Evento promovido pela APTS e ENS mostra que os corretores de seguros não estarão livres dos impactos da LGPD. Mas, terão oportunidades de negócios com o cyber risks

Palestrantes painel 1: Barbara Bassani, Carla Couto, Claudio Macedo Pinto e Rodrigo Silva

O seminário “LGPD na prática e soluções para Cyber Risks”, promovido pela Associação Paulista dos Técnicos de Seguro (APTS) em parceria com a Escola Nacional de Seguros (ENS), dia 21 de novembro, em São Paulo, se aprofundou na discussão sobre os impactos da Lei Geral de Proteção de Dados (LGPD) para os corretores de seguros, bem como sobre o cenário da segurança cibernética e as perspectivas para os seguros cyber risks.

Aspectos jurídicos - Do ponto de vista legal, a advogada Bárbara Bassani, da TozziniFreire Advogados, explicou que todos os corretores de seguros, independentemente do porte ou da área de atuação, devem se adequar à LGPD. “O corretor é detentor dos dados de seus clientes e deverá protegê-los, preocupando-se, inclusive, com o manuseio por funcionários ou por prestadoras de serviços”, disse. Para advogada Carla Couto, da TozziniFreire, apesar de criticada, a LGPD trouxe mais segurança jurídica.

Bárbara orientou os corretores a obterem o consentimento de seus novos clientes para a oferta de outros produtos. Já em relação à base de clientes anterior à lei, a advogada esclareceu que a LGPD não trata do legado e que essa tarefa ficará a cargo da Autoridade Nacional de Proteção de Dados (ANPD). No entanto, sugeriu aos corretores que se unam para defender seus interesses em relação ao legado de dados. “Apresentem estudos, fiquem atentos”, disse.

Gestão de riscos - “Segurança da informação é a espinha dorsal da LGPD”, disse Rodrigo Silva, diretor presidente da Turing Security. Ele lembrou que uma das atribuições da ANPD é receber denúncias, que podem vir até de algum concorrente. “Imagine a ANPD pedir relatório de impactos e

o empresário não ter, porque não fez nada, sequer começou. Melhor é evitar o caminho do litígio", orientou.

Silva explicou que não existe um software que dê conta da gestão de riscos, segurança cibernética e da privacidade e proteção de dados. Ele concluiu que a falta de entendimento da tecnologia traz forte risco à privacidade e proteção de dados. Já em relação às medidas de segurança cibernética (controle de acesso, criptografia, registro de log etc.), deixou claro que não são contra a privacidade, mas essenciais para mantê-las.

Foco nos corretores – A proteção de dados e os riscos cibernéticos são uma grande oportunidade de negócio para os corretores, acredita o diretor da APTS Cláudio Macedo Pinto, fundador da Clamapi, corretora especializada em riscos cibernéticos. Especialmente para os corretores, ele ensinou o caminho das pedras em 13 passos que orientam sobre como se adequar à lei, se proteger de ataques virtuais e vender seguro cyber risks.

Macedo sugeriu começar por pesquisas sobre o assunto, inclusive sobre a atuação de hackers, e estudar vários temas, como segurança da informação, legislação, clausulados das apólices, coberturas e exclusões do seguro e o questionário de risco. Buscar parcerias é importante, bem como proteger os dados da corretora. Por fim aconselhou o corretor a não desistir diante da resistência do cliente. "O cyber será uma espécie de seguro saúde para as empresas", previu.

Cibersegurança - De acordo com Marcos Nehme, CTO Field e diretor para América Latina e Caribe na RSA Security, a ideia da LGPD é criar confiança e, junto com ela, oportunidades de inovação, apesar da "dor de cabeça" que a implementação provocará. Para ele, todo esse processo é importante para a experiência do cliente, gerando confiança, valor na empresa e lealdade.

Nehme observou que é preciso ter atenção aos novos riscos, como, por exemplo, os e-mails maliciosos que instalam vírus específicos para roubar dados de determinados usuários, que não são detectáveis por antivírus. Dentre os desafios da adequação à LGPD, ele cita a identificação e o cuidado com os dados sensíveis. "Não tenha mais caderninho ou folhas na mesa com dados de clientes. Adote a prática da mesa limpa", disse. No aspecto da segurança, orientou a ter controle maior sobre quem acessa as informações e a criar processos de autenticação de usuários.

Crimes cibernéticos - Considerado um dos melhores hackers do mundo pelo Google e Facebook, o diretor da Elytron Security, João Lucas Brasio, explicou que o seu trabalho como "hacker do bem" é invadir os sistemas de empresas para detectar vulnerabilidades e torná-los mais seguros. Este trabalho é necessário, segundo ele, porque os casos de vazamentos e ataques cibernéticos estão aumentando ano a ano e as perspectivas não são boas. "A tendência é piorar cada vez mais", disse.

De acordo com Brasio, um dos motivos aumento de crimes cibernéticos é a própria internet, que funciona em três camadas: surface web, em que todos navegam e que responde por apenas 4% de todo o conteúdo; a deep web, cujo conteúdo não é indexado pelos buscadores, como é o caso de exames médicos e operações bancárias, concentrando 90% das navegações; e a dark web, na qual a navegação é anônima e, por isso, é utilizada para pedofilia, tráfico de drogas e crimes cibernéticos.

A lei e os riscos em debate – No talk show mediado por Claudio Macedo Pinto, o debatedor Sergio Oliveira, diretor jurídico da Tokio Marine Seguradora, deixou claro que os corretores poderão responder junto com as seguradoras pelo vazamento de dados, de acordo com a LGPD. "A responsabilidade solidária existe, inclusive a objetiva, aquela não precisa da comprovação da culpa. Por isso, os corretores devem se preocupar".

Victor Perego, Cyber Underwriter na AIG Seguros, disse que em suas apresentações costuma dividir os objetivos do seguro cibernético em três "pacotes". No primeiro, para cobrir os custos que a empresa terá para investigar, restaurar o sistema, enfrentar a paralisação (lucros cessantes) e lidar com a crise de imagem. No segundo, para atender ao aspecto regulatório (LGPD), cobrindo custos

com peritos, multas e publicidade do vazamento. No terceiro, o seguro cobrirá os custos das ações judiciais de terceiros em decorrência do vazamento de dados.

Uma das premissas básicas do seguro cibernético, segundo Hellen Deungaro Fernandes, gerente de subscrição de Linhas Financeiras na Zurich, é a exclusão de danos materiais ou danos tangíveis. “Se perco meu computador com os dados de clientes, não haverá cobertura para a máquina, mas apenas para o seu conteúdo”, disse. As demais exclusões são danos corporais e a transferência de valores.

Cláudio Macedo informou que a sua corretora, a Clamapi, está trabalhando junto com seguradoras para desenvolver coberturas de riscos cibernéticos exclusivas para pequenas e médias empresas, incluindo corretoras, com valores mais baixos. “A maioria dos corretores não precisa de um seguro de R$ 1 milhão, às vezes, R$ 50 mil já é suficiente”, disse.

Fonte: Márcia Alves, em 04.12.2019