10160698 08012.003074/2018-16

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

Nota Técnica n.º 395/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ

Processo n. 08012.003074/2018-16

Representante: Departamento de Proteção e Defesa do Consumidor (*ex-officio*)

Representado: Sky Serviços de Banda Larga Ltda.

Assunto: Exposição de dados pessoais de consumidores

Ementa: Averiguação preliminar. Exposição temporária. Arquivos de *logs*. Proteção à privacidade. Possível prática abusiva. Atuação pró-ativa da SKY para resolver o problema. Contratação de empresa independente. Entendimento do MPDFT no sentido de ausência de demonstração de exposição de dados de consumidores e de suficiência das providências adotadas. Exaurimento de finalidade. Sugestão de Arquivamento.

I. RELATÓRIO

Trata-se de Averiguação Preliminar iniciada *ex officio,* no âmbito do Departamento de Proteção e Defesa do Consumidor (DPDC), da Secretaria Nacional do Consumidor (Senacon), do Ministério da Justiça e Segurança Pública (MJSP), em face da empresa **Sky Serviços de Banda Larga Ltda.** (Representada), em razão de notícias sobre a exposição de dados de consumidores, tais como: nome completo, e-mail, senha de login do serviço, endereço de IP, métodos de pagamento, número de telefone e endereço residencial, o que teria atingido 32 milhões de consumidores brasileiros clientes da Representada e usuários da TV por assinatura.

Segundo a notícia, publicada em 05 de dezembro de 2018 no site "TechTudo", os dados dos clientes brasileiros da Representada ficaram expostos na Internet. A notícia tem com base o trabalho desenvolvido por pesquisador de segurança independente, o qual ao utilizar os recursos avançados do mecanismo de pesquisa Shodan encontrou vários servidores no Brasil, baseados no banco de dados da *Elasticsearch* que disponibilizavam as informações contidas sem autenticação. Entre essas informações, havia um grupo chamado "*digital-logs-prd*", que por simples comando expôs os dados dos clientes/consumidores da Representada. O pesquisador também revelou ter conseguido acessar informações confidenciais, como endereços residenciais e números de telefone de políticos de alto escalão, como governadores e funcionários do governo.

Com a finalidade de averiguar a veracidade dos fatos, por meio da Notificação nº 93/2018/CSA-SENACON/CGCTSA/DPDC/SENACON, de 13 de dezembro de 2018, o DPDC solicitou à Representada a apresentação dos seguintes esclarecimentos, sem prejuízo a outras considerações: *a) Quantos consumidores brasileiros tiveram suas contas invadidas? b) Como ocorreu o*

vazamento de dados? c) As notícias mencionam a coleta de dados pessoais, já listados acima. A Sky confirma que tais dados foram coletados? Além destes, existem outros dados ou informações objeto da atuação dos hackers? Se afirmativo, quais? d) Quais são as medidas que estão sendo adotadas pela Sky? Os consumidores afetados já foram informados? Especifique as ações tomadas de forma minuciosa. e) Como a Sky age para proteger os dados de seus usuários e de que instrumentos dispõe para que essa proteção seja efetiva?

Em resposta, datada de 28 de dezembro de 2018, a Representada explicou, a princípio, que o meio pelo qual o pesquisador obteve os dados era de difícil acesso e, portanto, somente poderia ter sido empregado por um nicho muito específico de pessoas com alto conhecimento tecnológico. Alegou ainda, que o time de tecnologia da informação da Representada identificou o erro de configuração em um servidor *ElasticSearch* da *AWS* e o corrigiu em 30 minutos após o contato do site Tecmundo, tempo esse que permitiu a exposição temporária de arquivos de *logs* armazenados no servidor que continha dados pessoais dos consumidores da Representada. Também afirmou que contratou a *Pricewaterhouse Coopers (PwC)* para realizar a investigação forense do servidor *ElasticSerach* da *AWS*. Além disso, pontuou que algumas informações veiculadas pelas notícias eram imprecisas, principalmente as abaixo elencadas:

> *"Não houve acesso indevido aos sistemas operacionais da SKY; o que ocorreu foi um erro de configuração em um servidor ElasticSearch da AWS possibilitando eventual acesso pela Internet a arquivos de logs da SKY por pessoa com conhecimento tecnológico avançado;*
> *Os arquivos continham milhões de linhas de log, todavia, conforme será demonstrado apenas algumas dessas linhas poderiam incidentalmente conter dados de consumidores. Diferentemente do noticiado pelo site TechTudo não existe qualquer possibilidade de dados de 32 milhões clientes brasileiros da SKY terem sido expostos, uma vez que a empresa tem menos de 6 milhões de clientes;*
> *Ao contrário do noticiado, não houve acesso a dados sensíveis de consumidores da SKY;*
> *Até esse momento, não há motivos para acreditar que qualquer dado de consumidor tenha sido acessado por terceiros ou removido dos arquivos de logs junto ao servidor ElasticSearch da AWS."*

Isto posto, a Representada abordou os questionamentos demandados por este Departamento, esclareceu, portanto, que não havia em que se falar de "contas de consumidores invadidas", já que nenhum sistema de segurança foi violado, especialmente suas bases de dados operacionais, mas que ocorreu apenas um erro de configuração temporário no servidor *ElasticSearch* da *AWS*, que permitiu a exposição de arquivos de *logs*, arquivos esses que continham, indiretamente, dados de consumidores. Para mais, elucidou que o apurado, até o momento da defesa, era, na verdade, uma exposição temporária de arquivos de *logs* que estavam armazenados em um servidor da *ElasticSearch*, em virtude de ausência de um sistema de autenticação para ingresso nessa base de dados de pesquisa. Reiterou que havia uma investigação forense para apurar o ocorrido, mas mesmo não concluída poderia deduzir que a exposição temporária de dados se deu por conta de erro de configuração de armazenamento do servidor da *ElasticSearch* da *AWS*, ocasionada por um terceiro contratado.

Ademais, informou que no estágio, à época, da investigação somente poderia confirmar a existência de uma configuração incorreta, e que a exposição resultante abarcaria, nos arquivos de *logs*, informações de dados pessoais de não mais de 1.6 milhões de clientes, sendo que em aproximadamente 1.45 milhões desses casos, os dados se limitariam a nome, endereço, número de telefone, data de nascimento e número de CPF (devidamente criptografado). Identificou-se também: *"(i) aproximadamente 106.000 (cento e seis mil) números de CPF, sem qualquer informação adicional; (ii)*

aproximadamente 24.000 (vinte e quatro mil) informações bancárias (nome do banco e número da conta) com números de CPF criptografados, mas sem nenhuma informação adicional e (iii) aproximadamente 5.000 (cinco mil) números de cartão de crédito (somente os quatro primeiros e os quatro últimos dígitos), sem nenhuma infrmação adicional". Mais uma vez, a Representada alega que os seus dados de produção, suas contas e as contas dos seus clientes não foram invadidos.

Em relação às medidas adotadas, a Representada apresentou que logo da correção do problema, com suporte de auditores externos da PwC, iniciou um processo de revisão de todos os seus sistemas para assegurar que não continham erros de configurações similares. Além do mais, adotou medidas preventivas e ações para evitar ameaças cibernéticas, dentre elas: *"a. Análise interna de doze contas AWS; b. Alteração de senhas e logins; c. Revisão das regras de segurança da SKY; d. Revisão e aperfeiçoamento dos controles de acesso; e. Alteração do endereço de IP; f. Alteração das chaves – gateway API; g. Alteração do URL Load Balancer; h. Remoção de publicação dos sites; i. Fechamento de todos os 700 Buckets"*. Com relação às contas AWS, foram tomadas as seguintes medidas: *"a. Alteração do caminho API Digital: API/IID do consumidor/login-CPF; b. Configuração do Setup e WAF em API Digital; c. Remoção de 70 tabelas Dynamodb referentes à AWS em São Paulo; d. Remoção de 55 tabelas Dynamodb referentes à AWS em Virgínia; e. Remoção de 12 buckets S3 (armazenamento da AWS)"*. Por fim, realizou-se também: *"a. Avaliação e análise de eventuais vulnerabilidades da API mobile.sky.com.br (API do antigo aplicativo da SKY, anterior ao Minha SKY); b. Análise de antigos códigos API, que estavam desativados em razão da inatividade das fontes"*.

No que tange aos instrumentos dispostos a efetivar a proteção de dados dos usuários, a Representada comunicou que desenvolveu e implementou uma política corporativa de "Proteção às Informações da Empresa e à Privacidade Individual", a qual tinha por objetivo definir todos os controles necessários à proteção da confidencialidade e integridade dos dados pessoais de seus clientes e funcionários, sendo assim, as seguintes medidas foram adotadas:

> *"**Autenticação:** todos os acessos a informações pessoais requeriam autenticação para confirmação da identidade do usuário.*
> ***Autorização:** todos os acessos a informações pessoais dependiam da demonstração da efetiva necessidade, e apenas eram concebidos após a devida autorização (gerência, etc.). Níveis de necessidade e autorização eram implementados em cada um dos sistemas internos da SKY por meio de um sistema de identificação e gestão de acesso.*
> ***Finalidade:** todos os acessos a informações deveriam ser limitados ao propósito de sua solicitação; (i) era concedido acesso ao mínimo de informações necessário e pelo menor período de tempo possível, somente para atender aos propósitos da solicitação; e (ii) somente era concedido acesso a destinatários que efetivamente necessitavam de tais informações.*
> ***Divulgação a terceiros:** a divulgação ou uso de Informações da Empresa por terceiros dependia da formalização de um Termo de Confidencialidade ou de qualquer outro documento ou compromisso de confidencialidade aprovado pelo departamento legal. Adicionalmente, todos os terceiros que eventualmente obtivessem acesso a informações pessoais da SKY deveriam antes ser submetidos a um processo de "análise de risco de terceiros". Por meio desse processo, o time de segurança da SKY devia assegurar que que os devidos controles fossem implementados pelos terceiros para proteger os dados pessoais em poder da SKY.*
> ***Comunicação e Treinamento:** a SKY comunicaria essa política a todos os usuários de informações da Empresa. Adicionalmente, a Empresa forneceria o devido treinamento aos usuários para execução dessa política.*
> ***Retenção e Destruição:** os registros relativos a requisições de acesso, aprovações e indeferimentos (e cancelamentos) do direito de uso de Informações da Empresa seriam mantidos, de acordo com cada tipo de informação e com a natureza de seu*

> *uso. As Informações da Empresa seriam destruídas com métodos seguros, e em conformidade os registos empresarias e período de retenção, de acordo com cada tipo de informação."*

Outrossim, a Representada anexou duas tabelas relativas a medidas gerais de proteção e a medidas técnicas de proteção. Enfim, ressaltou que a investigação ainda estava sendo apurada a fim de que não houvesse qualquer dúvida sobre o ocorrido, e defendeu que não houve danos aos consumidores. Solicitou que o trâmite da presente averiguação preliminar permanecesse sob sigilo até a sua conclusão.

Juntou-se aos autos o Relatório de Reposta a Incidente (8858713) elaborado pela PwC e apresentada em 28 de dezembro de 2018 e, à vista da conclusão das investigações sobre a exposição dos dados, a Representada solicitou uma reunião para apresentar esclarecimentos adicionais sobre o caso.

A reunião ocorreu nas dependências do MJSP em 19 de junho de 2019 com a presença de representantes do DPDC e da Representada. Esta última alegou que a denúncia, que originou o procedimento administrativo, teria diversas imprecisões, entretanto, confirmou a existência da vulnerabilidade na custódia dos dados de seus clientes e, mesmo que fosse de difícil acesso essas informações, adotou medidas para a correção do feito. Sobre o acesso de terceiros aos dados, afirmou que Fábio Castro (pesquisador) não realizou extração de dados de usuários, mas, na realidade, dois acessos no exterior resultaram na mencionada extração, não sendo possível alcançar a exatidão do conteúdo, mas a qualidade dos dados. Reiterou que a quantidade de consumidores afetados (32 milhões, na notícia) não correspondia à realidade. Informou também que, após a identificação da falha, contratou auditoria independente para avaliar a situação e criou um grupo de trabalho para estudar o assunto. Comunicou ainda, que trabalhou de forma célere para conter a situação e buscou aprimorar os mecanismos de proteção, ainda que não houvesse ocorrido a exposição de dados considerados sensíveis.

Da análise circunstancial, este Departamento constatou que a Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec) do Ministério Público do Distrito Federal e Territórios (MPDFT) instaurou Inquérito Civil Público, pela Portaria n° 30/2018 de 11 de dezembro de 2018, a fim de investigar o incidente da segurança do banco de dados da Representada.

É o relatório. Passa-se a opinar.

II. FUNDAMENTAÇÃO

No âmbito da Administração Pública, cada órgão ou repartição tem diferentes e específicas atribuições legais para garantir o direito dos cidadãos dentro de suas competências e especialidades. Na fiscalização das infrações às relações de consumo, todos os integrantes do Sistema Nacional de Defesa do Consumidor têm competência concorrente no exercício do poder de polícia administrativo, cabendo à Secretaria Nacional do Consumidor a coordenação da Política Nacional de Defesa do Consumidor, sendo-lhe outorgadas as atribuições de planejar, elaborar, propor e coordenar a política nacional de proteção ao consumidor.

De acordo com o Decreto nº 7.738/2012, que criou a Secretaria Nacional do Consumidor (Senacon), bem como o artigo 106 do Código de Defesa do Consumidor e o artigo 3º do Decreto n. 2.181/97, a Senacon é um órgão federal que concentra suas atividades no planejamento, elaboração, coordenação e execução da Política Nacional das Relações de Consumo.

Nesse sentido, a Senacon conta com o Departamento de Proteção e Defesa do

Consumidor - DPDC que, de acordo com o art. 18 do Regimento Interno da Senacon (Portaria nº 1.840, de 21 de agosto de 2012, publicada no D.O.U, de 22 de agosto de 2012 – Seção 1 – n. 163, fls. 26-29), é órgão de assessoria para análise, planejamento, fiscalização, acompanhamento do Sistema Nacional do Consumidor. Assim, de acordo com o inciso XI do mesmo artigo, compete ao DPDC fiscalizar demandas que envolvam relevante interesse geral e de âmbito nacional.

No que pertine às atribuições legais específicas do DPDC, deve ser destacado ainda o respeito do exercício do Poder de Polícia entre a União, os Estados, os Municípios, e o Distrito Federal, o qual segue a distribuição constitucional das competências administrativas, com base no Princípio da Predominância do Interesse. Cabe ainda a apreciação de matérias e questões de predominante interesse geral, ao passo que aos Estados ficam afetas as matérias de predominante interesse regional e aos municípios concernem os assuntos de interesse local.

Nesse sentido, por meio da Nota Técnica nº 328 CGAJ/DPDC/2008, firmou-se entendimento de que ao DPDC compete prioritariamente a análise de questões que tenham repercussão nacional e interesse geral.

Da análise dos autos, verifica-se que a representada já tomou as medidas reparatórias necessárias, tratando-se de medidas gerais de proteção e a medidas técnicas de proteção, a fim de garantir a devida proteção do consumidor e de seus dados.

Aliás vale colacionar os termos da homologação da promoção de arquivamento no âmbito do Ministério Público do Distrito Federal e Territórios - MPDFT (SEI 11237270), onde se conclui tanto que a Representada adotou as providências para o saneamento da falhas segurança como a ausência de demonstração de vazamento de dados de seus clientes.

Por tal razão, verificando-se que já ocorreu a adoção das devidas diligências, não se visualiza, por ora, outras a serem adotadas no presente feito, motivo pelo qual se sugere o seu arquivamento.

III. CONCLUSÕES

Ante o exposto, sugere-se o arquivamento do presente feito por exaurimento de finalidade, em razão da já tomada de medidas por parte da Sky Brasil Serviços Ltda., nos termos do art. 52 da Lei nº 9.784, de 1999, sem prejuízo da reapreciação do assunto caso novos elementos sejam apresentados pelos eventuais interessados.

À Consideração Superior.

LOUISE GABRIELLE ESTEVES SOARES DE MELO
Chefe da Divisão de Investigação

De acordo. Ao Coordenador-Geral de Consultoria Técnica e Sanções Administrativas.

RAFAEL ALVES LOURENÇO
Coordenador de Sanções Administrativas Substituto em exercício

De acordo. À Diretora do Departamento de Proteção e Defesa do Consumidor.

LEONARDO ALBUQUERQUE MARQUES
Coordenador-Geral de Consultoria Técnica e Sanções Administrativas

De acordo. Arquive-se.

JULIANA OLIVEIRA DOMINGUES
Diretora do Departamento de Proteção e Defesa do Consumidor

Documento assinado eletronicamente por **Juliana Oliveira Domingues**, **Diretor(a) do Departamento de Proteção e Defesa do Consumidor**, em 13/05/2020, às 18:31, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Leonardo Albuquerque Marques**, **Coordenador(a)-Geral de Consultoria Técnica e Sanções Administrativas**, em 14/05/2020, às 10:42, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Rafael Alves Lourenço**, **Coordenador(a) de Sanções Administrativas- Substituto(a)**, em 14/05/2020, às 11:38, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Louise Gabrielle Esteves Soares de Melo**, **Chefe da Divisão de Investigação**, em 14/05/2020, às 11:40, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **10160698** e o código CRC **3A355EB7**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Referência: Processo nº 08012.003074/2018-16 SEI nº 10160698