A propósito da silent cyber coverage

Se por um lado afirma-se que os dados pessoais correspondem, no século 21, ao petróleo de outrora, por outro lado não há dúvida de que com os bônus vêm os ônus, ora representados por demandas de

as que podem ser deflagradas contra aqueles que os detenham.

Sem embargo das pretensões indenizatórias a serem apresentadas pelos titulares dos dados que, eventualmente, sejam violados, a possibilidade de que a as autoridades responsáveis possam, desde 1º de agosto deste ano, aplicar as duras sanções previstas na Lei Geral de Proteção de Dados (artigo 52 da Lei nº 13.709/2018 [1]), vem reforçar o risco de responsabilização e, a reboque, a necessidade de que seja verdadeiramente sedimentada uma cultura em torno da proteção dos dados.

Sob a perspectiva das espécies contratuais securitárias que dialogam com as questões acima assinaladas, a primeira a despertar a atenção é o chamado contrato de seguro para riscos cibernéticos — no jargão anglo-saxão, o *cyber insurance* —, o que se explica com naturalidade considerando que, muitas vezes, os vazamentos de dados, paralisação de funcionamento de servidores, colapso de *softwares* e *hardwares*, além de danos reputacionais etc. terão como origem, essencialmente, o ambiente virtual representado pela grande rede.

A primeira visada, como se afirmou, de fato conduz a questão concernente ao tratamento/proteção de dados pessoais ao chamado seguro para riscos cibernéticos, mas um exame um pouco mais aprofundado revela que, na realidade, esses riscos podem repercutir também para outras espécies securitárias.

Pode-se pensar, e.g., nos seguros E&O (erros e omissões — seguro de responsabilidade civil profissional), considerando tomadores cuja atividade fim seja a prestação de serviços de tecnologia. Imagine-se, assim, uma sociedade dedicada ao desenvolvimento de *softwares* que, uma vez concebidos e entregues a um determinado contratante, causem-lhe severos danos de ordem material. Parece bem nítido que, para essa hipótese, um seguro E&O seria mesmo o mais indicado à tutela dos interesses patrimoniais da referida empresa de tecnologia [2].

Prosseguindo, pode-se pensar nos seguros de responsabilidade civil geral para situações nas quais um determinado risco cibernético venha a causar danos materiais a terceiros. É iterativo aqui o exemplo proveniente de perdas relevantes ocorridas nos Estados Unidos da América, originados no estado do Texas e espraiados por quase toda a costa leste daquele país, quando *hackers* invadiram os sistemas de tecnologia de uma distribuidora de combustíveis, colapsando-os [3].

A terceira espécie que se deseja ressaltar é a dos seguros D&O — os seguros de responsabilidades concebidos para, entre outros, diretores e membros dos conselhos de administração e fiscal. Não se deseja empregar aqui um tom alarmista, mas o exame realizado em mercados seguradores mais desenvolvidos que o brasileiro revela que a questão atinente aos riscos cibernéticos deixou de ser, apenas, um problema das empresas para passar a ser um problema de suas diretorias e conselhos de administração [4].

Os riscos cibernéticos, na atualidade, segundo estudo elaborado pela OCDE, representam um enorme potencial de perdas que, com efeito, *devem* ocupar as pautas das diretorias e conselhos de administração. A atualidade e relevância do tema requer que medidas sejam tomadas com o objetivo de implementar sistemas de segurança da informação/dados e, mais do que isso, zelar pelo seu funcionamento adequado ao longo do tempo [5]. Diante do cenário atual e de tudo o que vem sendo ventilado a respeito da matéria, é inegável o dever de cautela a ser diligentemente adotado pelas administrações de empresas, a buscar junto a especialistas (à luz do princípio do *rely on others*) a consultoria técnica mais adequada para a proteção do interesse social desses riscos cibernéticos e seus impactos. A ausência de diligência nesse contexto pode levar à responsabilização do administrador pelos danos causados.

Podem ser observadas nos Estados Unidos, na Europa, no Reino Unido e na Ásia diversas ações coletivas (*class actions*) fundamentadas, justamente, em violações aos sistemas de proteção de dados de usuários/consumidores, propostas contra diretores e conselheiros [6]. E não se está aqui a afirmar que os requeridos são, exclusivamente, os DPOs (*data protection officers*), isto é, os encarregados designados para essa função a teor do disposto no artigo 41 da Lei Geral de Proteção de Dados. As grandes sociedades abertas, comumente, disporão dos CROs — *chief risk officers* ou, também, dos diretores responsáveis pela tecnologia da informação [7]. Tudo isso, sem contar com a possibilidade de, nas companhas brasileiras, administradores serem chamados a responder por atos de outros administradores, na forma dos parágrafos 1º a 4º do artigo 158 da Lei das SA [8].

O título da presente coluna remete à chamada *silent cyber coverage*, temática que, na Europa e nos Estados Unidos da América, vem despertando a atenção de seus mercados de seguros e resseguro de uma maneira bem ampla. Sinteticamente, entende-se por *silent cyber coverage* a constatação segundo a qual um determinado programa de seguros do tomador não afirme, categoricamente, nem pela existência de cobertura para riscos de ordem cibernética, tampouco pela inexistência, ou seja, nota-se, de fato, um *silêncio* bem preocupante.

A oposição à *silent cyber coverage* seria a *affirmative coverage*, isto é, em vez de detectar-se uma ambiguidade, o conteúdo contratual concebido pelas partes primaria pela clareza quanto à efetiva cobertura ou exclusão dos riscos de origem cibernética [9].

Retomando a abordagem relacionada à interseção entre os riscos cibernéticos e a responsabilidade de administradores, a realidade vem revelando uma busca cada vez maior por parte de administradores participantes dessa arena tecnológica por seguros D&O que sejam capazes de lhes oferecer garantias tais como, e.g., antecipação de custos de defesa, danos à reputação/imagem, cobertura para multas impostas pelas autoridades responsáveis e, também, eventuais indenizações a serem pagas a terceiros decorrentes de problemas de ordem cibernética [10].

Sugere-se, assim, um olhar com redobrada atenção aos programas de seguros contratados pelas tomadoras e, de igual sorte, que as seguradoras revisitem os seus programas de resseguro, tudo com o objetivo de evitar a chamada *silent cyber coverage* e seus efeitos deletérios por ocasião das regulações/liquidações de sinistros.

Concluindo, deseja-se estabelecer um rápido paralelo que o mercado segurador brasileiro observou entre os ramos ambiental e D&O, possivelmente útil àquilo que, com efeito, provavelmente ver-se-á no curto/médio prazo com os ramos cyber e D&O.

Sintetizando temas complexos, o que se justifica pelos limites desta coluna, as tragédias ambientais de Mariana e Brumadinho, ocorridas em Minas Gerais, ocasionaram a perda de valor mobiliário das ações da mineradora responsável pelos sítios respectivos. A segunda catástrofe, em particular, trouxe à tona discussão acalorada a respeito da responsabilidade (ou não) de diretores e membros do conselho de administração da companhia, ao argumento de que poderiam/deveriam ter tomado medidas a fim de evitar o mau maior.

Verificou-se, à época, portanto, demandas típicas da arena dos seguros D&O motivadas por questões de fundo ambientais, ou seja, uma clara convergência entre os dois ramos. Ditas demandas de responsabilidade deveriam ter sido alocadas nos seguros D&O ou nos seguros ambientais — seguro de responsabilidade ambiental ou seguro ambiental típico?

A probabilidade de que inquietações como a acima referida também se apresentem agora com relação aos seguros *cyber* e D&O é concreta, cabendo aos segurados/tomadores, seguradores e resseguradores, além dos *brokers*, a serenidade para que tomem a decisões corretas no tocante às coberturas/alocações/exclusões. Deve-se a todo custo evitar a *silent cyber coverage*, e, consequentemente, todos os desgastes que a mesma, fatalmente, ocasionará.

[1] "Artigo 52 – Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I – advertência, com indicação de prazo para adoção de medidas corretivas; II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração […]".

[2] Curioso notar que, na origem, os seguros cibernéticos estiveram mesmo relacionados aos seguros de responsabilidade civil profissional: "Cyber insurance coverage has been available since the late 1970s. The market evolved from the technical risks/technical errors and omissions (E&O) sector. The 1980s saw the introduction of the first tech E&O insurance policies, which included cybersecurity insurance and were developed primarily for financial institutions as well as blue chip companies. The development and launch of cyber insurance as a stand-alone product was a response to the Y2K problem and was intended to close existing gaps in the insurance coverage of traditional property and casualty policies." (WREDE, Dirk et all. *Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market.* Disponível em The Geneva Papers on Risk and Insurance – Issues and Practice (2020), p. 660. https://doi.org/10.1057/s41288-020-00183-6, visitado em 27.09.2021).

[3] Há vasto noticiário a respeito: "Colonial hack: How did cyber-attackers shut off pipeline?" Disponível em https://www.bbc.com/news/technology-57063636.amp, visitado em 08.09.2021 e "Extreme weather is the culprit in the Texas power crisis, but that's not our worst problem", disponível em https://amp.usatoday.com/amp/4491652001, visitado em 08.09.2021.

[4] "On the flip-side, however, the day may come when the perceptions of regulators and investors change. Although cyber-attacks will undoubtedly continue to plague the business world, stakeholders will take increasingly closer looks at what was done to minimize the harm at the top." (YELLEN, Rob. *D&O risk in the age of cyber insecurity*. Disponível em https://www.willistowerswatson.com/en-US/Insights/2017/06/d-o-risk-in-the-age-of-cyber-insecurity, visitado em 20.09.2021).

[5] "Directors and Officers liability policies: Companies impacted by a significant cyber incident with implications for business performance could face lawsuits from shareholders over the role of company executives or the company's board in ensuring appropriate management of cyber risks (including response to a breach and, for US public companies, the level of risk disclosure relative to the SEC's disclosure guidance) – although so far, such lawsuits have rarely led to findings or settlements in favour of shareholders in the United States. In New York State, a director or senior officer of a financial institution is now required to certify compliance with the state's Cyber Security Requirements for Financial Services Companies which could provide a new avenue for shareholder claims". (OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris. p. 79. Disponível em http://dx.doi.org/10.1787/9789264282148-en, visitado em 03.09.2021).

[6] "The importance of this issue outside of the United States is likely to increase due to: (i) the spread of securities (and other) class action lawsuits to the United Kingdom, continental Europe and countries in Asia; (ii) the recent precedent of large (USD 1 billion) directors and officers settlements in the United Kingdom; and (iii) the implementation of the General Data Protection Regulation (GDPR) in 2018 which should lead to more widespread publication of data confidentiality breaches in Europe. The GDPR requires the establishment of a Data Protection Officer with responsibilities that could lead to liability and some insurers have accordingly extended their definition of insured persons to include Data Protection Officers." (*Ibid*, p. 79-80).

[7] Lei nº 13.709/2018. artigo 41. "O controlador deverá indicar encarregado pelo tratamento de dados pessoais. […]".

[8] Sobre o tema, vide os parágrafos 1º a 4º do artigo 158, LSA: "[…] §1º. O administrador não é responsável por atos ilícitos de outros administradores, salvo se com eles for conivente, se negligenciar em descobri-los ou se, deles tendo conhecimento, deixar de agir para impedir a sua prática. Exime-se de responsabilidade o administrador dissidente que faça consignar sua divergência em ata de reunião do órgão de administração ou, não sendo possível, dela dê ciência imediata e por escrito ao órgão da administração, no conselho fiscal, se em funcionamento, ou à assembléia-geral. § 2º Os administradores são solidariamente responsáveis pelos prejuízos causados em virtude do não cumprimento dos deveres impostos por lei para assegurar o funcionamento normal da companhia, ainda que, pelo estatuto, tais deveres não caibam a todos eles. § 3º Nas companhias abertas, a responsabilidade de que trata o § 2º ficará restrita, ressalvado o disposto no § 4º, aos administradores que, por disposição do estatuto, tenham atribuição específica de dar cumprimento àqueles deveres. § 4º O administrador que, tendo conhecimento do não cumprimento desses deveres por seu predecessor, ou pelo administrador competente nos termos do § 3º, deixar de comunicar o fato a assembléia-geral, tornar-se-á por ele solidariamente responsável".

[9] Há vasta literatura a propósito da *silent cyber coverage*. Exemplificativamente, remete-se a LACROIX, Kevin M. Addressing "Silent Cyber" and the Risk of Coverage Gaps. January 20, 2020. Disponível em https://www.dandodiary.com/2020/01/articles/cyber-liability/addressing-silent-cyber-and-the-risk-of-coverage-gaps, visitado em 27.09.2021.

[10] "Riscos cibernéticos na pandemia e LGPD aceleram Cyber Seguros e D&O". Disponível em https://www.revistaapolice.com.br/2021/02/riscos-ciberneticos-na-pandemia-e-lgpd-aceleram-cyber-seguros-e-do/#:~:text=Riscos%20cibern%C3%A9ticos%20na%20pandemia%20e%20LGPD%20aceleram%20Cyber%
., visitado em 22.09.2021.

Date Created
30/09/2021