Exclusão de cobertura para guerra cibernética

A contemporaneidade revela que o nosso entendimento a propósito do conceito de guerra vem sendo seriamente ampliado. Se, para fins de boa compreensão, admitir-se a existência das guerras física (presencial) e cibernética (deflagrada no ambiente tecnológico), não há dúvida de que o potencial lesivo [illegible]uas modalidades é mesmo terrível.

Para além da guerra e suas perdas respectivas, parecem caminhar conjuntamente as questões relativas ao terrorismo e à extorsão, a agravar ainda mais essa quadra de severos prejuízos. Embora um ataque terrorista não seja, *prima facie*, decorrente do que se possa entender por "estado de guerra", as suas consequências são equiparáveis. E, no ambiente cibernético, ganham notoriedade cada vez maior os pedidos de resgate formulados por criminosos a fim de restituir o acesso aos dados indisponibilizados por meio de s*oftwares* maliciosos (*ransomware*).

A literatura especializada, inclusive, no que se refere ao potencial lesivo dos ataques cibernéticos, já chegou a equipará-los a perdas sofridas pela humanidade como consequência de catástrofes nucleares [1] .

Antes de, propriamente, debater a exclusão de cobertura para terrorismo, extorsão e guerra nas apólices de seguros, entende-se pertinente percorrer o racional empregado por um determinado subscritor de risco no sentido de cobri-lo, ou de decliná-lo. Em geral, a absorção de um risco requer, por parte de uma seguradora, certa dose de previsibilidade e estatística (atuária). Tome-se, *e.g.*, o número de acidentes de automóveis ocorridos na zona sul da cidade do Rio de Janeiro, entre condutores de 30 a 40 anos de idade, do gênero masculino. Por mais que, individualmente, haja aleatoriedade no tocante à ocorrência do sinistro, o exame de um conjunto de amostras possui grande dose de assertividade, a permitir, como se comentou, elevadas margens de previsibilidade tendo em conta os parâmetros frequência e severidade [2].

Quando se tem em mente as consequências decorrentes de uma guerra, física ou cibernética, praticamente não há dados que permitam um exame mais assertivo, no sentido de poder comparar e, assim, prever perdas futuras. Há enormes dificuldades para quantificar as contingências financeiras decorrentes, por exemplo, da Guerra da Coreia (1950-1953), da Guerra do Golfo (1990-1991), da Invasão do Iraque (2003), ou, mais recentemente, da Guerra entre Rússia e Ucrânia (2022). E, na exata medida em que falta estatística/previsibilidade, mais refratária será a indústria do seguro à subscrição de riscos dessa natureza.

É com esse raciocínio que contratos de seguros os mais diversos comumente excluem a cobertura para guerra, terrorismo ou extorsão, tendo como norte as chamadas guerras físicas. Com o advento das chamadas guerras cibernéticas, esse padrão de comportamento estaria a sofrer mudanças dignas de notas?

Em meados de 2017, um ataque cibernético ganhou notoriedade a nível global. Chamado de *Petya* ou *NotPetya*, esse terrível vírus se espalhou quase que de maneira instantânea pela França, Alemanha, Itália, Polônia, Estados Unidos, além de Rússia e Ucrânia. As perdas foram contabilizadas em mais de US$ 10 bilhões, espraiando-se em *1st party* (sofridas pelos próprios segurados) e *3rd party* (sofridas por terceiros), decorrentes da inutilização de *hardware* e *software*, interrupção de negócios, vazamento e perda de dados etc. Especulou-se que a iniciativa tenha sido engendrada pelo governo russo, que, por sua vez, sempre negou a autoria [3].

No que diretamente interessa à presente coluna, as perdas sofridas pela Mondelez International Inc., uma das maiores companhias de alimentos de mundo, foram estimadas em mais de US$ 100 milhões. O referido vírus se instalou em seus sistemas de TI e, quase que automaticamente, causou a perda de 1.700 servidores, além de 24 mil laptops. Conhecida seguradora global foi responsável pela emissão de uma apólice *all risks property* à segurada, ou seja, não fora requisitada a emissão de um seguro típico para riscos cibernéticos [4].

Avisado e regulado o sinistro pela seguradora, a conclusão foi pela negativa de cobertura, essencialmente com fincas em cláusula contratual que excluiu os riscos relacionados à guerra, nos seguintes termos:

"This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss:

2) (a) ***hostile or warlike action in time of peace or war****, including action in hindering, combating or defending against an actual, impending or expected attack by any: (i)* ***government or sovereign power (de jure or de facto)****; (ii) military, naval, or air force; or (iii) agent or authority of any party specified in I or ii above."* (Grifou-se)

Das partes acima realçadas, interessante observar que o conteúdo da cláusula excludente é amplo, a compreender atos hostis e assemelhados à guerra tanto em tempos de paz quanto em tempos de guerra; na sequência, atos por iniciativa de órgão de governo ou de organização soberana de fato ou de direito, isto é, independentemente de reconhecimento formal, também acrescentam densidade à exclusão.

Segundo interessante artigo elaborado por Dominic T. Clarke [5], esta teria sido a primeira oportunidade na qual uma seguradora teria invocado a exclusão de cobertura guerra (leia-se, para guerra "física") para negar indenização derivada de ataque cibernético, a revelar, portanto, o ineditismo do tema.

Debates a propósito do alcance da exclusão de cobertura para guerra não são novos nos Estados Unidos. Clarke menciona, *e.g.*, o caso *Vanderbilt v. Travelers' Insurance Company*, julgado em 1920 [6]. Um navio britânico, quando fazia a travessia de Nova York a Liverpool, fora atingido por projétil proveniente de um submarino alemão, vindo a naufragar. A discussão se referiu ao alcance da exclusão de cobertura para guerra no âmbito de uma apólice de seguro de vida de um dos viajantes que se encontrava a bordo da embarcação.

Embora os Estados Unidos da América não tenham formalmente participado da 1ª Guerra Mundial, a Corte de Justiça de Nova York entendeu que o navio afundou como consequência de um ato de guerra, prestigiando, portanto, a cláusula contratual desafiada.

De maneira mais refinada, as perdas relacionadas aos ataques à base americana de Pearl Harbour, no Havaí (dezembro de 1941), um pouco antes do ingresso formal daquele país na 2º Grande Guerra, motivaram acalorados debates a respeito do que deveria ser entendido por atos de guerra (*acts of war*) e estado de guerra (*state of war*). Em *Gladys Ching Pang v. Sun Life Assurance Co. of Canada* [7], a demanda foi proposta por beneficiário de seguro de vida de um bombeiro que acabou morto pelo ataque à referida base. Segundo os termos da apólice, eventos fatais causados de maneira acidental motivariam o recebimento do dobro do capital segurado, sem embargo da existência de cláusula contratual que excluía a cobertura em caso de guerra declarada.

No caso, como o ataque à Pearl Harbor justamente antecedeu o ingresso formal dos Estados Unidos na guerra, ou seja, ainda não havia guerra declarada, a Corte do Havaí entendeu pela procedência da pretensão do beneficiário, designadamente porque não havia que se confundir um ato de guerra (*act of war*) com o estado de guerra (*state of war*) [8].

Passando a refletir a propósito da exclusão para guerra, terrorismo e extorsão no ambiente cibernético, pode-se intuir que as apólices por assim dizer genéricas, para riscos nomeados (um seguro *property*, abstratamente considerado), não estão preparadas para lidar com riscos dessa magnitude. Até a data de publicação desta coluna, não se tem notícia do julgamento do caso *Mondelez vs Zurich*; nada obstante, se essa mesma temática fosse endereçada aos tribunais brasileiros, parece razoável assumir que as partes não imaginaram, por ocasião da concepção do contrato, que os riscos para guerra cibernética estariam cobertos (Código Civil, artigos 112 e 113).

Por outro lado, no contexto de um seguro próprio para riscos cibernéticos, o exame do tema requer uma atenção diferenciada. Mesmo considerando as chamadas guerras físicas, é preciso ter em mente que, há tempos, organizações não estatais motivam perdas próprias às chamadas guerras convencionais. Considerando que uma organização terrorista, ao menos em tese, não possui laços com governos formalmente estabelecidos, uma exclusão para guerra baseada na necessidade de seu reconhecimento formal por governo parece dissociada da realidade que já se mostra presente.

No contexto das chamadas guerras cibernéticas, essa realidade cambiante mostra-se ainda mais latente. Que grupo anônimo — ou, melhor dizendo, "Anonymous", parafraseando a mais conhecida e temida organização coletiva com vistas aos ataques cibernéticos, deixará rastros, isto é, divulgará o governo ou organização a que pertence, por ocasião de seus ataques [9]?

O alerta da OCDE é incontestável. Os riscos cibernéticos se qualificam como a principal ameaça à sociedade em que vivemos. Sob a perspectiva dos riscos e coberturas para guerra, terrorismo e extorsão nesse ambiente, é preciso repensá-los com a gravidade e a atualidade exigidas [10].

[1] *"This was not, however, the work of regular criminal hackers. The CIA believed the attacks to have been a Russian state-sponsored attack on Ukraine. It concluded with a high degree of confidence that the Russian GRU military spy agency created NotPetya with the goal of disrupting Ukraine's financial system. The military hackers used malware that appeared to be ransomware, which encrypts data and decrypts it only if a ransom is paid, to make it appear as though criminal hackers were responsible rather than a nation state. Because of this deception, it took days to understand that NotPetya was permanently deleting data. The result was more than $10 billion in damage, according to Tom Bossert, a United States Homeland Security adviser at the time of the attacks. While there was no loss of life, Bossert characterised the attacks as being 'the equivalent of using a nuclear bomb to achieve a small tactical victory'."* (GREENBERG, Andy. *The untold story of NotPetya, the most devastating cyberattack in history*. Disponível em: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-codecrashed-the-world/. Visitado em 2/6/2022.

[2] O que remete à clássica lição do matemático suíço Jacob Bernoulli e à conhecida "Lei dos Grandes Números", tão importante à ciência atuarial e à atividade securitária.

[3] NAKASHIMA, Ellen. *Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes.* Disponível em: The Washington Post https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes., visitado em 2.6.2022.

[4] Para mais informações a respeito do caso, consulte-se: https://www.databreachninja.com/wp-content/uploads/sites/63/2019/01/MONDELEZ-INTERNATIONAL-INC-Plaintiff-v-ZURICH-AMERICAN-INSURANCE-COMPANY-Defenda.pdf

, visitado em 2/6/2022.

[5] CLARKE, Dominic T. *Cyber Warfare and the Act of War Exclusion*. International Comparative Legal Guides. Insurance & Reinsurance 2020. 9th ed., p. 11-16.

[6] https://casetext.com/case/vanderbilt-v-travelers-insurance-co, visitado em 1/6/2022.

[7] Conforme: https://casetext.com/case/pang-v-sun-life-assur-co-of-canada?q=Gladys%20Ching%20Pang%20v.%20Sun%20Life%20Assurance%20Co.%20of%20Canada&so , visitado em 1/6/2022.

[8] Vale dizer que, segundo relato de Dominic Clarke, pouco tempo depois a Corte de Apelações de Nova Iorque entendeu que, nada obstante o não ingresso formal dos Estados Unidos na 2ª Grande Guerra, à época do ataque à base de Pearl Harbour já havia o chamado estado de guerra. Nesse sentido: *New York Life Insurance Company v. Bennion*, disponível em https://casetext.com/case/new-york-life-ins-co-v-bennion, visitado em 1/6/2022.

[9] Para uma referência ao indigitado grupo, veja-se: https://tecnoblog.net/responde/qual-a-origem-e-historia-do-grupo-anonymous/, visitado em 1/6/2022.

[10] OECD. *Enhancing the Role of Insurance in Cyber Risk Management*. Paris: OECD Publishing, 2017. Disponível em http://dx.doi.org/10.1787/9789264282148-en, visitado em 2/6/2022.

Meta Fields