

Por Antonio Penteado Mendonça



De repente o planeta acordou de ponta cabeça com um ataque cibernético que atingiu mais de 150 países. Alguns lugares sofreram danos sérios, outros foram chantageados, o mercado de moeda eletrônica foi afetado, redes de todos os tamanhos foram desligadas para impedir o ataque, bilhões de dólares deixaram de circular, enfim, a economia, a segurança e o conforto de grande parte da humanidade sofreu danos mais ou menos graves.

Quem fez isso? Quem conseguiu a proteção que salvou o mundo? Será que houve isso? Será que ainda temos consequências escondidas dentro das máquinas, esperando a hora certa para darem o novo bote? São muitas perguntas e poucas respostas. Depois do ataque, a imprensa comentou, as redes sociais expressaram a opinião de milhões de pessoas, o medo se fez presente para, lentamente, ser esquecido e hoje ninguém mais fala do assunto porque outros escândalos, outras tragédias, outros eventos já substituíram o ataque cibernético.

Se há poucos anos alguém tinha 15 minutos de fama, atualmente, com as comunicações em tempo real, as redes sociais, as várias formas de transmissão de dados, o máximo que alguém pode almejar é menos do que 5 minutos, e isso se a tragédia for muito grande.

Mas o ataque cibernético levanta algumas questões importantes que não foram respondidas ou, pelo menos, as respostas não foram divulgadas. Quem foi o responsável? Foi uma ação coletiva? Se sim, coordenada por quem? Não foi uma ação coletiva? Foi o quê?

Tão importante quanto, quais os danos máximos que algo no gênero pode causar às sociedades atacadas? Será que existe alguém que pode ser responsabilizado pelos danos, ainda que não tendo sido o seu causador?

É possível se falar em responsabilidade civil numa situação estas? Se sim, quem pode ser responsabilizado? Ou será que o evento se enquadra nos chamados casos fortuitos ou atos de Deus?

Mas como incluir um ataque cibernético no rol dos casos independentes da vontade do ser humano se ele é causado por seres humanos? E a responsabilidade objetiva, será que não pode ser invocada para o ressarcimento de prejuízos decorrentes do ataque em função de alguém de alguma forma ser responsável por alguma parte do sistema que gerou o prejuízo?

Será que o provedor de internet pode ser responsabilizado? Será que o operador de uma rede social pode ser responsabilizado? Será que alguém que deveria fazer uma entrega urgente, que não é feita em função do ataque, pode ser responsabilizado?

As questões são as mais diversas e extremamente abrangentes. O risco é novo, há pouca

experiência sobre o assunto e, no entanto, os prejuízos possíveis atingem bilhões, ou mesmo trilhões de dólares.

É evidente que as seguradoras e resseguradoras estão seriamente preocupadas. Danos decorrentes de eventos desta natureza não são mais ficção, estão aí, aconteceram, atingiram pessoas, governos, empresas e organizações de todas as naturezas. Os prejuízos diretos e indiretos são reais e podem atingir somas expressivas.

Os clausulados mais comuns cobrem ou excluem situações como esta? No caso de silêncio do texto, como deve ser feita a interpretação das coberturas? Os seguros para riscos cibernéticos atuais são suficientes para fazer frente ao risco? Os cálculos atuariais estão corretos e o prêmio está taxado de acordo com a realidade? As garantias estão corretamente formuladas? As exclusões são as mais indicadas? São exageradas? São insuficientes? O mercado tem capacidade para assumir as perdas decorrentes de outro ataque global em proporções ainda maiores? Os governos estão adotando as medidas de proteção a seu cargo? As empresas diretamente envolvidas com o funcionamento e distribuição da rede estão implementando as ações necessárias a evitar a propagação dos danos?

Todas estas questões mostram a falta de preparo do planeta para lidar com o que aconteceu. A fragilidade das defesas ficou evidente. O ataque foi um sucesso e abre caminho para outros ataques mais devastadores. Será que estaremos preparados?

**Fonte:** O Estado de S. Paulo, em 05.06.2017.