Riscos cibernéticos e o mercado de seguros brasileiro

01/08/2022

A Lei Geral de Proteção de Dados (LGPD, nº 13.709, de 14 de agosto de 2018; em vigor desde 18 de setembro de 2021) trouxe ao país novo estado de consciência sobre a segurança da informação.

O tema não era novidade no ambiente empresarial que, ciente da importância da preservação de informações, já adotava relevantes medidas limitativas do uso de dados sigilosos. Mas a LGPD amplificou tais práticas, em prol de um ambiente virtual mais seguro, protetivo da privacidade, da intimidade, da autodeterminação individual, da honra e da imagem. Passou a disciplinar, de forma generalizada, as condutas pertinentes ao uso de dados pessoais e (tão importante quanto) a responsabilizar por eventual descumprimento os agentes que atuam no tratamento desses dados.

O vazamento de dados pessoais é um dos itens dentro de um gradiente mais amplo denominado *risco cibernético*. A sofisticação e o alcance dos ataques por meios virtuais modernos mimetizaram e amplificaram, no ambiente virtual, a vastíssima gama de riscos à incolumidade individual perpetrado por criminosos na vida *off-line*.

Em 2021, foram reportados no Brasil mais de 88,5 bilhões de tentativas de ataques cibernéticos, um aumento de mais de 950% com relação a 2020 (com 8,5 bi).[1] As principais formas de ataque são a distribuição de aplicativos (*malicious software* ou *malware*) capazes de roubar senhas, credenciais, informações financeiras (*botnet redline stealer*), controlar os dispositivos das vítimas (*remote code execution*) ou sequestrar dados para a cobrança de resgates (*ransomware*), geralmente em criptomoedas.[2]

Na maior parte das vezes o ataque ocorre mediante publicidade enganosa *on-line* ou esquemas de engenharia social. O ofensor cria enredo fictício *on-line* ou *off-line* para induzir a vítima, que passa a prestar informações por: (i) medo ou senso de urgência (*phishing*), *e.g*. pedido de atualização de um cadastro bancário; (ii) criação de vínculo de confiança com o ofensor (*pretexting*), *e.g*. utilização de falsa credencial pelo ofensor; (iii) visando a uma recompensa tangível (*baiting*), *e.g*. ganhar milhas; ou (iv) visando a uma recompensa intangível (*quid pro quo*), *e.g*. promessa de aumento da velocidade do computador.

Outra modalidade de ataque observada com grande frequência no Brasil – e aqui ocorreu a impressionante marca de 10% do total dos ataques dessa natureza visto no mundo — é o ataque DDoS (*Distributed Denial of Service*). Neste, o invasor ou grupo de invasores sobrecarrega o tráfego de internet do seu alvo, criando instabilidade ou queda do sistema.

O aumento de todos esses crimes, associado às obrigações da LGPD, impulsionou os programas de segurança digital no Brasil. Observam-se massivos investimentos em equipamentos, *softwares* e treinamento de pessoal; bem como a revisão das políticas internas, especialmente no trato com fornecedores. No entanto, mesmo as técnicas mais avançadas são incapazes de proteger de forma absoluta os sistemas de dados das empresas cujos modelos de negócio, muitas vezes, dependem da interface virtual com o grande público. Nesse cenário, o seguro cibernético ganha papel de destaque como ferramenta de gestão de risco.

É a partir do arquétipo securitário do ramo de responsabilidade civil que essa proteção vem sendo ofertada pelas seguradoras sediadas no Brasil – especialmente aquelas controladas por entidades norte-americanas ou europeias. Ou seja, as apólices são desenhadas para garantir os riscos de danos a terceiros no ambiente cibernético, incluindo custos de defesa, multas ou outras sanções impostas pelas autoridades aplicadoras da LGPD (desde que decorrentes de conduta culposa do segurado) e até despesas para a recomposição reputacional.

Em caráter acessório, sujeitas a sublimites de valor e, na maioria dos casos, a elevadas franquias, observam-se, adicionalmente, coberturas fora dos contornos da responsabilidade civil. Destacam-se (i) a cobertura para restauração de dados corrompidos por ação criminosa, (ii) a cobertura de lucros cessantes por perda de rede e (iii) a cobertura para pagamento de resgate de *ransomware*.

Como produtos securitários que são, os seguros de riscos cibernéticos também se sujeitam à dicotomia coberturas x exclusões, pautadas pelo grau de aversão ou aceitação do risco por seguradoras e, principalmente, resseguradoras em nível global. Quando se trata de seguro cibernético, essas (re)seguradoras têm se deparado com muitas incertezas (aleatórias), em contraposição aos riscos (mensuráveis) que se acostumaram a garantir. Isso tende a limitar a aceitação do risco por meio de vasto arsenal de exclusões. Mesmo aquelas tradicionais — como guerra e terrorismo, propriedade intelectual e exclusões do mercado de capitais — carregam um peso muito maior no seguro cibernético.

Seguindo esta cautela, as apólices atualmente comercializadas no Brasil não oferecem — embora juridicamente estejam autorizadas a oferecer — coberturas amplas para danos sofridos pelos próprios segurados, exceto no caso das coberturas adicionais acessórias, já mencionadas. Ademais, mesmo as coberturas de responsabilidade civil praticadas no mercado nacional trazem exclusões para danos materiais, excetuando destruição de dados; e danos corporais.

Tal limitação é grave a depender do nível de automação empregada na atividade do segurado. Se este utiliza acesso remoto para a execução de atividades que se materializam fora do ambiente virtual, *e.g*. sinalização de eventos críticos de trânsito em uma rodovia, o atual estado das garantias servirá para pouca coisa.

Mas isso não ocorre por má vontade das seguradoras. A virtualização das atividades empresariais exponencializa os riscos. A materialização frequente destes segue padrões estatísticos ainda não mapeados, de modo que a oferta de amplas coberturas pelas seguradoras, sem ressalvas como as indicadas acima, pode implicar risco sistêmico de elevadas proporções, apto a colocar em xeque a solvência do sistema securitário.

Tais restrições ocorrem em nível global. O pool ressegurador londrino Lloyds vem, desde 2018, indicando como linha mestra de subscrição de riscos de todas as naturezas que os (re)seguradores prevejam, de forma clara, se os riscos cibernéticos estão cobertos ou excluídos.[3] Em vista disso, apólices tradicionalmente silentes sobre esse aspecto, *e.g*. responsabilidade de administrador (seguro D&O), passaram a definir expressamente as consequências para sinistros decorrentes de eventos cibernéticos, geralmente excluindo-os da cobertura básica. Com isso, os denominados *silent cyber risks*, que não eram identificados no momento da contratação e, assim, estavam tacitamente cobertos, carregando incerteza para as seguradoras, receberam tratamento específico.

No Brasil, esta orientação vem ganhando forma desde 2020, mas foi a partir da Circular Susep nº 637, de 27 de julho de 2021, que a matéria ganhou contornos regulatórios. Tal circular distinguiu o seguro de responsabilidade civil compreensivo riscos cibernéticos (RC riscos cibernéticos) como ramo específico do grupo responsabilidades, favorecendo a segregação destes riscos pelas seguradoras, de modo que estas uniformizem suas carteiras segundo critérios estatísticos mais precisos e, assim, afastem a incerteza latente do *silent cyber risk*. Ou o risco cibernético é coberto e precificado, ou está excluído.

Na perspectiva do segurado, impõe-se a necessidade de compreender e lidar com as exclusões de riscos cibernéticos mediante contratação separada ou combinada de diversas apólices para cobrir um determinado risco em todas as suas facetas. Exemplificativamente, se um advogado pretende garantir o risco de causar dano a seu cliente em decorrência de erro profissional relacionado a evento cibernético, deverá contratar, complementarmente ao Seguro de Responsabilidade Civil Profissional (E&O — *errors and omissions*), a cobertura de riscos cibernéticos, que é oferecida como acessória à apólice E&O ou em apólice autônoma de risco cibernético.

Se por um lado as limitações atuais descritas dos seguros cibernéticos oferecidos parecem depor contra a sua aceitação no meio empresarial, é indiscutível que sua contratação é importante passo na conscientização sobre a gestão de riscos cibernéticos em sentido amplo. A interação colaborativa entre segurado e seguradora, principalmente no ambiente de grandes riscos, pode fomentar a sinergia entre ambos, desde a subscrição da apólice até a regulação de um sinistro. O aprendizado decorrente desta interação será crucial para o desenvolvimento de uma estrutura de segurança cibernética que

extrapole a visão securitária sobre esse tipo de risco.

Tal movimento obrigará segurado e seguradora a mudarem de uma visão estática para uma visão dinâmica da segurança cibernética. Ou seja, ao lado da proteção contra as consequências dos riscos cibernéticos, incorporada principalmente na apólice de seguro, deverão abordar as causas daqueles riscos para preveni-las ou, ao menos, mitigá-las.

Assim como cuidar da saúde permite a redução de doenças graves, gerir preventivamente os riscos cibernéticos reduzirá significativamente a sua materialização.

Nesse âmbito, se as seguradoras passam a ter "a pele em jogo" quando emitem apólices de riscos cibernéticos, podem induzir ou mesmo apoiar seus clientes por meio de serviços de valor agregado focados no entendimento e preparação para riscos cibernéticos, fornecendo consultores de segurança, *compliance* e conformidade, técnicos de rede e *hardware*, especialistas em "anti-vazamento" etc. As apólices de seguro podem incentivar a contratação destes especialistas pelo segurado por mecanismos de precificação e recompensa.

Particularmente no Brasil, cujo Produto Interno Bruto é fortemente dependente de pequenas e médias empresas, este modelo é mais propenso a chamar a atenção do potencial segurado e, ao mesmo tempo que auxilia no cumprimento da LGPD, aproxima-o das seguradoras.

Um modelo de gestão de riscos cibernéticos estruturado em duas camadas — a parte inferior com a implementação de atividades rotineiras de incremento à segurança informacional e a parte superior com coberturas de danos (e de crise) raramente usadas — ajudaria a promover uma relação de confiança simbiótica entre seguradora e segurado. Ao mesmo tempo, criaria um ambiente virtuoso de identificação e tratamento dessa nova modalidade de risco. Invertendo a máxima de Thomas Gray: se ignorância não é uma benção, é salutar a sabedoria sobre os riscos cibernéticos.

[1] Fortiguard-labs. **Relatório de ciberataques no Brasil: 2021**. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021. Acesso em: 07.jun.2022.

[2] Tendência análoga é observada nos Estados Unidos, com perdas estimadas de US$ 6,9 bilhões somente em 2021. **Federal Bureau of Investigation – Internet crime report 2021**. Disponível em: efaidnbmnnnibpcajpcglclefindmkaj/https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf . Acesso em 08.jun.2022.

[3] **Lloyd's moves to address Silent cyber risk**. Disponível em: https://www.ciab.com/resources/lloyds-moves-to-address-silent-cyber-risk/. Acesso em: 09.jun.2022.

Fonte: https://conjur.jumps.com.br/2022-ago-01/pensando-lapis-riscos-ciberneticos-mercado-seguros-brasileiro/