do que é que nós estamos falando? Porque os que são da tecnologia da informação conhecem bem, mas nós temos, acompanhando agora, muitas pessoas que não têm uma noção, que querem apenas entender como se proteger.

Poderia explicar por favor?

O SR. EMILIO SIMONI (*Por videoconferência*.) - Muito bem colocado, Senador. Obrigado pelo aviso.

Ransomwares são tipos de golpes que, quando eles infectam um computador ou um celular ou uma empresa, eles vão roubar todos os dados ali disponíveis. Quando a gente fala de pessoas, eles roubam fotos, roubam mensagens e bloqueiam o acesso ao conteúdo original. Eles apagam ou eles colocam uma senha de acesso. Quando a gente fala de computadores em empresas, eles roubam documentos, também roubam banco de dados e apagam tudo o que está disponível ali. Apagam o banco de dados, apagam os arquivos, apagam *backups*, de forma que eles passam a solicitar o pagamento de resgate para devolverem esses dados, além de existir também o que a gente chama de *double extortion*, que é uma extorsão dupla. Como muitas empresas hoje têm uma cópia *offline*, que é uma cópia que não está na rede, acontece de cibercriminosos não terem sucesso na extorsão inicial, que seria para devolver os dados. Então, eles passam a cobrar também para que esses dados não sejam expostos na internet.

É por isso que a gente vê, às vezes, na notícia, "grupo de *ransomware* expõe dados da empresa X e da empresa Y no seu *site*, na *dark web* ou *deep web"*, porque a empresa ou pagou e teve os arquivos devolvidos, mas também vai estar suscetível à extorsão dupla, ou ela não pagou, porque tinha um *backup*, e, nesse caso, o cibercriminoso vai cobrar o resgate para não expor na internet. Caso ela não pague, esse arquivo vai ser disponibilizado na internet para qualquer um que conheça o *site* do cibercriminoso, o *site* do grupo de *ransomware*, e possa baixar.

Então, todos os dados confidenciais da empresa ou das pessoas vão ser bloqueados, vão ser roubados. Eles são exfiltrados, o que quer dizer que eles são tirados dos computadores, dos bancos de dados, dos celulares, e estão de posse do cibercriminoso, além de serem apagados. Então, é isso que o *ransomware* faz. Eles são programas especializados em roubar os seus dados e bloquear o acesso aos seus dados, de forma que você só vai tê-los de volta ou não expostos na internet se você pagar um resgate, que normalmente é muito alto, quando a gente fala de empresas, ou tem valores mais baixos, quando a gente fala de indivíduo.

Falando um pouco de números que envolvem ataques de *ransomware* em especial. A gente tem uma estimativa de danos, este ano, de US$20 bilhões de ataques específicos de *ransomware*. Acontece um ataque de *ransomware* novo, no mundo, a cada 11 segundos. Este ano, o número de ataques praticamente dobrou com relação a 2020.

Quando a gente fala de pedidos de resgate que vieram a público, o maior deles até o momento foi de 11 milhões, noticiado pelo Grupo JBS, pagos para devolver ou acertar os seus dados e pela não divulgação dos dados. Até o momento, a gente tem o número de 3,8 milhões de ataques somente no Brasil. O Brasil é o segundo país hoje mais atacado por *ransomwares*, perdendo somente para os Estados Unidos. Isso é um número extremamente preocupante porque, por outro lado, a gente tem um outro estudo, que a gente não abordou aqui, que diz que o Brasil está entre um dos últimos colocados quando a gente fala em resiliência ao ataque de *ransomware* e em identificar o ataque de *ransomware*.

Então acontece que, no Brasil, pode demorar semanas até a empresa identificar que a rede dela está sendo tomada por um grupo de cibercriminoso. Também acontece muito de o cibercriminoso, quando percebe que a vítima é uma empresa de grande porte, que tem muitos dados, não efetuar a destruição dos dados nesse primeiro momento. Ele pode passar até

meses estudando a arquitetura da empresa. Ele pode utilizar, inclusive, inteligência artificial para calcular o valor ótimo de resgate, baseado no lucro da empresa, no tamanho da empresa, na quantidade de dados, até que ele chegue à etapa final de destruição de dados.

Como é esse ciclo de vida de um *ransomware*? Primeiro, identificar a vítima, achar a vítima, infectar a vítima, identificar o ambiente, identificar soluções de proteção, desativar soluções de proteção, fazer movimento lateral, que é basicamente identificar computadores na rede, bancos de dados na rede e infectar também esses outros computadores, até que, no final, haja efetivamente a destruição dos dados e o roubo dos dados que são feitos previamente nessas etapas anteriores. Então, quando os dados são destruídos, o cibercriminoso está de posse de todos os dados da empresa.

Vou falar um pouco do valor médio de resgate. Há um valor médio de US$570 mil para empresas.

Como funciona o ciberataque de *ransomware*? Eu falei agora há pouco do ciclo de vida do *ransomware*, em que se faz a infecção, o reconhecimento do ambiente, a desativação das defesas, a infecção de outros computadores que estão naquela mesma rede, a destruição de banco de dados, a identificação de banco de dados, a exfiltração de dados, até efetivamente destruir todos os dados ali disponíveis e exibir a cobrança do resgate. Até pouco tempo, era muito comum que *ransomwares* chegassem por *e-mails*, em que se passavam por atualização de sistema, instalação de *plug-in* de Flash - a temática mais comum. A gente via muito o golpe "príncipe da Nigéria", que também é bem famoso. Mas a gente tem agora uma diversificação. Além de vir por *e-mails*, os cibercriminosos estão se aproveitando dessa abundância de dados vazados e do reaproveitamento de senhas. Então, é muito comum eles simplesmente identificarem infraestruturas abertas na internet, com acesso remoto, como *softwares* utilizados por empresas para suporte ou para TI. Eles logam no sistema e não quebram nada. Simplesmente pegam uma senha vazada, logam no sistema da empresa e passam a operar remotamente o sistema da empresa, instalar o *ransomware* ali, identificar o ambiente e fazer todo tipo de ataque.

Também acontece de eles explorarem vulnerabilidades. Houve grandes vulnerabilidades expostas na internet recentemente. Na semana passada, houve o caso do sistema de *log* da Apache, que permitiu aos criminosos efetuarem comandos remotamente. Então, eles exploram a vulnerabilidade de sistemas não atualizados e infectam o sistema com *ransomware*. Houve também casos de aliciamento de pessoas de dentro das empresas - é o que a gente chama de *insider*. Eles contactam funcionários que eles mapearam previamente e que têm acesso privilegiado, oferecendo grandes quantias em dinheiro - às vezes, 20%, 40% e até metade do valor pago do resgate. Então, se um resgate vai chegar a cobrar US $2 milhões, US$3 milhões, eles oferecem para o aliciado US$1 milhão, US$2 milhões. Então, é um poder de persuasão muito forte. Eles vão cobrar que o aliciado execute o *ransomware* dentro da empresa, desative barreiras de proteção. E todas as combinações acabam gerando um impacto muito grande.

Falando de senhas, o Marco DeMello, que é o CEO da PSafe, tem falado que as senhas são o câncer da internet - esse é o grande problema que a gente tem hoje.

Quando a gente fala em autenticação, há três pilares: "o que você sabe", "o que você é" ou "o que você tem", sendo que "o que você sabe" é o pilar mais fraco, pois basta um ataque de engenharia social, que é um ataque em que a pessoa engana você, fazendo você colocar a senha em um *site* que não é o verdadeiro, para a pessoa acessar o sistema se passando por você ou, então, para pegar um dado vazado em que há uma senha sua. Essa senha é reaproveitada numa VPN, que é um sistema de acesso remoto a uma empresa, num *e-mail*, e a pessoa consegue acessar. O pilar "o que você tem" já é um pouco mais forte, porque, muitas vezes, é uma autenticação de dois fatores: um celular ou um dispositivo fixo que você conecta. E o pilar "o que você é", que é uma das formas mais seguras que a gente tem hoje, que é o reconhecimento facial, o reconhecimento de voz, o reconhecimento biométrico.

Então, algo que a PSafe tem falado é que as senhas têm que ser extintas, têm que ser trocadas pelo que você é, que é a sua biometria, a sua face, ou a sua voz.

E, falando de senha, a gente pode ver aqui que as senhas mais comuns dos últimos dois anos são extremamente fáceis de serem deduzidas. São quebradas por *brute force*, em alguns minutos, como a 123456, que foi, novamente, este ano, a senha mais utilizada. A 123mudar; a teste123; Flamengo... A gente vê que tem bastante flamenguista participando. Então é algo extremamente preocupante.

E é isso. É uma temática bastante abrangente. A gente tem uma diversidade de muitos golpes no Brasil, o que torna realmente um grande desafio falar dessa temática.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Muito obrigado, Emilio.

Tem uma das senhas aí, a Flamengo, este ano ela ficou muito fraca mesmo. *(Risos.)*

É verdade. É uma senha que este ano não ajudou muito a maior torcida organizada do Brasil.

Obrigado, Emilio.

Vamos partir aqui para as perguntas e as colocações.

Por exemplo, a Raíssa Siqueira, do Rio de Janeiro: "Quais as iniciativas para que esses números diminuam? Afinal, isso traz prejuízo para milhões de brasileiros".

O Marcos Ribetti, do Espírito Santo: "[...] o que precisa mudar e/ou permanecer para estimular e disseminar a cultura de proteção de dados no País?".

William Silva: "Com um vazamento dessa magnitude, o que a população deve esperar dos órgãos responsáveis? Há algum perigo de esse vazamento ocorrer novamente?".

Então eu vou compilar essas perguntas aqui, Dra. Patrícia e Dr. Waldemar, no seguinte sentido: quanto à legislação, hoje, o que nós aqui, Congressistas, podemos propor como mudanças, como avanços? Quais são os pontos que a OAB de São Paulo entende que nós precisamos avançar e também, Dr. Waldemar, quais os pontos que nós precisamos trabalhar para garantir mais segurança?

E depois nós vamos abrir para discutir também a questão das punições. A legislação brasileira hoje já prevê punições para o caso, por exemplo, do *ransomware*, desses crimes cibernéticos? Ela é específica, ou nós precisamos modificar a tipificação penal para que a gente possa punir realmente quem agir de má-fé com isso?

Então, a primeira colocação em torno das perguntas, Dra. Patrícia: a legislação brasileira atende, para que a gente possa dizer que estamos caminhando num sentido de mais segurança?

A SRA. PATRÍCIA PECK PINHEIRO (Para expor. *Por videoconferência*.) - Bem, Senador, primeiro, acredito que a gente deu o primeiro passo, o da legislação, e ela foi muito bem feita e orientada, como bem colocado também pelo Dr. Carlos Bruno, com referências internacionais. Nós nos inspiramos no Regulamento Geral sobre a Proteção de Dados europeu. Mas nós temos que pensar no contexto Brasil. Nós temos um cenário desafiador aqui, e acredito, sim, que há espaço para melhorias na nossa legislação. De que maneira? Nós vamos iniciar um ciclo de fiscalização e a possibilidade de aplicação de multa. Quando previmos, na nossa legislação, para onde vai o recurso dessa multa, que está previsto ir para o Fundo de Direitos Difusos, o FDD, de certo modo, a gente tem uma autoridade hoje, a ANPD, que vai precisar de recurso e de orçamento, para ter um porte e uma capacidade de atuação em nível Brasil.

Hoje, se você olhar, em efetivo de pessoas e de estrutura, nós ainda precisamos de muito mais, até se a gente comparar com outros países, como acontece com a autoridade nacional de proteção de dados do Reino Unido, o chamado ICO, que tem uma equipe muito maior e tem mais atuação. Então, talvez um olhar de como poderíamos viabilizar o alcance de recursos, quer seja aquilo que venha de destinação da multa ou aplicação de taxas. São sugestões que acontecem em outros países e que não chegamos a esse ponto aqui de previsão da nossa legislação.

Rapidamente, uma outra frente que foi comentada é no sentido do combate efetivo na parte criminal. Nós chegamos, em 2021, a ter a Lei 14.155, para tentar melhorar a aplicação de penalidades na fraude eletrônica, no estelionato digital, aumentando a aplicação de pena e até viabilizando um pouco mais a questão investigatória. Entendo que o mesmo deveria ser feito no sentido de uma tipificação específica relacionada ao sequestro de dados e uma pena específica mais elevada. Isso, de fato, nós não temos. Se a gente olhar os crimes relacionados a dados pessoais, isso não está previsto. A Lei de Proteção de Dados Pessoais não trouxe uma parte criminal. Isso depende, sim, da atualização do nosso Código Penal, e que a gente eleve esse tipo de crime para uma pena mais elevada. Então, acho que há espaço, sim, de atuação, de colaboração aqui da Casa Legislativa para a gente evoluir nesse sentido.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Muito obrigado, Dra. Patrícia.

Dr. Waldemar, na sua opinião, a legislação precisa avançar em quais pontos para garantirmos ou pelo menos caminharmos com mais segurança, uma vez que, pelo que os senhores todos colocaram, a questão dos vazamentos é um problema que nós vamos ter que conviver com ele. Mas como vamos fazer para pelo menos minimizar, Dr. Waldemar?

O SR. WALDEMAR GONÇALVES ORTUNHO JÚNIOR (Para expor. *Por videoconferência*.) - Eu vejo de uma forma, vamos dizer, a fiscalização é importantíssima, ela tem que ser uma fiscalização responsiva. Nós temos visto, pela nossa ouvidoria, quais são os pontos que oferecem mais riscos para desencadear os nossos planos de fiscalização.

Acho importante deixar claro que a lei é muito moderna, a nossa lei prevê praticamente os pontos que devem ser focados. Nós necessitamos dar o tempo que a ANPD necessita de maturidade, ou seja, de traçar essas normas e de iniciar realmente esse processo investigativo para colher resultados. Nós vemos como importantíssima a parte de educação para os diversos setores, para o titular de dados. Nós vimos, na apresentação da PSafe, que muitas vezes são senhas extremamente fáceis. Então, há uma necessidade da governança das empresas, do sistema de governança em trabalhar em senhas mais fortes, dupla autenticação. São medidas que vão minimizar bastante esses vazamentos. A responsabilidade sobre o controlador de dados é importante. Então, nós vemos que, de uma forma positiva, a nossa atuação vai reduzir esses vazamentos de

dados, incidentes de dados de forma geral, mas há a necessidade de o coletivo trabalhar de uma forma conjunta. Não vão ser com Senacon, ANPD, Ministério Público, Polícia Federal trabalhando de forma isolada que nós vamos obter um resultado melhor, mais efetivo; há uma necessidade de se formar rede.

Posso citar, por exemplo, o Ministério da Defesa. Ele tem um exercício anual guardião em que diversos setores são acionados a treinamentos na área de energia, na área de telecomunicações, na área de sistema financeiro, na área nuclear em que se simulam ataques, e as empresas passam a ter as suas respostas como um treinamento. Então, esse nosso treinamento e essa nossa capacitação a uma pronta resposta são bastante importantes, e, é claro, a empresa tem que investir em segurança. Ela tem de analisar os dados que ela tem, quais são os riscos que esses dados oferecem aos seus titulares e trabalhar de uma forma anterior a ter um ataque, para proteger de uma forma mais eficaz esses dados com as diversas ferramentas que a tecnologia, o desenvolvimento tecnológico nos traz no momento atual.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Dr. Waldemar, eu acredito que o senhor tenha respondido assim até já à pergunta do Josué Rodrigues, lá do Rio Grande do Sul, que era: "Como criar mecanismos de proteção de dados ao ponto de que cada vez mais a sociedade seja incentivada a viver de forma digital?'"

O senhor está colocando - e até o Emilio colocou também - que um dos primeiros pontos é a própria defesa. A pessoa que vai ter os dados disponibilizados para empresas de telefonia, de cartão de crédito ter senhas fortes e ficar atenta à questão de movimentos diferentes do que normalmente ela coloca.

Obrigado, Josué.

Agora, Dr. Waldemar, seguindo aqui, eu tenho a pergunta da Elisa Valadão, lá de Minas Gerais, que diz o seguinte: "A fiscalização da ANPD junto aos órgãos e entidades públicas acontecerá sob demanda, ou seja, a partir de denúncias?"

O SR. WALDEMAR GONÇALVES ORTUNHO JÚNIOR (*Por videoconferência*.) - Nós já temos feito sob demandas, sob denúncias, mas também nós passamos a monitorar os diversos setores. Vamos ver de uma forma bem objetiva: 50 colaboradores não seriam suficientes para nós fiscalizarmos todas as empresas do nosso País. Então, é um fator em que nós já estamos atuando.

Começamos a receber diversas denúncias, diversos questionamentos de farmácias. Pronto, já reunimos a nossa equipe tecnológica, que passou a trabalhar com as associações ligadas ao setor de farmácia, e começamos a já prevenir para, no próximo ano, já como nosso foco, atuar neste setor.

Então, nós trabalhamos onde há o maior risco de danos ao titular ou o maior risco que possa ocasionar em diversos setores. Então, é dessa forma que nós estamos trabalhando e, claro, atendemos as diversas denúncias que chegam ao nosso canal de comunicação.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Emilio, há aqui uma pergunta do Erick Faria, também mineiro: "Devemos criar uma autenticação para o uso do CPF, como OTP. Os dados já foram vazados e continuarão sendo. Devemos pensar na segurança!".

Primeiro, eu gostaria que você, se puder, explicasse o que é OTP e se, de fato, nós poderíamos criar códigos extras para garantir mais segurança na utilização do CPF. Qual é a sua opinião?

O SR. EMILIO SIMONI (Para expor. *Por videoconferência*.) - OTP vem do inglês *one-time password*. A ideia é que exista uma senha que só possa ser utilizada uma vez, e, depois, essa senha é invalidada. É uma opção melhor do que só possuir uma senha de algo que você sabe, mas, na verdade, qualquer forma de autenticação complementar vai sempre estar ajudando.

Então, a tecnologia sempre tem um balanço de acessibilidade com a parte de dificuldade de acesso. Você tem que disponibilizar os dados, mas tem que garantir que tenha segurança nesse acesso.

Então, o OTP, sim, é válido, assim como qualquer outro segundo fator de identificação, como a biometria.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Ele teria que ser, por exemplo, obrigatório por lei? Nós poderíamos propor que as empresas que recebem, guardam, armazenam esses dados e, naturalmente, façam transações com eles, sejam financeiras, comerciais... Teria que existir uma lei obrigando a criação desse protocolo ou as empresas por si sós poderiam adotar o OTP?

O SR. EMILIO SIMONI (*Por videoconferência*.) - Não só o OTP. Seria algo muito interessante que empresas que trabalham com dados confidenciais, dados sensíveis fossem incentivadas a que todo mundo que tenha acesso a esses dados tenha um fator de autenticação mais robusto, não somente uma senha, mas também um reconhecimento facial ou

biométrico, uma senha de acesso, quaisquer outros mecanismos que não se baseiem somente em um pilar que seria algo que você sabe, como é a senha hoje.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Vocês acham, Dr. Waldemar e Dra. Patrícia - vou abrir o áudio aqui para que possam comentar, por favor -, que nós precisaríamos de uma legislação específica, por exemplo, criando novos mecanismos de autenticação?

O que a senhora acha, Dra. Patrícia?

A SRA. PATRÍCIA PECK PINHEIRO (Para expor. *Por videoconferência*.) - Nós temos já hoje, em termos de legislação, previsão de tipos de assinatura, que permitem a utilização de métodos de autenticação dessa natureza, desde quando criamos a MP 2.200. Então, talvez aqui seria muito mais no campo de se observar aquela discussão da identidade única, centralizando isso, mas acredito que a legislação já nos contempla o esforço necessário para permitir que o uso de senhas dessa maneira já seja viável. Não enxergo que haja necessidade de legislação para permitir métodos novos de autenticação. Já se pode usar a senha, já se pode usar a biometria como segundo fator de autenticação, mas aqui o ponto é - e é algo que o Brasil já vem discutindo há bastante tempo - uma identidade digital única, forte para o brasileiro. Acho que vale o grupo de trabalho se dedicando mais nesse sentido.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Dr. Waldemar, qual é a opinião do senhor? A doutora colocou que a legislação já permite, mas, ou seja, não temos uma obrigatoriedade, cada um pode escolher o seu sistema. Precisaríamos criar legalmente um instrumento que obrigasse, por exemplo, uma segunda forma de autenticação além da senha? *(Pausa.)*

O áudio, por favor, Dr. Waldemar.

O SR. WALDEMAR GONÇALVES ORTUNHO JÚNIOR (Para expor. *Por videoconferência*.) - Consegui agora!

Eu acho que o mercado vai regular isso, Senador. As melhores senhas são aquelas nossas próprias - biometria, reconhecimento facial -, sem dúvida nenhuma.

Eu tenho experiência de locais em que se colocou uma política de senha extremamente segura, mas com mudanças, vamos dizer, quinzenais. E hoje cada um tem uma de série de senhas em suas cabeças. Chegou a um ponto que era só levantar o teclado que você tinha o *login* e senha, fruto da grande dificuldade que se causava ao usuário. Então, eu acho que o próprio mercado vai se encarregar disso em função dos riscos quando qualquer acesso indevido ocorra. Então, acho que não deveríamos interferir neste momento. Acho que a legislação já descreve todos esses processos de uma forma bastante completa.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Agora, Dr. Waldemar, a Lilian Chagas, do Rio de Janeiro, pergunta aqui: "Como será a responsabilização no caso de incidentes de vazamento de dados pessoais ocorridos em organizações públicas?".

A questão é a seguinte: essas empresas que têm os dados vazados estão sendo multadas no Brasil - como o Procurador Dr. Carlos colocou no início, "o Estado brasileiro exigindo responsabilidade daqueles que detêm os nossos dados" -, elas estão sendo punidas, Dr. Waldemar?

O SR. WALDEMAR GONÇALVES ORTUNHO JUNIOR (*Por videoconferência*.) - A punição inicia até mesmo com a advertência. Nós vemos que aquela punição que vai para a manchete de jornais, normalmente, são as pecuniárias. Essas são as menos relevantes para a empresa. É claro que uma empresa não quer ser punida no seu bolso, mas, se nós olharmos, isso não volta para o titular de dados, vamos dizer, normalmente isso daí pode ir para outros setores. Nós vemos que são protelados sempre esses pagamentos através de recursos. E nós vemos que a reputação de uma empresa é o que ela tem de melhor, que leva anos para construir e pode ser desconstruída de uma forma bastante rápida. A punição mais séria seria a suspensão do tratamento de dados ou a extinção dos bancos de dados.

E o setor público tem não só a ANPD, mas tem outros órgãos trabalhando em cima disso, como CGU, TCU, não tem a parte pecuniária, mas têm sido bastante acionadas as empresas que têm algum incidente de dados como compartilhamento ou vazamento de dados.

Eu só lembro que nós temos um processo até a punição. Nós temos que ter certeza do que aconteceu. Não basta uma notícia em jornal, em televisão para nós já prejulgarmos. Então, nós temos esse cuidado. Nós estamos neste processo em conjunto com outros órgãos, como Polícia Federal, Ministério Público, que podemos citar aqui no momento.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - A Dra. Patrícia citou a questão da criação até de uma força-tarefa, por exemplo, contra ciberterrorismo. Isso já está previsto, Dr. Waldemar, Dra. Patrícia, se a senhora quiser comentar mais? Mas eu achei interessante porque estamos falando de vazamento de dados pessoais, mas temos que pensar também na questão da segurança de dados essenciais, na segurança do País, de defesa. Essa força-tarefa já está prevista na legislação?

A SRA. PATRÍCIA PECK PINHEIRO (Para expor. *Por videoconferência*.) - Olá, Senador.

Eu não tenho conhecimento dessa previsão para a construção da força-tarefa. Entendo que seria oportuno esse tipo de encaminhamento. Isso poderia estar, inclusive, fazendo parte da continuidade de previsão da política de segurança cibernética, Política Nacional de Segurança Cibernética. Acho que é importante que a gente possa enxergar a necessidade da construção da força-tarefa. Isso já ocorre em outros países. A gente já teve a oportunidade de fazer alguma referência ao *benchmarking*.

E eu queria aproveitar para fazer um complemento à minha fala anterior, porque, assim, hoje todo brasileiro tem a sua iniciação de vida digital, muito utilizando dispositivos de mobilidade, especialmente os celulares. A gente está indo aí para o 5G. Assim como quando a gente pensa em indústria automobilística, que a segurança vem de fábrica e exigimos colocar o cinto de segurança, entendo que, provavelmente, o que possa evoluir em termos de indústria é a gente pensar que segurança tem que vir de fábrica. Então, provavelmente, o que pode ser algo para se enxergar em termos legislativos é a padronização de que o recurso tem que vir de fábrica. A exigência de pedir o fator duplo de autenticação na hora em que o usuário está habilitando a sua configuração de conta ali do celular é algo que seria pertinente. Hoje, muitas vezes, depende da vontade do usuário. Se ele quiser, ele coloca um fator duplo de autenticação, que melhoraria muito a sua proteção e evitaria o sequestro dos seus dados. Então, se isso viesse como padrão, exigência, como o cinto de segurança tem que vir no carro, de fábrica, se viesse como padrão na hora em que você configura o celular e na hora que você configura as aplicações, isso poderia ser uma exigência regulatória, só para complementar a fala.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Muito obrigado, doutora. É interessante: um padrão de fábrica para a segurança.

Dr. Waldemar, nós vamos caminhar para o encerramento da nossa audiência pública, e eu vou fazer aqui agora o meu comentário do que aprendi aqui das falas de todos. Percebo que há um conhecimento profundo de cada um que participou conosco. Agora, eu saio daqui muito preocupado, porque nós demoramos demais a agir no Brasil em termos de proteção de dados e de ciberataques, criamos uma legislação que ainda não está totalmente implementada, inclusive nos órgãos públicos. O próprio Estado brasileiro ainda não se adaptou, não se colocou dentro de padrões de conhecimento e de, vamos dizer assim, preservação e proteção do que a própria lei exige. E sinto que nós não estamos dando a importância devida a um assunto para o qual o mundo inteiro já acordou, como disse o Emilio, que é bilionário, que é o novo garimpo, que são as informações que nós temos hoje digitalizadas das várias áreas, vários setores da economia.

Eu gostaria que o senhor comentasse isto, o senhor como nosso representante da autoridade nacional nesse assunto: onde nós vamos caminhar, como nós vamos caminhar e para qual direção caminharemos no sentido de mudarmos esse assunto. Mais debates, chamar a autoridade, chamar mais ao debate. Como o senhor disse, o próprio mercado pode regular? Então, seria muito interessante que, em novos debates, os setores e os atores dessa área pudessem participar e levar, vamos dizer assim, um pouco mais de debate ao País sobre esse assunto.

Eu termino esta audiência pública e caminho para o encerramento bastante preocupado, dizendo que nós brasileiros estamos muito vulneráveis a esses ataques e a esse vazamento de dados, Waldemar.

O SR. WALDEMAR GONÇALVES ORTUNHO JUNIOR (Para expor. *Por videoconferência*.) - Nós temos grandes desafios. Por exemplo, quando eu vejo que houve vazamento dos meus dados, com a quantidade de vezes que eu já forneci esses dados em comércio, em empresas, em *sites*, descobrir onde houve esse vazamento é o grande desafio que nós temos pela frente.

A nossa LGPD, no seu art. 50, já prevê uma autorregulação. Então, estamos trabalhando de uma forma forte com diversos setores. Como a lei geral afeta diversas, diferentes empresas e setores, nada melhor do que o setor dizer onde estão suas dificuldades, onde estão seus riscos e tudo mais. Então, é um PL até do Senador Antonio Anastasia, que está na Câmara. Nós estamos trabalhando de uma forma a incentivar com que as empresas pensem nisso, trabalhem nisso e atuem juntamente com a autoridade.

Eu vejo também, se nós compararmos com a Europa, que teve uma lei aprovada em 2016, mas é um resultado de diretivas que tratam até 1995 e até datas anteriores. Ela já tem uma cultura enraizada, o titular de dados já tem essa preocupação com os seus próprios dados. Eu acho que é um caminho de mudança de cultura. Ele não é imediato, mas ele tem que ser percorrido e com todos os nossos colaboradores. E com debates, como a iniciativa deste debate de hoje, nós podemos acelerar esse processo. É preocupante, é um problema mundial. E o Brasil está caminhando também em uma forma a levar essa proteção de dados aos seus titulares, como todos almejam. E todos esses têm esse mesmo objetivo.

Eu sou bem otimista, Senador. Eu acho que em breve nós alcançaremos resultados promissores.

O SR. PRESIDENTE (Carlos Viana. PSD - MG) - Muito obrigado.

Quero agradecer desde já a participação inicial do Dr. Carlos Bruno Ferreira da Silva, Procurador da República por Minas Gerais; ao Dr. Waldemar Gonçalves Ortunho Junior, Diretor-Presidente da Autoridade Nacional de Proteção de Dados; à Dra. Patrícia Peck Pinheiro, Presidente da Comissão Especial de Privacidade e Proteção de Dados da seccional de São Paulo da Ordem dos Advogados do Brasil; e ao Emilio Simoni, que é Executivo de Segurança da PSafe, que nos trouxe aqui os atuais dados. Eu agradeço aos senhores pela gentileza.

Esta audiência pública é apenas o início.

Encerro, mais uma vez dizendo da preocupação e da vulnerabilidade a que estamos expostos e que o Brasil precisa tratar desse assunto como uma questão realmente de defesa nacional, não só dos dados pessoais, mas principalmente dos ciberataques ao nosso serviço público e à exposição de dados e também de controle no País.

Nada mais havendo a tratar, declaro encerrada a presente reunião.

Muito obrigado a todos que participaram. Até breve!

(Iniciada às 11 horas e 03 minutos, a reunião é encerrada às 13 horas e 07 minutos.)