Silveira e Baqui: Os seguros cibernéticos e o ransomware

O ataque cibernético sofrido pelo Superior Tribunal de Justiça na última terça-feira (3/11), que inclusive chegou a interromper as sessões de julgamento por videoconferência das seis turmas, tem repercutido nos noticiários [1]. Segundo comunicado do ministro Humberto Martins, presidente do STJ, divulgado no final do último dia 5, os links para a rede mundial de computadores foram desconectados como

que um vírus estava circulando na rede [2].

A corte, na tentativa de mitigar os danos, ainda suspendeu os prazos processuais [3] e recomendou a todos os usuários internos que não utilizem seus computadores, ainda que pessoais, que estejam conectados com algum dos sistemas informatizados do tribunal [4]. A Polícia Federal foi acionada para investigar o ataque e o site e demais sistemas seguem fora do ar.

Infelizmente, notícias como essa estão cada vez mais comuns, porque cresce exponencialmente o número de ataques cibernéticos mundo afora e no Brasil [5] — sobretudo do tipo *ransomware*, ou extorsão cibernética —, o que torna um desafio à atuação preventiva na proteção dos dados pessoais tratados, bem como a recuperação ou mitigação dos danos provenientes dos ataques.

Com a vigência da Lei Geral de Proteção de Dados brasileira, que atribui aos agentes de tratamento o dever de segurança, impondo-lhes a *"utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão"* (artigo 6º, VII) e sujeitando-lhes à responsabilidade civil (artigo 42) e a penalidades administrativas (artigo 52) em caso de violação a esse dever, o risco decorrente de ataque aumenta substancialmente.

Diante desse cenário, que poderá envolver grande impacto financeiro e reputacional, não só para as grandes empresas, mas também as pequenas e médias, é que se expandem os seguros contra riscos cibernéticos no setor privado.

Consoante lição de Domingos Afonso Kriger Filho, *"o desenvolvimento da atividade securitária acha-se hoje indissociavelmente ligado à evolução da concepção de acidente, que face a complexidade da vida moderna, deixou de ser visto como um infortúnio ou fato excepcional (…) passando a ser, em suma, uma constante social"* [6].

2023 - www.conjur.com.br - Todos os direitos reservados.

Tal noção, sem dúvida, é que impulsiona o seguro contra riscos cibernéticos, pois o acidente — e os danos operacionais, reputacionais e de responsabilidade dele provenientes — não são mais questão de "se", mas de "quando".

No final dos anos 1990 surgiram nos Estados Unidos as primeiras apólices de seguro de responsabilidade cibernética, tendo por público-alvo companhias de tecnologia da informação gerenciadoras de sistemas e redes de outras empresas e consumidoras [7] e mídia digital [8]. No início dos anos 2000, as apólices começaram a cobrir acesso não autorizado, segurança de rede, perda de dados e sinistros relacionados a *malwares* [9]. Em meados dos anos 2000, começaram a ser incluídas coberturas para interrupção de negócios, extorsão cibernética e danos aos ativos de rede [10]. Com a promulgação da *California Security Breach and Information Act*, em 2003, as companhias de seguro tiveram de se adaptar e passaram a fornecer cobertura para perícias de TI e segurança da informação, relações públicas, monitoramento de crédito e notificação de consumidores, bem como defesa regulatória e multas e penalidades relacionadas à notificação dos consumidores [11].

Assim, hoje o seguro cibernético pode ser definido como aquele direcionado para perdas patrimoniais e decorrentes de responsabilidade civil que resultem de um ataque a partir de computador ou sistemas de tecnologia da informação de uma empresa [12].

Nos Estados Unidos, em 2010, os seguros autônomos contra riscos cibernéticos eram oferecidos por cerca de 50 companhias, número que dobrou nos últimos dez anos [13]. Em 2018, o prêmio dos seguros cibernéticos ofertados de forma individualizada somava U$ 1,1 bilhão e, apesar de ter dobrado desde 2015, ainda representa menos de 0,5% de todas as apólices de não-vida (*property and casualty* — P&C) [14].

No Brasil, o ramo compreensivo de riscos cibernéticos, pertencente ao grupo responsabilidades (0327) foi acrescentado no final de 2018, por meio da Circular Susep 579, de 13 de novembro de 2018, a partir da observação do crescimento desse risco. Atualmente, há 12 empresas que oferecem seguros nesse ramo, com uma soma de R$ 49 milhões de reais em prêmios [15], sendo as três maiores a AIG Seguros Brasil S.A. (R$ 23,8 milhões), a Allianz Seguros S.A (R$ 6,9 milhões) e a Zurich Minas Brasil Seguros S.A. (R$ 6 milhões) [16].

Só no primeiro semestre de 2020 já se registrou um aumento de 80% em relação a 2019 no que diz respeito ao montante dos prêmios [17], provavelmente em resposta à então iminente vigência da LGPD e o aumento dos riscos gerados pela pandemia da Covid-19, que aumentou o trabalho remoto e, consequentemente, a exposição a ataques cibernéticos.

Ransomware ou extorsão cibernética

Na mídia, circula informação de que *"todos os dados e sistemas que estavam nos servidores do STJ foram criptografados"*, incluindo a caixa de e-mails dos ministros, e que foi pedido resgate [18].

2023 - www.conjur.com.br - Todos os direitos reservados.

No comunicado do presidente do Superior Tribunal de Justiça se afirma que *"o ataque hacker bloqueou, temporariamente, com o uso de criptografia, o acesso aos dados"*, mas não se menciona se algum resgate foi solicitado. Contudo, de acordo com matéria publicada no portal *G1*, ministros teriam confirmado que houve tal pedido, mas não deram detalhes [19].

De fato, um dos principais tipos de ataques cibernéticos é o causado por *ransomware*, também denominado de extorsão cibernética, que consiste em um *malware* que invade e bloqueia o acesso aos dados, ao *website*, aos sistemas ou outros recursos críticos da vítima, normalmente com a exigência de pagamento de uma quantia para devolver o acesso [20]. Esse tipo de *software* malicioso pode invadir qualquer tipo de computador, incluindo *desktops*, *laptops*, *tablets*, *smartphones*. E o objetivo do *hacker* não é destruir ou bloquear o dado de forma permanente, mas garantir o pagamento rápido do resgate [21].

Nos Estados Unidos, não só empresas, mas vários governos locais e agências sofreram extorsão cibernética, havendo notícias de declarações de estado de emergência e até mesmo pagamentos de resgate [22]. De acordo com pesquisas recentes, de janeiro a maio de 2020, *"o Brasil lidera a lista dos países mais afetados por ataques de ransomware empresariais ao redor do mundo"*, o que pode ser explicado, em parte, pelo trabalho remoto decorrente da pandemia [23]. Foram amplamente noticiados recentes ataques a grandes empresas. Enquanto umas negaram ter pago o resgate — normalmente solicitado em *bitcoins* ou criptomoedas —, outras evitaram responder tais questionamentos [24].

Em geral, aconselha-se a não pagar pelo resgate, para evitar estimular essa espécie de crime cibernético e por não haver garantia de restauração dos dados [25]. Há, inclusive, iniciativas que disponibilizam ferramentas para descodificação de *ransomware* [26]. O Tesouro Americano chegou a emitir recente comunicado alertando a possibilidade de aplicação de multas a empresas que facilitam o pagamento de resgate, caso este seja feito a pessoa ou entidade constante de lista denominada *Specially Designated Nationals and Blocked Persons* [27].

No caso do STJ, o ministro Humberto Martins afirma que os dados criptografados estão preservados nos sistemas de *backup* do tribunal, incluindo os processos judiciais, contas de e-mails e contratos administrativos. E que a equipe da Secretaria de Tecnologia da Informação trabalha junto com as empresas prestadoras de serviços de tecnologia ao tribunal, bem como com o Centro de Defesa Cibernética do Exército Brasileiro, na restauração dos sistemas de informática.

Contudo, quando inexiste uma cópia de segurança, muitas vezes não resta outra alternativa à vítima [28]. Por isso é comum a existência de cobertura a *ransomware* em apólices de seguro cibernético, que normalmente incluem o valor pago pelo resgate, o custo para contratação de um especialista para negociar com os *hackers* e o custo para uma análise forense a fim de determinar como foi feita a invasão e recomendar formas de evitar novas invasões no futuro [29].

2023 - www.conjur.com.br - Todos os direitos reservados.

Tal cobertura gera muitas polêmicas. Enquanto alguns acusam as companhias de seguro de encorajarem esse tipo de ataque cibernético ao pagarem rapidamente os resgates — por julgarem ser uma forma mais rápida e barata de recuperar os dados, em vez da tentativa manual de recuperação [30], outros defendem que a escolha sobre pagar o resgate é do segurado, que muitas vezes se vê diante de uma escolha entre pagar o resgate ou encarar o risco de perdas operacionais muito maiores, que podem se estender por semanas ou meses e que, se não tiverem cobertura para tais perdas, será ainda maior a probabilidade de pagaram o resgate [31].

A partir de uma análise das três maiores seguradoras atuantes nesse ramo de seguros no Brasil, verifica-se que a AIG inclui como extensão opcional a cobertura para "extorsão na internet" [32]. Também a Zurich inclui tal cobertura como adicional. Já a Allianz inclui tal cobertura em suas condições gerais do seguro de Responsabilidade Civil por Ataques Cibernéticos, sujeita a um limite máximo de indenização.

Conclusão
É crescente o número de seguros contra riscos cibernéticos no Brasil e no mundo, que poderá se revelar uma boa alternativa em face à crescente responsabilidade civil e administrativa decorrente de violações ao dever de segurança que se sujeitam as empresas que lidam com dados pessoais.

Contudo, deverão ser cuidadosamente analisadas as apólices de seguro, sobretudo para verificar a cobertura ou a necessidade de contratação adicional para o risco decorrente de extorsão cibernética, que tem sido bastante comum no Brasil e pode colocar em risco dados pessoais e outros dados sensíveis das empresas.

Quanto ao Superior Tribunal de Justiça, teremos de continuar a acompanhar as notícias e torcer para que os sistemas sejam rapidamente restabelecidos para continuidade da prestação jurisdicional da Corte da Cidadania e identificados os responsáveis pelo ataque.

[1] https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/stj-e-alvo-de-ataque-de-hacker-e-policia-federal-investiga-o-sistema Acesso em 4 nov. 2020.

[2] https://g1.globo.com/politica/noticia/2020/11/05/invasao-de-computadores-nao-afetou-informacoes-de-processos-diz-presidente-do-stj.ghtml Acesso em 5 nov. 2020.

[3] RESOLUÇÃO STJ/GP N. 25 DE 4 DE NOVEMBRO DE 2020. Disponível em: https://www.cjf.jus.br/dje/infra/js/pdf/web/viewer.html?file=https%3A%2F%2Fwww.cjf.jus.br%3A443%2F ASSINADO.PDF%26amp%3BstatusDoDiario%3DASSINADO Acesso em 5 nov. 2020.

[4] Cf. https://www.facebook.com/stjnoticias/photos/a.10150813555331852/10157355910396852/.

2023 - www.conjur.com.br - Todos os direitos reservados.

[5] *"O Brasil sofreu mais de 1,6 bilhão de tentativas de ataques cibernéticos no primeiro trimestre do ano, de um total de 9,7 bilhões da América Latina. É o que indicam dados coletados pela Fortinet através de sua plataforma que coleta e analisa incidentes de segurança cibernética em todo o mundo"* . Disponível em: https://olhardigital.com.br/fique_seguro/noticia/brasil-teve-mais-de-1-6-bilhao-de-ataques-ciberneticos-em-tres-meses/100420 Acesso em 20 ago. 2020.

[6] KRIGER FILHO, Domingos Afonso. O contrato de seguro no Direito brasileiro. Rio de Janeiro: Labor Juris, 2000. p.16

[7] GRANATO, Andrew. POLACEK, Andy. The growth and challenges of Cyber Insurance. Chicago Fed Letter, No 426, 2019.

[8] ProWriters. Cyber Insurance Blog. The evolution of cyber insurance. Disponível em: https://prowritersins.com/cyber-insurance-blog/cyber-insurance/ Acesso em 20 ago. 2020.

[9] ProWriters. Cyber Insurance Blog. The evolution of cyber insurance. Disponível em: https://prowritersins.com/cyber-insurance-blog/cyber-insurance/ Acesso em 20 ago. 2020.

[10] ProWriters. Cyber Insurance Blog. The evolution of cyber insurance. Disponível em: https://prowritersins.com/cyber-insurance-blog/cyber-insurance/ Acesso em 20 ago. 2020.

[11] ProWriters. Cyber Insurance Blog. The evolution of cyber insurance. Disponível em: https://prowritersins.com/cyber-insurance-blog/cyber-insurance/ Acesso em 20 ago. 2020.

[12] ROMANOSKY, Sasha. et al. Content analysis of cyber insurance policies: how do carriers write policies and price cyber risk? Disponível em: https://www.ftc.gov/system/files/documents/public_comments/2017/10/00012-141437.pdf Acesso em 20 ago. 2020.

[13] ProWriters. Cyber Insurance Blog. The evolution of cyber insurance. Disponível em: https://prowritersins.com/cyber-insurance-blog/cyber-insurance/ Acesso em 20 ago. 2020.

[14] GRANATO, Andrew. POLACEK, Andy. The growth and challenges of Cyber Insurance. Chicago Fed Letter, No 426, 2019.

2023 - www.conjur.com.br - Todos os direitos reservados.

[15] No período de novembro de 2018 a junho de 2020.

[16] Dados extraídos da SUSEP. Disponíveis em: http://www2.susep.gov.br/menuestatistica/SES/resp_premiosesinistros.aspx Acesso em 20 ago. 2020.

[17] Até dezembro de 2019, o prêmio total desse segmento de recurso era de R$ 21,435 milhões. Até junho de 2020 o valor passou para R$ 38,371 milhões. Atualmente já está em R$ 49,277 milhões. http://www2.susep.gov.br/menuestatistica/SES/resp_premiosesinistros.aspx.

[18] https://obastidor.com.br/justica/hacker-criptografou-todos-os-processos-e-emails-do-stj-19; https://obastidor.com.br/justica/hacker-cobra-resgate-de-dados-sequestrados-do-stj-26 e https://migalhas.uol.com.br/quentes/335987/hacker-invade-stj–sequestra-dados-e-cobra-resgate.

[19] https://g1.globo.com/politica/noticia/2020/11/05/invasao-de-computadores-nao-afetou-informacoes-de-processos-diz-presidente-do-stj.ghtml Acesso em 5 nov. 2020.

[20] https://www.irmi.com/term/insurance-definitions/ransomware#:~:text=Coverage%20for%20losses%20associated%20with,and%20(3)%20the%20
.

[21] https://content.naic.org/cipr_topics/topic_ransomware.htm.

[22] Por exemplo: https://www.businessinsider.com/louisiana-declares-state-of-emergency-after-cybersecurity-attack-2019-11; https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html; https://www.zdnet.com/article/second-florida-city-pays-giant-ransom-to-ransomware-gang-in-a-week/; https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html.

[23] https://www.kaspersky.com.br/blog/empresa-brasil-ransomware-pandemia/15527/.

[24] https://g1.globo.com/economia/tecnologia/noticia/2020/07/03/ataques-ciberneticos-aumentam-com-pandemia-e-atingem-companhias-eletricas-no-brasil-e-no-mundo.ghtml.

[25] https://blog.avast.com/pt-br/ransomware-os-3-principais-motivos-que-voce-nunca-deve-pagar.

[26]Cf. https://www.nomoreransom.org/pt/index.html,

2023 - www.conjur.com.br - Todos os direitos reservados.

https://www.avast.com/pt-br/ransomware-decryption-tools.

[27] Cf. Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments do Department of the Treasury. Disponível em: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf. Acesso em 6 out. 2020.

[28] https://www.cbc.ca/news/technology/ransomware-cyber-insurance-pros-and-cons-1.5453619.

[29] https://www.irmi.com/term/insurance-definitions/ransomware#:~:text=Coverage%20for%20losses%20associated%20with,and%20(3)%20the%20
.

[30] https://www.cbc.ca/news/technology/ransomware-cyber-insurance-pros-and-cons-1.5453619.

[31] https://www.marsh.com/us/insights/research/cyber-insurance-supporting-fight-against-ransomware.html#:~:text=Far%20from%20being%20part%20of,ransomware%20and%20other%20cyber%

[32] *"Pagamento de qualquer perda por extorsão sofrida pelo Segurado exclusivamente como resultado de uma ameaça de segurança."* https://www.aig.com.br/seguros/cyber-edge#accordion-child_pr_cr_accordion_2.

Date Created
10/11/2020

2023 - www.conjur.com.br - Todos os direitos reservados.