

O SECTOR SEGURADOR DESAFIOS E OPORTUNIDADES – O QUE SE SEGUE?

A transformação digital, o uso crescente da tecnologia e a utilização massiva de dados são uma realidade inegável e incontornável nos dias de hoje.

POR **INÊS ANTAS DE BARROS**

ASSOCIADA COORDENADORA DE COMUNICAÇÕES,
PROTECÇÃO DE DADOS & TECNOLOGIA,
A CONVITE DA ASSOCIAÇÃO PORTUGUESA DE SEGURADORES

Esta nova realidade traz consigo novas “ferramentas” que permitem criar novos e mais inovadores modelos de negócio, de distribuição de contratualização e interface dos stakeholders nas várias dimensões B2: o B2B, B2G e sobretudo B2C. O sector segurador não é, naturalmente, indiferente a esta realidade, assistindo-se a uma alteração de paradigma na forma como as empresas do sector segurador desenham os seus produtos, prestam serviços e se relacionam com os reguladores, com as outras empresas do ecossistema segurador e com os clientes – com ganhos a vários níveis associados à desmaterialização de processos, à agilização de procedimentos e à simplificação generalizada da relação com os tomadores e beneficiários de seguros.

A evolução e inovação tecnológica têm, efectivamente, sido o factor mais relevante para uma transformação inovadora do sector segurador como hoje o conhecemos.

Nos últimos anos, o sector segurador começou a sofrer uma mudança sem precedentes, resultante da utilização crescente de novas tecnologias (como a inteligência artificial, o cloud computing ou o blockchain) e da capacidade de recolha

e tratamento de grandes quantidades de dados (big data).

Estas ferramentas têm permitido ao sector segurador desenvolver produtos mais “targeted”, métodos de subscrição digitais, e ser um apoio ao negócio, seja na fixação de preços, na detecção e combate à fraude, entre outros domínios.

Contudo, associadas à crescente utilização de novas tecnologias e à recolha de grandes quantidades de dados, surgem as ameaças cibernéticas, crescentes e cada vez mais sofisticadas. De acordo com o World Economic Forum (“Global Risks Report 2021”), os riscos associados às falhas

de cibersegurança e à quebra de infra-estruturas de TI constituem um dos 10 riscos mais prováveis e com mais impacto para os próximos 10 anos.

Os incidentes de segurança têm colocado vários desafios jurídicos e operacionais às organizações, exigindo uma abordagem holística das várias vertentes – jurídica, técnica, operacional, negócio e humana.

Considerando as obrigações legais e regulamentárias, actuais e futuras (que, em determinados sectores, serão num futuro próximo ainda mais exigentes), a cibersegurança requer a adopção de uma nova abordagem, que esteja à altura dos novos desafios.

«Os riscos associados às falhas de cibersegurança e à quebra de infra-estruturas de TI constituem um dos 10 riscos mais prováveis»

O RGPD IMPÕE ÀS ORGANIZAÇÕES

QUE APLIQUEM
MEDIDAS TÉCNICAS
E ORGANIZATIVAS
ADEQUADAS PARA
ASSEGUARAR UM NÍVEL DE
SEGURANÇA ADAPTADO
AO RISCO

O sector segurador é um dos mais impactados pelos novos riscos e ameaças decorrentes dos ciberataques, não apenas por ser um dos mais “apetecíveis” para os atacantes, mas também porque, onde existe risco, existem oportunidades.

O aumento do número de ataques, com consequências cada vez mais complexas, representa também uma inegável oportunidade de negócio para as empresas de seguros, na medida em que fomentará o desenvolvimento e procura de produtos de cobertura de riscos cibernéticos.

Mas existe mais um factor que irá, a breve trecho, colocar definitivamente, e de forma incontornável, a cibersegurança na agenda “C level executives” – o novo quadro legal europeu no domínio da cibersegurança.

As obrigações de segurança de informação aplicáveis ao sector segurador

Actualmente, as empresas de seguros estão já sujeitas a um conjunto exigente de obrigações de segurança de informação que decorrem, essencialmente, do Regulamento Geral sobre a Protecção de Dados (RGPD).

De facto, enquanto organizações que tratam dados pessoais (incluindo dados sensíveis ou categorias especiais de dados) e informação confidencial, as empresas de seguros estão, já actualmente, sujeitas a um conjunto de obrigações legais que implicam, entre outras, a de implementação de medidas técnicas e organizativas para protecção dos dados contra tratamento não autorizado ou ilícito e contra a perda, destruição ou danificação accidental. Estas medidas serão ajustadas e personalizadas conforme a natureza mais ou menos sensível da informação e dos dados em causa.

O RGPD impõe às organizações que apliquem medidas técnicas e organizativas adequadas para assegurar um nível de segurança adaptado ao risco, tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares.

As empresas de seguros estão ainda