Seguro de riscos cibernéticos

MODERADOR: LAURO VIEIRA DE FARIA (ENS)

Como é evidente, a tecnologia da informação tornou-se fator essencial para a vida cotidiana em nossas sociedades. No entanto, os enormes benefícios que confere vêm em par com riscos significativos relacionados à segurança, integridade e falha de diversos processos inerentes a sua natureza, o chamado risco cibernético.

PARTICIPARAM DOS DEBATES

- ***Camila Leal Calais,*** *formada em Direito pela Instituição Toledo de Ensino, membro da Associação Internacional de Direito de Seguros (AIDA) e sócia no escritório Mattos Filho, Veiga Filho, Marrey Jr. e Quiroga Advogados.*
- ***Flávio Sá,*** *administrador de empresas pela Universidade Presbiteriana Mackenzie, com extensa experiência em seguros de responsabilidade civil profissional (erros & omissões), D&O (responsabilidade civil dos administradores) e Riscos Cibernéticos e gerente de seguros de linhas financeiras da AIG Brasil.*
- ***Giseli Giusti Tilger,*** *bacharel em Gestão Ambiental, com MBA em Gestão e Tecnologias Ambientais, ambos pela USP, e subscritora de Casualty Insurance na Munich Re do Brasil.*
- ***Paulo Marcos Rodrigues Brancher,*** *mestre em Direito Civil Comparado e doutor em Direito Econômico pela PUC-SP, membro e codiretor do Comitê de Proteção de Dados da International Technology Law Association (ITechLaw) e sócio no escritório Mattos Filho, Veiga Filho, Marrey Jr. e Quiroga Advogados.*
- ***Thales Dominguez Barbosa da Costa,*** *formado em Direito pela Faculdade de Direito de São Bernardo do Campo, pós-graduado pela Escola Paulista de Direito e advogado na Mattos Filho, Veiga Filho, Marrey Jr. e Quiroga Advogados.*

Em escala crescente e num mundo cada vez mais conectado, o risco cibernético tem o poder de restringir o impulso benéfico da tecnologia e afetar adversamente a economia internacional. Essa evolução significa que a confiabilidade da conectividade digital como força motriz para o crescimento econômico e o desenvolvimento social está agora em perigo. Como sempre, o setor de seguros terá cada vez mais papel fundamental na sua abordagem e gerenciamento.

Os desafios, entretanto, são grandes, desde a possibilidade de o risco cibernético se manifestar de modo sistêmico até a dificuldade mesma de avaliação dos valores em risco. Foi pensando nesses novos panoramas e tendo em vista a recente Lei Geral de Proteção de Dados que a revista Cadernos de Seguro entendeu ser oportuno organizar uma mesa-redonda sobre o tema com especialistas experientes e altamente competentes do mercado de seguros nacional.

Cadernos: Esta é uma mesa-redonda sobre riscos e seguros cibernéticos e, em nome da Escola Nacional de Seguros, agradeço muitíssimo a presença de vocês, que são especialistas gabaritados no assunto. Para iniciar, dou a palavra ao Flávio, que gentilmente nos disponibilizou as instalações da AIG, e gostaria de perguntar como está o mercado de seguros cibernéticos no Brasil e quais são as suas perspectivas.

Flávio: A AIG oferece o seguro cibernético no Brasil desde 2012. Globalmente, e também nacionalmente, a AIG foi a seguradora pioneira nesse tipo de proteção. Lançar esse produto localmente era muito mais uma iniciativa de tentar explicar esse risco, que há alguns anos era difícil de tangibilizar. Isso até para grandes empresas, que tinham o desafio de mensurar as exposições aos riscos que possuíam com ativos digitais e quais eram os riscos que a seguradora poderia absorver. Ainda mais porque o Brasil não tinha uma legislação específica sobre o tema. Havia fundamentos legais, mas não uma proposta clara como existe na atualidade, com o Marco Civil da Internet e mais recentemente com a a Lei Geral de Proteção de Dados, que entra em vigor em fevereiro de 2020.

No início, apresentávamos às empresas casos de sinistros que tinham ocorrido na Europa e nos EUA, logo, sob outras legislações. Apesar de no Brasil existirem casos similares, estes não eram públicos ou então pouco divulgados. Entretanto, no ano de 2017, houve ataques cibernéticos globais, em particular, o do *ransomware* (extorsão cibernética) chamado *"WannaCry"* e o *"NotPetya"*. Episódios como esses foram emblemáticos e ajudaram o mercado de seguros e as empresas a tangibilizar um tipo de risco cibernético, aliás, dos mais simples, mas com consequências que podem ser severas.

O ocorrido despertou então o interesse dos corretores e dos clientes em entender o risco, e tal atitude tem crescido significativamente. A aprovação da GDPR, ou seja, da *General Data Protection Regulation*, que é a legislação europeia, vigorando desde 25 de maio de 2017, impactou clientes em nosso país e aumentou a busca por apólices para a transferência do risco ao mercado segurador. Apesar de a legislação brasileira não estar ainda em vigor, percebe-se uma preocupação maior com essa proposta, porque seu delineamento terá caraterísticas locais.

Ajudaram também nesse processo casos emblemáticos de vazamento de dados em que o Ministério Público vem atuando, mesmo sem a legislação específica estar em vigor, e obrigando as empresas a notificarem o usuário final que seus dados foram vazados. Para realizar essa notificação há gastos e uma determinada estrutura de que a empresa precisa dispor, e isso tem também cobertura na apólice.

É uma área de seguros ainda em expansão, mas com evolução rápida e positiva nos últimos anos, como o seguro de responsabilidade dos administradores, o D&O, ou o seguro ambiental, que são relativamente novos no país. Porém, o seguro cibernético tem potencial de crescer de forma muito mais rápida. Ele é disperso, está em todas as operações, de todas as empresas. Quando consultamos os *Risk Managers* sobre as maiores preocupações das companhias, surge sempre o risco cibernético. No mundo todo ele está no topo, como 1º, 2º ou 3º colocado, e isso incentiva o mercado de seguros a se adaptar, fornecendo cobertura.

Camila: É interessante você falar isso, **Flávio,** porque o risco cibernético tem um potencial de geração de perdas que sequer conseguimos mensurar, e o evento com maior incidência pode ser aquele que ainda não aconteceu. Considerando nossa evolução tecnológica, talvez sempre estejamos um passo atrás. Não temos como verificar precisamente as exposições ou valores em risco, pois estes são muito diferentes dos riscos de *property* e outros. Logo, a transferência de risco para a seguradora nunca vai ser 100% porque talvez não haja cobertura para o que vier a ocorrer no futuro.

> ***"Quando consultamos os Risk Managers sobre as maiores preocupações das companhias, surge sempre o risco cibernético.***
>
> *No mundo todo ele está no topo, como 1º, 2º ou 3º colocado, e isso incentiva o mercado de seguros a se adaptar, fornecendo cobertura."*

FLÁVIO SÁ

Essa é uma preocupação geral. Algo que vemos hoje como inofensivo, por exemplo, um tipo de vírus, pode ser capaz de quebrar uma empresa daqui a cinco anos.

Cadernos: Isso remete à questão da precificação. É difícil precificar esse risco?

Camila: A precificação vai se basear no que é mensurável e em quanto a seguradora quiser tomar de risco. O risco puro dificilmente será segurado, porque ainda não temos consciência dos limites de perdas.

Giseli: Um exemplo é o *WannaCry*, que aconteceu no ano passado e impactou mais de 150 países e muitas empresas. Conseguiu-se um software com a finalidade de reverter seus danos. Porém, já há expectativa de uma nova versão desse tipo de vírus e que será de controle ainda mais difícil.

Cadernos: Vocês podem descrever o que foi especificamente esse vírus?

Giseli: Foi um tipo de *malware*, isto é, um vírus que se autorreproduz e cujo objetivo era a extorsão. Os criminosos pediram de US$ 300 a US$ 600 por sistema ou dispositivo, e davam prazo para pagamento.

Flávio: Os prazos eram de 3, 6 e 7 dias para a pessoa ou empresa pagarem. Em até três dias, o valor era US$ 300, e em até seis dias subia para US$ 600. Se o usuário não pagasse em sete dias, perdia os dados. O pagamento era em *bitcoins* e o impacto foi muito grande.

Paulo: É importante ouvir isso, porque percebemos que a economia, o comportamento, tudo migra para o digital. Um exemplo é o quanto nossa vida hoje depende muito menos de visitar agências bancárias. Está tudo à mão, quase não é mais preciso entrar em filas. Cada vez mais concentramos todos os nossos dados e informações valiosas no ambiente digital. É para ele que vão os principais riscos, e onde tem valor certamente tem gente querendo destruí-lo ou dele se apropriar. Conforme falamos, um vírus utilizado em larga escala deixa muito claro que a empresa precisa ter sistemas de segurança e também garantias, para si mesma e seus usuários.

Isso me lembra o caso Facebook - Cambridge Analytica, que envolveu a coleta não autorizada de informações de 87 milhões de usuários: quando o escândalo foi revelado e se viu o que poderia ser feito com os dados, aconteceu uma desvalorização brutal das ações da empresa. Isso também é um risco do ambiente cibernético e que não tem nada a ver com ataque de *hacker*, mas com a maneira como uma companhia protege os dados e com sua forma de fazer negócios.

Flávio: No mercado de seguros, conforme falamos, a questão é como mensurar o risco. De maneira simples, costumamos separar os riscos da própria empresa segurada, aqueles chamados de "riscos de primeira parte", dos riscos de responsabilidade civil ou de danos causados a terceiros. No risco de responsabilidade civil tradicional é preciso avaliar a exposição que pode afetar esses terceiros, que é algo muito subjetivo, ainda mais no mundo digital. Esse é um dos desafios para clientes e corretores analisarem qual a exposição cibernética.

Camila: Esse risco é curioso, porque é tanto de primeira parte quanto de terceira parte. No risco cibernético existem vários casos. Por exemplo: danos sofridos pelo próprio segurado e danos causados a terceiros pela possível violação de sistema desse segurado. Vemos muito no seguro cibernético a ênfase na cobertura de responsabilidade civil, mas obviamente ele não se resume a RC. Redes inteiras podem ser destruídas, entre outros prejuízos. Fala-se da possibilidade de um ataque cibernético em automóveis de última geração, podendo afetar, claro, a vida do motorista. Que seguro será levado em conta nesse caso: o de vida ou o *cyber*?

Flávio: A grande discussão nas seguradoras é como bem caracterizar o risco cibernético. Hoje, no mercado, há seguro para riscos intangíveis, como o prejuízo causado pelo vazamento de um banco de dados, ou então o custo para a recuperação de um banco de dados que foi corrompido por um ataque cibernético ou mesmo o lucro cessante que foi causado pela interrupção da rede do cliente. Mas existem também as perdas físicas (ou tangíveis), ligadas a pessoas ou a propriedades. Quando se separam esses dois grandes universos, a questão é se o seguro *cyber* vai ser analisado por todas as áreas de negócio da companhia, como seguro de propriedade, de responsabilidade civil, seguro de vida, de automóvel, ou se vai haver um setor que consiga analisar riscos cibernéticos em todos os seguros. É uma grande indagação e o mercado ainda está se adaptando para respondê-la.

Camila: É um risco muito disruptivo, não só no lado cibernético, mas até na operacionalização da seguradora que irá tomar o risco.

Flávio: Sim, e existe a dúvida sobre se o *underwriter* está preparado para analisar o risco cibernético, que é perene e vai encostar em todas as áreas da seguradora. A depender do setor, é difícil imaginar o tipo da responsabilidade a ser assumida. Por exemplo: o *WannaCry* afetou hospitais, mas as pessoas continuaram a precisar de atendimento. Se o acesso a prontuários eletrônicos for interrompido, o hospital deve encontrar outra maneira de continuar a atender os pacientes. Dependendo da efetividade do plano de

> ***A precificação vai se basear no que é mensurável e em quanto a seguradora quiser tomar de risco.*** *O risco puro dificilmente será segurado, porque ainda não temos consciência dos limites de perdas."*

CAMILA LEAL CALAIS

continuidade de negócio, pode vir a paralisar sua operação, causando inúmeras consequências aos pacientes. A apólice de risco cibernético pode auxiliar o segurado a recuperar os dados destruídos pelo *ransomware*, além de amparar o lucro cessante pela paralização do sistema. Consultando a cobertura de lucros cessantes da apólice tradicional de *property*, o segurado perceberá que esse risco provavelmente estaria excluído e que não há cobertura.

Paulo: Atualmente, na legislação, há padrões em termos de Marco Legal e responsabilização. A Lei 13.709/2018 (Lei Geral de Proteção de Dados, ou LGPD) teve uma inspiração consumerista em larga escala. Com base na visão do Ministério Público foi feito um trabalho muito grande na Secretaria Nacional do Consumidor (SENACOM) e muito do que prevê a lei tem forte semelhança com o Código de Defesa do Consumidor. Para o titular do dado que sofreu uma violação existe o direito de acionar tanto quem coletou a informação como quem a processou – que pode ter sido até um terceiro, pode ser o local de armazenamento, uma *cloud*, enfim, agentes que o titular não tem a menor ideia de quem sejam. Porém, a lei impõe a responsabilidade solidária entre eles. O titular pode até ter concordado com a política da empresa para a qual repassou seus dados, sabendo que haveria compartilhamento da informação, mas sendo a responsabilidade solidária, a empresa deve saber quem são seus parceiros de negócios, no intuito de mitigar um pouco o risco. Se o segurado se une a um colaborador sem um nível de segurança adequado, ou que não tenha uma apólice com cobertura ideal para recompensá-lo, não garantindo ser a empresa solvente e responsável, estará assumindo um risco muito maior do que o comum. A legislação traz essa inovação, e fará as empresas pensarem na importância das apólices de seguro ligadas a riscos cibernéticos.

Flávio: Eu tenho uma pergunta para o **Paulo**: quando começamos a abordar os clientes e a mapear risco, cogitamos possíveis cenários, incluindo catástrofes. Nosso papel é pensar em situações de alta complexidade e em como transferir esse risco para o mercado segurador. Às vezes há situações não cobertas, mas o risco é conhecido, pode ser mapeado e, para enfrentá-lo, é traçado um plano. Há clientes em diferentes estágios frente a seus riscos, do inicial ao avançado, e o seguro cibernético é a última camada de proteção. Em relação a uma possível catástrofe, o segurado tende a estudar o assunto, se informar, trabalhar com controle. Antes da Lei Geral, para implementar controles e contratar a apólice os clientes pensavam muito mais no próprio risco. Não havia grande preocupação com a responsabilidade civil nem com as consequências da exposição de dados. Pergunto: a legislação traz uma percepção de risco maior quando se fala em responsabilidade civil, vazamento de dados e terceiros acionando o seguro?

Paulo: A legislação pontua um risco civil. Geralmente, a preocupação do cliente é com vazamento de informações, com a revelação do conteúdo do dado. O risco que a lei apresenta é maior, pois prevê uma autoridade administrativa de proteção, que aguardamos ser criada em breve. Na condição de ente regulado, a seguradora deverá cumprir a lei como um todo, e um incidente de vazamento gera responsabilidade civil e sanção administrativa. A percepção do risco será aumentada, pois há a questão do vazamento

"Mesmo antes da Lei Geral de Proteção de Dados, o MP vem sendo enfático em relação ao assunto, *contatando empresas grandes de cada nicho de negócios e esclarecendo que é preciso ter um sistema de proteção de dados."*

PAULO MARCOS RODRIGUES BRANCHER

de dados e do descumprimento da lei. A legislação traz um grande rol de direitos do titular, como acesso, modificação e portabilidade do dado. Se não houver preparo para isso, a empresa estará descumprindo a lei e será passível de sanções. Isso tudo não só pela medida de segurança da organização mas porque há novos riscos, como dano patrimonial e dano à imagem. Quanto mais a empresa compreender a importância do seguro, melhor.

Giseli: Se as pessoas antes não sabiam que tinham um problema de dados vazados, o fato de agora haver essa notificação obrigatória por lei não pode gerar mais reclamações?

Paulo: Tenho uma percepção conservadora em relação a isso. Acho que a lei tem o grande mérito de conscientizar cada um de nós sobre o fato de que possuímos ativos de valor, ou seja, os nossos dados pessoais nas mãos de terceiros. Estes precisam perceber que é preciso tratar os dados no grau de responsabilidade prometido. De novo, fazendo uma comparação com o Código de Defesa do Consumidor: se você compra um eletrodoméstico para sua casa e o aparelho não funciona, há a percepção exata do quanto seu patrimônio foi lesado. A demanda individual é mais natural. Porém, o meu conservadorismo decorre da novidade de que o dado pessoal não é necessariamente uma preocupação para a geração mais jovem.

Cadernos: Hoje existe inclusive a ideia de que privacidade é coisa do passado.

Paulo: Sim, existe um pouco essa questão cultural. Mesmo quando alguém pouco se preocupa com a privacidade, se tiver algum direito negado, como o acesso a dados pessoais, ou o poder de corrigi-lo, em que nível esse incômodo vai despertar uma demanda ou uma reclamação? Será necessário um esforço individual maior do que a simples infração da lei. Ou seja, o dano tem que valer como um prejuízo pessoal, e isso vai requerer trabalho e atuação relevantes das associações de classe e do Ministério Público. Ao falarmos em proteção de dados, geralmente o primeiro enfoque se liga ao produto ou serviço que a empresa oferece. Existe a infraestrutura de serviços etc., contudo, há também dados manuseados por funcionários, que englobam não só o faturamento da empresa mas também a forma como ela trata seus associados. Logo, a atuação não será apenas do Ministério Público para o consumidor. O Ministério Público do Trabalho também vai checar como estão sendo tratados esses dados, e a empresa terá que prestar atenção ao risco que corre nesse *front*. Mesmo antes da Lei Geral de Proteção de Dados, o MP vem sendo enfático em relação ao assunto, contatando empresas grandes de cada nicho de negócios e esclarecendo que é preciso ter um sistema de proteção de dados. Do contrário, será aberto inquérito civil para investigação, haverá ação civil pública e existirão demandas de indenização. Tudo isso representa uma mudança cultural.

Cadernos: A nova lei prevê a criação de uma agência reguladora?

Paulo: O projeto de lei previa uma autoridade, mas foi vetado por vício no procedimento legislativo. Por ser uma agência pertencente ao Poder Executivo, era desse poder que deveria partir a proposta. Como isso não aconteceu, no âmbito do Legislativo havia risco de o projeto ser declarado inconstitucional. Daí, uma multa emitida e contestada no Judiciário poderia realmente ser considerada indevida por inconstitucionalidade. O Presidente rejeitou a iniciativa, mas se realmente quiser fazer vingar tal lei deve criar essa agência o quanto antes.

Flávio: Houve também um decreto do Banco Central que é relevante para a exposição cibernética, pois prevê que os entes regulados tenham um executivo do conselho responsável pela segurança de dados, uma figura passível de responsabilização em caso de descumprimento do normativo. Já vínhamos percebendo tal movimento de segregar a tecnologia do profissional de *cyber security*. Com essa medida, o setor bancário saiu na frente. Isso acontece também em outros setores?

Paulo: Quem está na frente, de fato, é o Banco Central, o que afeta instituições financeiras e demais entidades que operam com meios de pagamento. São resoluções que impõem medidas de segurança, até mais pesadas do que a própria lei. As agências federais se inspiram umas nas outras.

Camila: Acho que outros setores cujos entes regulados tenham acesso a muitos dados podem se valer dessa experiência. O caminho natural é que primeiro venha o sistema financeiro, mas acho que os mercados de seguros, de capitais e de saúde e previdência complementar fechada não ficarão atrás. Quanto mais os "desbravadores" tomarem esse caminho, outros seguirão a mesma linha. Fica muito mais fácil adotar certa severidade em relação aos entes regulados quando já existe um pioneiro que é respeitado por todos, inclusive pelo Estado. Logo, não é de se esperar nada mais leve no futuro do que a atitude do Banco Central.

Cadernos: A lei brasileira de proteção de dados foi baseada em legislação da União Europeia. Existem agências reguladoras lá também?

Paulo: Não, o que existe na União Europeia é uma regulação um pouco diferente do que nós costumamos ver e que age por diretivas regulamentadas para serem eficazes nos respectivos países. A GDPR, ou regulação geral de proteção de dados, demorou dois anos para se efetivar e começou a valer este ano. As regulações são autoaplicáveis, mas cada país-membro da UE tem a sua própria autoridade de proteção de dados, algumas mais enfáticas que outras. Nesses países percebe-se uma cautela na aplicação de sanções, porque a ideia de uniformização que traz a lei pode ter um risco, se cada autoridade entender de um jeito os artigos descritos. Por mais que o Brasil tenha se inspirado nesse modelo, não sabemos bem que interpretação e tipo de atuação ocorrerão aqui.

Camila: Embora os seguros contra riscos cibernéticos na Comunidade Europeia tenham o mesmo nome, eles são bastante diferentes entre si. Há riscos que dificultam a padronização e talvez isso nem seja possível. Existe um trabalho muito forte junto aos potenciais segurados para que consigam realizar boa gestão de seus riscos cibernéticos ou, pelo menos, que comecem a entendê-los e busquem transferências de risco fazendo pesquisa de mercado, porque as seguradoras têm produtos variados. Algumas focam nas coberturas de responsabilidade civil e outras oferecem um seguro mais próximo ao de *property.* Na verdade, usamos a mesma terminologia para um seguro que possui facetas bastante distintas e esse é um desafio do mercado.

Flávio: o mercado muda e os produtos também. Um *ransomware* como o *WannaCry* é um risco relativamente novo, mas os produtos atuais já dão cobertura e outros vão surgir. Com a legislação, vários clientes têm questionado a gestão de dados de terceiros – fornecedores, parceiros, etc. Alguns casos se deram por fatores simples. Um exemplo famoso foi o de uma empresa que tinha um fornecedor de manutenção de equipamentos e que podia trocar arquivos de pagamento. Diferentemente do *WannaCry,* que foi massivo, esse foi planejado pelo hacker que escolheu o lado mais fraco, o do fornecedor, que não tinha o mesmo nível de segurança da contratante. Por isso é interessante verificar como as empresas gerenciam a cadeia de parceiros e fornecedores porque a exposição não está só nela, existe também na relação com essas empresas.

Paulo: Às vezes o inimigo está dentro da empresa. Existem empresas que, por desinformação, distribuem o mesmo *login* e senha para funcionários operarem determinada plataforma.

Giseli: Há pesquisas sobre vazamento de dados que concluíram que os responsáveis muitas vezes são empregados e ex-empregados – e isso ocorre no Brasil em percentual muito mais alto do que no exterior.

Cadernos: Frequentemente cita-se o Brasil como um dos países que têm maiores problemas de vazamento de dados e ataques cibernéticos.

Camila: As estimativas são várias, mas todas apontam para problemas muito sérios aqui. Acredito que ainda não temos uma cultura de proteção de dados. No âmbito empresarial, vemos agora, por meio da LGPD, que as empresas se preocupam e querem entender o tema. Infelizmente, o

interesse é mais voltado para entender o risco em exposição e menos em realizar as modificações na cultura empresarial que majoram tal risco. Nas reuniões em que estive, poucos empresário dizem querer um treinamento para seus colaboradores a fim de sensibilizá-los para a questão.

Flávio: Na AIG, contratamos um *underwriter* com experiência no mercado de segurança cibernética. Ele fazia trabalho de campo em outras empresas. Ou seja, até mesmo para uma seguradora, é preciso lançar mão desses especialistas no dia a dia. Um episódio interessante foi o de uma grande empresa que pretendeu testar o nível de entendimento e maturidade digital de seus clientes. Houve três ou quatro tipos de testes. Um dos primeiros trabalhos foi mostrar um e-mail muito bem elaborado: 75% das pessoas clicaram nele. Essa era a porta de entrada para o produto. Em outra comunicação, um nível abaixo e que já não parecia tanto a página real, metade das pessoas clicou. Em um e-mail simples, cheio de erros de Português e de caráter duvidoso, ainda assim 25% das pessoas clicaram. É uma carência de cultura, mesmo.

Camila: A respeito da falta de sensibilidade à privacidade: esse é um fato também geracional, porque os mais jovens não ligam tanto para isso. Os brasileiros, em geral, não estão preocupados. Dinamicamente, esbarramos na forma de controle que temos. Passamos nossos dados com certa facilidade.

Cadernos: Na verdade, não há opção: para operar na economia moderna é preciso frequentemente abrir os dados pessoais.

Camila: Sim, mas com controles, como no exterior. Aqui é diferente, é uma questão de "*mindset*", necessidade de abrir a cabeça, mudar a cultura. Eu levei meses até conseguir olhar o tema de outro modo, porque a falta de sensibilidade é um comportamento arraigado no Brasil. Pensar em dados pessoais hoje em dia é uma disruptura. Temos que perceber o assunto como uma estrutura comportamental, que caminha rapidamente para outros estágios.

Giseli: Isso se dá até nos termos de consentimento de aplicativos no celular. A pessoa fica tão ansiosa para baixar um aplicativo que consente em dar informações que determinam aonde ela vai e em fornecer outros dados pessoais e confidenciais.

Paulo: Há uma brincadeira de um escritório de advocacia nos EUA em relação a isso: essa empresa persuadiu uma outra companhia a lançar um produto *fake* em que nos termos de uso havia uma cláusula pela qual a pessoa concordava em vender sua alma ao demônio. 95% dos indivíduos aceitaram. No fundo, é o que a gente faz quando se submete a esses termos sem ler.

Thales: Voltando a pensar em organização, em um mundo corporativo que exija sigilo profissional, se o médico, por exemplo, que tem todos os registros do paciente em sua máquina, compartilhar a senha com um funcionário, isso pode ser vazado? Esse tipo de facilidade alcança os *smartphones*. Ao cadastrar um aplicativo de pedidos de comida, você fornece seu endereço, nome e número de cartão de crédito. Se alguém *hackear* essa empresa, terá acesso aos seus dados, incluindo o que armazenar em razão da profissão. Se a mesma senha for usada para tudo, pior ainda. Quanto mais facilidade o mundo virtual traz, maior é a exposição. Temos a mesma responsabilidade com o computador de casa e com o do escritório? Há pessoas que dizem preferir abrir o e-mail no trabalho porque é mais seguro. A negligência no ambiente profissional é um dos componentes culturais mais arraigados.

Cadernos: Como está a demanda de seguro cibernético? Existem organizações que confiam mais em medidas de gerenciamento, como antivírus e *firewall*, do que em seguro?

Camila: São questões diferentes. Não dá para prescindir de uma boa gestão de riscos. A seguradora vai tomar o risco que entende ser capaz de subscrever naquele momento. A atividade securitária não é uma muleta que vai substituir uma boa gestão de risco do titular.

Flávio: Existia essa mentalidade no passado, mas vem mudando. Há cinco anos, se eu perguntasse quem já foi atacado por um vírus como o *WannaCry*, a resposta era "zero". Mas, numa palestra que dei há pouco tempo, alguns corretores afirmaram ter sido prejudicados. A perspectiva do *WannaCry* foi emblemática no mercado porque tangibilizou o risco. Disseram: "Minha lista de vencimentos de clientes se perdeu", etc.

Giseli: Os fatores para o sucesso do seguro cibernético estão aí. Existem sinistros. Mais e mais o mundo vai se conectando, com processos que não eram anteriormente automatizados e passaram a ser. Mesmo pequenas empresas, como, por exemplo, uma padaria, estão estabelecendo conexões com a rede mundial de computadores. À medida que essas empresas se automatizam, ficam também mais expostas a riscos de ataque. Há também a legislação. Esses três componentes atuam para aumentar a demanda pelo seguro cibernético.

Cadernos: O risco cibernético pode ser sistêmico. Em que medida isso é um problema para as seguradoras subscreverem? Qual o papel do resseguro?

Flávio: Esse é um grande desafio. No mercado, há uma situação que se chama "*clash*", ou seja, um episódio que

> ***O que prevemos que vá acontecer com o risco cibernético é algo muito próximo do que houve com o seguro de catástrofes naturais, talvez até maior.*** *A estimativa de perdas relativas a risco cibernético em 2018, inclusive financeiras, é de 1% do PIB mundial, ou cerca de US$ 600 bilhões."*

GISELI GIUSTI TILGER

pode ser alarmante e acionar várias apólices ao mesmo tempo. Quando pensamos em risco cibernético, voltamos a nos perguntar quais são as apólices para esse contexto e como cada uma foi desenhada. Também temos que usar o resseguro, claro.

Giseli: Há técnicas de controle de acúmulo de exposição a riscos. É possível fazer simulações, como no caso de catástrofes naturais. As resseguradoras ganham dinheiro subscrevendo tais riscos. O que prevemos que vá acontecer com o risco cibernético é algo muito próximo do que houve com o seguro de catástrofes naturais, talvez até maior. A estimativa de perdas relativas a risco cibernético em 2018, inclusive financeiras, é de 1% do PIB mundial, ou cerca de US$ 600 bilhões. Hoje isso é controlável em termos de acúmulo de riscos, mas conforme os processos são mais automatizados e os ataques vão surgindo mais complexos, a exposição tende a crescer.

Paulo: Daqui a cinco anos essa nossa conversa pode ter uma perspectiva completamente diferente. Em relação à evolução tecnológica, não conseguimos enxergar a dimensão que tem, por exemplo, a "internet das coisas". Cremos que os equipamentos vão conversar entre si, mas não sabemos como a nossa vida vai mudar por causa da conectividade, dados transferidos, serviços agregados e troca de informações. Se uma "ponta" parar de funcionar, haverá repercussão de abrangência desconhecida. Ou seja, esses US$ 600 bilhões de hoje são totalmente baseados em um cenário que estará mudando constantemente.

Giseli: O risco cibernético está presente em todas as facetas da vida. É preciso conhecê-lo. No mercado brasileiro, infelizmente, ainda há a mentalidade de que "*cyber risk* é algo que não se vê", ou "a demanda está fraca ainda" etc. Mas a exposição é real. E há o famoso "*silent cyber*": as exposições potenciais, mas não transparentes, ao risco cibernético nas apólices tradicionais de *property* e RC. Se as seguradoras e as empresas não ficarem atentas em casos de sinistro, estarão desatualizadas em pouco tempo.

Flávio: Em média, cada pessoa está conectada hoje com quatro ou cinco *gadgets*, entre celular, *tablets* e outros mais. Em 2020 estaremos com 20 ou 30 *gadgets*, um crescimento exponencial. Nos EUA, por exemplo, houve um ataque no qual a pessoa chegou em casa, ligou a televisão *smart* e viu que ela tinha sido "sequestrada". Para "liberá-la" era necessário pagar um resgate.

Camila: Existe também o caso de um hotel na Áustria em que invadiram o sistema de TI do estabelecimento e os hóspedes ficaram presos em seus quartos. Os hackers, então, pediram resgate para liberar as pessoas. Foi um sequestro de verdade. E há a possiblidade de travar fechaduras

> ***Uma seguradora especializada deve estabelecer o fundo segurado como proteção.***
>
> *Além da transferência do risco existe um componente forte: é necessário decidir o que fazer num momento de crise, quais medidas vão ser tomadas, como mitigar e barrar essa exposição."*

THALES DOMINGUEZ BARBOSA DA COSTA

inteligentes em carros. **Flávio**, no mercado, você vê outro grande desafio além da própria operacionalização do seguro nesse mundo novo, do risco analisado pelas mais diversas áreas já consolidadas nas seguradoras, ou você busca ter uma área única olhando especificamente para o risco cibernético?

Flávio: Hoje, via de regra, as apólices costumam excluir o risco cibernético. Uma evolução serão as apólices que ofertam algum nível de cobertura. Existe a apólice específica, que cobre o risco financeiro cibernético. O maior desafio para os próximos anos é explicá-lo. Quantificar pode ser difícil, mas já começamos a mapear. Outro dia um corretor me perguntou: "Como dizer ao meu cliente quanto custará esse seguro? Qual o valor real em risco? R$ 5 milhões, R$ 10 milhões?" Esse é o desafio. Ninguém conhece melhor o negócio do que o próprio cliente, então é preciso pensar em cenários. É um produto que foge ao tradicional porque é preciso mais tempo de investimento.

Cadernos: O corretor também precisa se aprofundar mais?

Flávio: Sim. Os maiores clientes têm a figura do *Risk Manager*, mas os menores clientes tratam com o financeiro ou com a área de compras, e esses dois setores não estão acostumados a quantificar o risco cibernético. Para negociar é preciso juntar as áreas de *compliance*, jurídico e TI, de modo a aferir a exposição. O esforço de identificar e quantificar riscos é muito trabalhoso. Não estamos lidando com um seguro tradicional, em que a exposição é tangível. A Escola Nacional de Seguros, inclusive, tem investido em conscientização e treinamento para esse mercado. Pessoalmente, tenho falado bastante com os corretores que percebem uma demanda importante de cobertura do risco cibernético. Temos diversas iniciativas nesse sentido: explicamos o que é e como funciona esse seguro.

Giseli: Penso que haja também uma barreira do preço, porque existe uma cultura restritiva. Não que o seguro seja caro, mas estamos numa crise econômica. O *budget* para seguros é sempre complicado.

Flávio: Está acontecendo algo como o seguinte: o departamento de TI pede para aprovar R$ 10 milhões para fechar todos os riscos correspondentes através dos instrumentos tradicionais. Só que esse departamento só consegue aprovar R$ 3 milhões. Por que não transferir a diferença de risco para a seguradora? Há empresas que já veem a questão como investimento em vez de custo, pois não conseguem ter todos os controles. Daí transferirem parte do risco para a seguradora.

Giseli: Acho que isso tem a ver com a forma como se vende e como se coloca o seguro. O *cyber* tem muitos serviços

agregados, então quando acontece um problema é preciso notificar as pessoas, e isso traz intranquilidade. Quem é sujeito à GDPR tem 72 horas para notificar, então se a seguradora já apresentou o serviço talvez seja muito mais fácil, pois tudo vai estar pronto.

Cadernos: Há várias coberturas adicionais no *Cyber Insurance*, não?

Giseli: Sim. Tem cobertura para contratar um assessor de imprensa, um relações-públicas, para ajudar na imagem da empresa que foi *hackeada*, sendo a reputação o maior ativo intangível que uma organização possui. Esses serviços agregados podem auxiliar o segurado a perceber que ele tem mais uma ferramenta para a gestão de seu risco. São um gasto, mas fico feliz que a mentalidade esteja mudando.

Cadernos: É possível identificar e processar criminalmente quem cria essas ameaças digitais?

Thales: Em relação ao *bitcoin*, ninguém sabe quem o inventou. Existe uma pessoa a quem atribuíram a autoria, mas que nunca a assumiu. É algo tão despersonalizado que sequer se sabe quem criou.

Camila: Pode ter sido até uma superinteligência artificial. Hoje se está despersonificando tudo. Mas ao mesmo tempo há colaboração de grupos enormes ao redor do mundo, cada um adicionando um pouquinho de inovação e tecnologia, o que é interessante.

Flávio: Para crimes, o conceito é o mesmo. Antes, quem cometia o delito estava exposto. Agora, colabora com pessoas pela rede e faz o ataque. É menos custoso e é um desafio para a sociedade pensar a respeito.

Paulo: Há um projeto de lei no Brasil voltado para criptomoedas. Já que não existe uma regulação específica, o relator desse documento fez um voto para criminalizar a criptomoeda. Em um projeto como esse, sem entidades fortes conseguindo articulação, quem toma a frente é o Ministério Público e Polícia Federal. Proibir é a forma mais fácil de controle do que é desconhecido. Este é um sinal da luta inglória das autoridades de investigação em relação aos delitos. A criptomoeda é a forma como as pessoas podem ser compensadas anonimamente. Um depósito tem notas em série. Logo, pode ser feito um rastreamento. Com a criptomoeda, não. As autoridades também têm dificuldades para identificar crimes a partir de simples usos da internet, como a autoria de um IP, porque precisam de uma ordem judicial, o que atrasa as decisões. Em todas as áreas há a luta do crime organizado contra o Estado desorganizado – em escala global, não só no Brasil. Um crime cibernético se sofistica de modo muito mais rápido e acentuado do que a polícia consegue se equipar. As autoridades de investigação podem até obter resposta adequada para isso, mas a criptomoeda é um código serial e não há como saber quem está do outro lado. No *WannaCry* conseguiu-se rastrear a quantidade de dinheiro depositada em uma conta. A estimativa foi de US$ 150 mil, mas o prejuízo causado foi de bilhões de dólares.

Camila: Há muito o que mudar em termos de conceito e de forma de pensar. O direito criminal clássico busca a identidade da pessoa. É preciso pesar muitas questões e desapegar de diversos aspectos. A estrutura jurídica brasileira e do mundo todo não faz mais sentido ou, na verdade, não atende a tudo. Quando falamos de inovação, olhamos muito para a parte tecnológica, mas é preciso mudar também a estrutura cultural: aplicar novas ideias, processos e modos de agir. Dentro do que temos hoje, quanto a institutos e estatutos legais, fica difícil classificar o que ocorre.

Cadernos: A responsabilidade civil objetiva, de certa forma, facilita o seguro de RC, pois responsabiliza desde logo o agente que causa o dano imediato. Não facilita também o seguro cibernético?

Flávio: Sim, podemos não conhecer de imediato o *hacker*, mas conhecemos quem não protegeu os dados devidamente. Logo, é possível responsabilizar os dirigentes e quem permitiu que os danos ocorressem. Não existe instituição que seja impenetrável atualmente. Os *hackers* querem atingir determinado sistema e o atacam. Pode ser um funcionário, em conluio com um terceiro, ou uma instituição buscando os dados: é difícil pensar exatamente o tamanho dessa responsabilização e do risco.

Thales: Um exemplo é o consultor de TI que crê ter indicado a melhor tecnologia possível em termos de proteção de dados e mesmo assim a empresa foi invadida. Do ponto de vista de responsabilidade solidária e da responsabilidade objetiva, primeiro é preciso indenizar os consumidores, ou seja, quem teve o prejuízo. Só depois a empresa verá com seu prestador ou consultor se era realmente a melhor forma de proteção. Como não é possível perceber a autoria de um ataque ou identificar em uma estrutura grande quem errou primeiro, deve-se prestigiar a vítima com a indenização. Uma seguradora especializada deve estabelecer o fundo segurado como proteção. Além da transferência do risco existe um componente forte: é necessário decidir o que fazer num momento de crise, quais medidas vão ser tomadas, como mitigar e barrar essa exposição. A seguradora tem um papel fundamental, e a rede de prestadores que a ajuda pode auxiliar a não haver um prejuízo ainda maior para o segurado e para os consumidores. ●