Revista
Opinião.Seg

Nº 16 - MAIO 2019

AIR e Sandbox

Tecnologia

Informação

LGPD

Risco

Solvência

Perícias Atuariais

Comitê de Auditoria

Distribuição

PRICL

Previdência Privada

Diversidade

Garantia Judicial

IFRS 17

Auditoria Atuarial

RONCARATI EDITORA

Eles fazem as projeções mais mirabolantes. Aplicam Teorias da Credibilidade, do Risco e dos Jogos. Executam Avaliação Atuarial. Realizam Teste de Adequação de Passivo (TAP). Aprofundam-se nos estudos do IFRS. Analisam Processos Estocásticos. Tudo isso dentro de prazos apertados e em meio a enormes equações. Amam a matemática e o resultado do seu trabalho
PARABÉNS!
3 de abril
Dia do Atuário
IBA
Instituto Brasileiro de Atuária
www.atuarios.org.br

Editorial

Nesta edição da Opinião.Seg, a primeira de 2019, mantivemos a livre escolha de temas a serem tratados por nossos articulistas. Acreditamos assim contribuir para a divulgação de informações ao mercado, graças à pluralidade dos assuntos, todos de muita importância.

Entre os temas aqui discutidos, a Lei de Proteção de Dados Pessoais se destaca pelo número de vezes em que é apresentada, deixando patente que os impactos e desafios para o setor já estão sendo bastante discutidos muito antes de sua entrada em vigor, em agosto de 2020.

Com a chegada do novo governo, a discussão sobre a necessária e esperada reforma da Previdência apresenta capítulos diários e gera incertezas para o empresariado, que adia investimentos. Acreditamos ser essencial a aprovação da reforma para a retomada do crescimento.

No setor de seguros, a curto prazo, a união da Susep com a Previc já foi anunciada pelo ministro Paulo Guedes.

A nova Superintendente da Susep, economista Solange Vieira, em sua posse ressaltou a relevância do setor de seguros como um alicerce de proteção ao cidadão e de crescimento para empresas e grandes segmentos. Segundo ela, é necessário flexibilizar o ambiente regulatório e harmonizar as leis aos avanços tecnológicos. "Precisamos desregulamentar e desburocratizar o setor, aumentar a competição, garantir segurança jurídica e, acima de tudo, tornar seguro um produto simples e acessível à população", afirmou.

Na prática, já se encontra em consulta pública minuta de Resolução CNSP que cria o Sistema de Registro Eletrônico das Operações das Sociedades Seguradoras, Entidades Abertas de Previdência Complementar, Sociedades de Capitalização e Resseguradores Locais (SRO).

Agradecendo a generosidade dos articulistas em compartilhar conosco suas reflexões, convidamos a todos para a leitura desta edição.

CHRISTINA RONCARATI
Maio de 2019

Índice

3 **EDITORIAL**
Christina Roncarati

6 **"QUANTO MAIS INFORMAÇÃO, MELHOR!"**
Celso Paiva

8 **A TECNOLOGIA E O MERCADO DE SEGUROS**
Jaqueline Suryan e Juliana Strohl

10 **LEI GERAL DE PROTEÇÃO DE DADOS E REPERCUSSÃO PARA O SETOR DE SEGUROS PRIVADOS NO BRASIL**
Angélica Carlini

14 **APÓLICES EM EXCESSO OU APÓLICES A SEGUNDO, TERCEIRO, ENÉSIMO RISCO**
Walter Polido

18 **OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS NO MERCADO DE SEGUROS E RESSEGUROS**
Marcia Cicarelli Barbosa de Oliveira, Camila Affonso Prado e Laura Pelegrini

23 **SOLVENCY REQUIREMENTS FOR INSURERS IN EUROPE AND BRAZIL – A COMPARATIVE LAW ANALYSIS**
Carsten Franz Otto

26 **IMPACTOS DA LEI DE PROTEÇÃO DE DADOS**
Danielle Djouki e Lillian Castilho Menini

29 **A IMPORTÂNCIA DA ASSISTÊNCIA TÉCNICA EM PERÍCIAS ATUARIAIS**
Heitor Rigueira

32 **PLANEJAMENTO FINANCEIRO E A IFRS17**
Joel Garcia

34 **COMITÊ DE AUDITORIA EM SEGUROS: ANJO DA GUARDA OU ENCOSTO?**
Assizio Oliveira

44 **ANÁLISE DE IMPACTO REGULATÓRIO (AIR) E SANDBOX REGULATÓRIO NO MERCADO SEGURADOR**
Simone Negrão

47 **DISTRIBUIÇÃO DE SEGUROS**
Thomaz Kastrup, Karen Schiavon e André H. Jahara

51 **PRINCÍPIOS E REGRAS DE DIREITO APLICÁVEIS AO CONTRATO DE RESSEGURO INTERNACIONAL – *PRICL***
Sergio Ruy Barroso de Mello

57 **É HORA DE TER CALMA**
Antonio Penteado Mendonça

59 **SEGURO GARANTIA JUDICIAL: UMA EVOLUÇÃO LEGISLATIVA E JURISPRUDENCIAL EM BENEFÍCIO DE TODOS**
Diógenes Gonçalves, Gianvito Ardito e Raíssa Lilavati Barbosa Abbas Campelo

63 **A AUDITORIA ATUARIAL E DE BENEFÍCIOS PARA AS ENTIDADES SUPERVISIONADAS PELA PREVIC**
Marco Pontes

68 **A LEI GERAL DE PROTEÇÃO DE DADOS**
João Marcelo Ricardo Máximo dos Santos e Géssika Sampaio da Fonseca

89 **PREVIDÊNCIA PRIVADA: AS ENTIDADES DO "SISTEMA S" E A PARIDADE CONTRIBUTIVA**
Paulo Sogayar

94 **LGPD E (RE) SEGUROS**
Bárbara Bassani e Carla do Couto Hellu Battilana

101 **A DIVERSIDADE E O AMBIENTE ÉTICO DA EMPRESA**
Valeria Camacho Martins Schmitke

Revista **Opinião.Seg**

Número 16 – maio de 2019
ISSN 2176-5944

A revista eletrônica Opinião.Seg é editada pela Editora Roncarati e distribuída gratuitamente.

Os textos publicados nesta revista são de responsabilidade única de seus autores e podem não expressar necessariamente a opinião desta Editora.

EDITORA RONCARATI LTDA
Fone: (11) 3071-1086
www.editoraroncarati.com.br
contato@editoraroncarati.com.br

ACI
American Conference Institute

Com tradução simultânea inglês-português
Portuguese-English Simultaneous Translation Available

OBTENHA CRÉDITOS
CLE/CPE

9ª Cúpula sobre

ANTICORRUPÇÃO BRASIL

Workshops interativos pré-evento
21 de maio de 2019

22 e 23 de maio de 2019 | Hotel InterContinental, São Paulo

Desconto especial para participantes do Brasil

Palestrantes do setor público:

Ministro Wagner de Campos Rosário
Ministro da Transparência e
Controladoria-Geral da União (CGU)

Ministro Benjamin Zymler
Tribunal de Contas da União (TCU)

Ministro André Luiz de Almeida Mendonça
Advogado Geral
Advocacia-Geral da União (AGU)

Carla Veríssimo
Procuradora Regional da República
Ministério Público Federal (MPF)

Paulo Roberto Galvão de Carvalho
Procurador da República
Ministério Público Federal (MPF)

Laura Alonso
Secretaria de Ética Pública, Transparencia y Lucha contra la Corrupción, Oficina Anticorrupción
Ministerio de Justicia y Derechos Humanos de Argentina

Participe de discussões de alto nível em vários formatos:

- Mesas redondas de benchmarking em compliance
- Sessões de perguntas e respostas com os membros do Advisory Board da Cúpula
- Diversas oportunidades de networking
- Entrevistas com executivos de empresas
- Coquetel para networking

ENTREVISTA ESPECIAL COM CEO

Visão macro: Como o combate à corrupção se enquadra nos objetivos mais amplos de uma multinacional

Pedro Parente
Global Chief Executive Officer
BRF SA

Benchmarking em Compliance com profissionais de anticorrupção:

- Avon
- Getinge
- Ambev
- Samsung
- BRF
- Johnson & Johnson
- Allergan
- Embraer
- Petrobrás
- BTG Pactual
- Braskem
- Telefônica
- In Loco

Inscreva-se já | AmericanConference.com/**BrazilAC** | +1 416-926-8200

Uma empresa C5 Group
Informações empresariais em um contexto mundial

“Quanto mais Informação, melhor!”

CELSO PAIVA
Diretor da Alfa Seguradora

Hoje, ontem e sempre o nosso mercado orbita em torno da informação.

Se mesmo em momentos de crise, o mercado de seguros se apresenta, em geral, num crescimento constante e com resultados lucrativos na maioria das suas operações, é porque tecnicamente evoluímos.

É certo que vários são os fatores para este relativo sucesso do nosso segmento. Porém, um ponto importantíssimo precisa ser destacado: o poder da informação. Sem informação não há tecnologia que nos permita avançar, evoluir... Ela é a base para tudo.

E não poderia ser diferente.

Vivemos de estudos atuariais, de bases de dados consistentes, de modelagens estatísticas, de atualizações constantes dessas bases, criando alicerces seguros (sem trocadilhos...), nos preparando para a chegada, num futuro muito próximo, da inteligência artificial a favor do segmento de seguros.

O mercado tem evoluído cada dia mais rápido com a sofisticação de seus produtos, direcionamentos focados para públicos específicos, diferenciação de preços por segmento, cada vez mais assertivo nos agrupamentos de “iguais” (Pessoa X Persona), e isso só pode ser alcançado com investimentos na qualidade das

informações, as quais, por sua vez, nos auxiliam nas tomadas de decisão corretas no crescimento e em bons resultados técnicos.

Hoje, e cada vez mais, a análise técnica supera a necessidade da "venda pela venda". É claro que nossa "bicicleta" tem que continuar pedalando... que sem "Vendas" nosso segmento não se sustenta, mas a "venda técnica", baseada em INFORMAÇÃO, é a bola da vez!

A sofisticação e a riqueza de uma boa base de dados são a sustentação para tudo o que mencionei aqui. **Quanto mais informação, melhor**!

A precificação, a segmentação e os agrupamentos nascem daí!

Os acessos diretos entre as companhias e seus segurados têm que ser estimulados, contando sempre com a participação do corretor, pois esta é uma avenida de duas mãos, todo mundo ganha... é o famoso bordão: "ganha, ganha"!

É de extrema importância que tenhamos acesso aos dados dos nossos segurados. Nosso parceiro de vendas, o corretor, também precisa participar deste enriquecimento das informações. Para ele, a abordagem, a oportunidade de angariar negócios, nasce também e, principalmente, da informação prévia. Como chegar na hora oportuna no nosso consumidor? Através da informação, claro!

Sem informação, como prestaremos um bom serviço para os nossos segurados? Para os nossos parceiros? Para a nossa distribuição?

A "comunicação" também nasce da informação, da riqueza dos dados, na troca deles e assim por diante.

Não há mais espaço para "a proteção do **meu** banco de dados"... Nossos dados estão disponíveis de alguma forma... na "nuvem", tenham certeza!

O mundo não é mais "meu", é de todos "nós". Mas por quê?

Porque a tecnologia da informação está presente em qualquer lugar, em qualquer segmento, em cada atividade, em todos os detalhes das nossas ações... Gostaríamos até de continuar sendo um "livro (aparentemente) fechado", que só quem tivesse permissão teria acesso a ele, mas, na prática, isso já não é mais possível!

Vamos nos unir, mercado, para termos mais e mais informações compartilhadas e, na medida que cada um de nós tenha acesso a elas, as utilize da melhor maneira que nos convier, devolvendo para o nosso consumidor mais transparência, mais segmentação, melhor precificação, com muito mais serviços, barateando nossa operação e revertendo ao consumidor um preço mais ajustado para cada produto do nosso segmento.

Compartilhar é fundamental! E...

Quanto mais informação, melhor!

A tecnologia e o mercado de seguros

JAQUELINE SURYAN

Sócia da prática de Seguros, Previdência e Saúde do escritório Azevedo Sette Advogados. Graduada e mestre em Direito do Estado pela Pontifícia Universidade Católica de São Paulo (PUC/SP). MBA em Gestão de Negócios de Seguros e Previdência pela Fundação Instituto de Administração (FIA/SP). Membro da Associação Internacional do Direito do Seguro (AIDA), do Instituto Brasileiro de Direito Constitucional (IBDC) e do Instituto de Previdência Complementar e Saúde Suplementar (IPCOM). Autora de diversos artigos e capítulos de livros relacionados com o mercado

JULIANA STROHL

Associada da prática de Seguros, Previdência e Saúde do escritório Azevedo Sette Advogados. Graduada pela Universidade Presbiteriana Mackenzie, pós-graduada em Contract Design pela Fundação Getulio Vargas (FGV) e cursando especialização em Direito e Tecnologia na Escola Politécnica de Engenharia da Universidade de São Paulo (EPEUSP). Autora de diversos artigos relacionados com o mercado de seguros

Recentemente foi publicada notícia[1] relevante trazendo informação de que seguradoras de Nova York, nos Estados Unidos, estariam começando a utilizar os dados constantes de redes sociais e outras fontes não tradicionais sobre seus clientes, a fim de determinar o preço de suas apólices.

Com o impacto do avanço da tecnologia afetando a vida de milhões de pessoas no mundo, tanto no âmbito pessoal quanto no profissional, notícias como esta estão, cada vez mais, deixando de ser exceção e se tornando corriqueiras em cotidiano das pessoas.

E, ao que tudo indica, com o mercado de seguros não será diferente: ele está muito próximo de passar por uma grande renovação devido aos grandes avanços da tecnologia. De fato, as mudanças já começaram a ocorrer, porém podem não ter sido percebidas (ainda) pelos segurados.

Diversos são os exemplos do uso das mais modernas ferramentas tecnológicas no mercado securitário.

Como em qualquer mercado, o mercado de seguros enfrenta grandes desafios e, um dos principais, é a questão de sua precificação. Sabe-se que muitos fatores interferem na aferição dos valores envolvidos nas apólices, seja no âmbito da importância segurada, como nos casos dos seguros de responsabilidade civil, seja nos valores dos prêmios, seja nos valores relacionados com os custos de comercialização do seguro.

No tocante à análise do risco de per si, ela muitas vezes pode não estar de acordo com a realidade do segurado, tendo em

1 www1.folha.uol.com.br/tec/2019/02/seguradoras-de-ny-podem-usar-redes-sociais-para-avaliar-clientes.shtml. Acesso em 06/02/2019.

vista que a seguradora busca estabelecer perfis de risco de acordo com suas características *versus* a probabilidade de sinistro, o que pode trazer diversas inconsistências.

Exemplo disso é o enquadramento de segurados em tipos de risco: segurados com o mesmo perfil, que se enquadrariam em um mesmo segmento, podem ter diversas características que tornem o risco totalmente distinto e traga discrepâncias na precificação efetuada pela seguradora.

E nesse ponto a tecnologia pode se mostrar uma grande aliada. Um dos grandes exemplos de como essa influência pode ser disruptiva é a telemetria, que consiste na utilização de dispositivos para captação e transmissão de dados em tempo real. Essa tecnologia é capaz de medir, rastrear e comandar veículos à distância, por exemplo.

Também há a criação de diversos aplicativos para monitoramento da saúde, como os denominados *wearables*, que são dispositivos eletrônicos que, quando utilizados por uma pessoa, podem coletar uma variedade de dados sobre seu usuário, tal como seus hábitos, o que implicaria em uma aferição de riscos bem mais precisa.

E é justamente nesses vieses que vêm surgindo cada vez mais as *insurtechs*, buscando incrementar a eficiência do modelo vigente da indústria de seguros.

Ocorre, no entanto, que no mercado de seguros brasileiro muitas iniciativas e novos modelos por vezes não conseguem prosseguir ou alcançar seu potencial em virtude de restrições legais ou regulatórias do nosso ordenamento.

Exemplo de fácil percepção sobre o acima é a regulamentação vigente atinente à comercialização de seguros por meios remotos. Muito se avançou, é verdade, porém o mercado brasileiro ainda está em fase embrionária em termos de aproveitamento do potencial que a tecnologia pode trazer.

A necessidade de cumprimento de requisitos para possibilitar a oferta de seguros por aplicativos, SMS ou outros meios tecnológicos existentes acaba diminuindo sua abrangência, facilidade ou acessibilidade.

Da mesma forma, os produtos que podem ser ofertados também, muitas vezes, não conseguem refletir o potencial de inovação que os novos modelos tecnológicos podem trazer de benefícios ou facilidades, uma vez que há regras gerais por vezes difíceis de serem superadas na criação de produtos diferentes e inovadores.

Claro está que a Superintendência de Seguros Privados vem se mostrando bastante receptiva ao diálogo com os players do mercado para poder progredir não apenas na regulamentação, que deve(ria) avançar na mesma velocidade que as tecnologias, mas também no sopesamento de regras e sua aplicabilidade caso a caso em situações não previstas.

Impossível, no entanto, que a regulamentação consiga acompanhar o atropelo tecnológico que estamos vivenciando nos últimos anos. Novos dispositivos, novos modelos de negócios, novos acessos, novos players, novas plataformas, novos mundos antes sequer imaginados. E tudo isso em apenas alguns anos.

Para acompanhar tamanho dinamismo, a criação de normas mais flexíveis e abrangentes pode se mostrar como uma alternativa.

Uma norma, por exemplo, de meios remotos que não contenha rol ou mecanismo objetivo de oferta de seguro, mas sim diretrizes e princípios norteadores da atuação dos players, possibilitaria a sua aplicação mesmo com os avanços dos modelos de oferta de seguros que ainda estão por vir e que, neste momento, sequer imaginamos como poderão operar.

É claro que essas diretrizes deverão pautar a atuação dos players do mercado de seguros sempre em atendimento às normas consumeristas, direitos dos segurados, boa-fé e transparência, bem como qualquer utilização de dados deve ser pautada nos parâmetros de proteção e privacidade, tais como previstos nas normas recentemente publicadas sobre o tema.

Certo é que a inovação pode ser uma grande aliada do mercado e que a tecnologia aproxima as partes e encurta caminhos, restando aos participantes do mercado conseguirem utilizá-la de modo eficaz, consciente e alinhada ao desenvolvimento do setor.

Lei Geral de Proteção de Dados e Repercussão para o Setor de Seguros Privados no Brasil

ANGÉLICA CARLINI
Advogada e Docente da UNIP[1]

CARLINI
SOCIEDADE DE ADVOGADOS

Introdução

Dois importantes textos de lei foram aprovados recentemente no Brasil e merecem a atenção dos profissionais e estudiosos de seguros: a Lei n.º 13.709, de 14 de agosto de 2018, chamada de Lei Geral de Proteção de Dados ou, simplesmente, LGPD; e, a Medida Provisória 869, de 27 de dezembro de 2018, já prorrogada[2].

A Lei n.º 13.709, de 2018, dispõe sobre a proteção de dados pessoais no Brasil e a Medida Provisória, além de alterar alguns aspectos específicos do texto de lei, cria a Autoridade Nacional de Proteção de Dados.

A partir de maio de 2018 a União Europeia já havia adotado o Regulamento Geral de Proteção de Dados aplicável a todos os países daquele bloco e, a todos que operem no espaço econômico europeu. Isso havia obrigado muitas empresas brasileiras

1 Pós-Doutorado em Direito Constitucional. Doutora em Direito Político e Econômico. Doutora em Educação. Mestre em Direito Civil. Mestre em História Contemporânea. Graduada em Direito. Advogada e sócia de Carlini Sociedade de Advogados.

2 Mesa Diretora da Câmara dos Deputados (MESA) – Ato Declaratório n. 17, de 27/03/19, do Presidente da Mesa do Congresso Nacional, prorroga a vigência da Medida Provisória nº 869, de 27/12/18, pelo período de sessenta dias. DOU de 28/03/19, Seção 1, Página 3.

a se adaptarem ao novo regramento europeu, em razão das relações econômicas e societárias mantidas com empresas europeias ou, por sua atuação naquele espaço.

A Lei Brasileira de Proteção de Dados entrará em vigor em agosto de 2020 e o debate que ela provoca tem sido marcado por intensa participação dos operadores do setor de seguros.

Reflexões sobre a Aplicação da LGPD

O objetivo da LGPD brasileira é proteger os direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da personalidade natural e, para isso é necessário dispor sobre o tratamento de dados pessoais, inclusive nos meios digitais, para evitar que a operação com esses dados coloque em risco as pessoas naturais.

Importante destacar que a defesa do consumidor é um dos fundamentos da proteção de dados pessoais adotada pela LGPD e, em vários artigos há expressa referência a princípios consumeristas para sustentação das determinações do novo texto de lei.

Em princípio, não há nenhum problema de ordem técnico-jurídica para que as duas leis atuem em caráter de complementaridade. A linha de pensamento denominada *diálogo das fontes* introduzida no Brasil pela Prof.ª Dra. Cláudia Lima Marques baseada em estudos de Erick Jayme, professor da Universidade de Heidelberg[3], estuda exatamente essa possibilidade, de duas ou mais leis atuarem em caráter complementar na proteção de direitos, em especial de vulneráveis. Com o *diálogo das fontes* se evita a antinomia de normas e o proceder hermenêutico se aproxima do *sopesamento,* para que a lei mais adequada prevaleça na aplicação ao caso concreto determinado.

O que causa preocupação no que se refere a aplicação do Código de Defesa do Consumidor (Lei n.º 8.078, de 1990) juntamente com a nova lei geral de proteção de dados, é a designação da autoridade competente para realizar a fiscalização e eventual punição, quando constatadas práticas em desconformidade com a lei. Será competente a Autoridade Nacional de Proteção de Dados ou, serão competentes os membros do Sistema Nacional de Direitos do Consumidor? Essa é uma questão da maior importância porque em um estado de forte tradição autoritária como o Brasil, a falta de indicação clara da autoridade competente para fiscalizar e punir permite a duplicidade de práticas, com inegável prejuízo para os setores econômicos e consequente judicialização das decisões adotadas em caráter administrativo.

Em nosso entendimento, tendo sido criada uma Autoridade Nacional de Proteção de Dados definida como órgão da administração pública federal, integrante da Presidência da República, não há dúvida de que essa entidade terá supremacia sobre qualquer órgão de defesa e proteção do consumidor para fiscalizar e, eventualmente, punir empresas que não se adequem às determinações da Lei Geral de Proteção de Dados – LGPD.

As competências especificadas para a Autoridade Nacional de Proteção de Dados, ANPD, no artigo 55-J da Medida Provisória 869, de 27 de dezembro de 2018, parecem não deixar dúvida a esse respeito e, o artigo 55-K da mesma medida determina, expressamente, que *a aplicação das sanções previstas nesta Lei (LGPD) compete exclusivamente à ANPD, cujas demais competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências*

3 MARQUES, Claudia Lima. *O "diálogo das fontes" como método da nova teoria do direito: um tributo a Erik Jayme.* In MARQUES, Claudia Lima (coordenação) *Diálogo das Fontes. Do Conflito à Coordenação de Normas no Direito Brasileiro.* S.Paulo: Revista dos Tribunais, 2012, p.19-20.

correlatas de outras entidades ou órgãos da administração pública.

Assim, está vedado que outros órgãos como os PROCONs, por exemplo, pretendam fiscalizar ou punir empresas que pratiquem operações de tratamento de dados porque a lei especial é a Lei Geral de Proteção de Dados que tem órgão específico para fiscalização e aplicação de sanções.

No âmbito do poder judiciário não é incomum que decisões sejam fundamentadas em mais de um texto legal, o que poderá ocorrer em casos concretos cuja discussão tenha por fundamento a aplicação da lei de proteção de dados e da lei de proteção e defesa do consumidor, por exemplo. Mas, no âmbito administrativo da fiscalização e da sanção administrativas, somente a Autoridade Nacional criada pela Medida Provisória 869, de 2018, é que tem competência para isso.

Cumpre lamentar que a Autoridade Nacional de Proteção de Dados não tenha sido criada como Agência, nos moldes daquelas já existentes e que atuam no cenário nacional como a ANS, ANAC, ANVISA, entre outras. Se há que se lamentar a inoperância de algumas agências é possível reconhecer, no entanto, que outras têm atuado bem e, consagrado essa contribuição de inspiração anglo-saxã como elemento que conferiu maior dinamismo e competência técnica para a regulação no Brasil.

A criação da Autoridade Nacional de Proteção de Dados vinculada diretamente à Presidência da República deixa margem a questionamentos e, a dúvidas sobre a eficiência do órgão. O modelo de agência vinculado a um ministério como o da Justiça no caso da LGPD, teria sido opção mais adequada até porque é inegável que as agências já fazem parte do cenário administrativo e jurídico nacional, foram objeto de inúmeros e robustos estudos acadêmicos e técnicos e, nos últimos anos têm dialogado com mais maturidade com a sociedade, com os agentes econômicos regulados e com o próprio poder judiciário.

De fato, a Teoria da Deferência já angariou maior robustez no Brasil, inclusive em julgados do Superior Tribunal de Justiça na sensível área da saúde suplementar. Por essa teoria explicam Jordão e Cabral Júnior[4]

> A "teoria da deferência" corresponde à tese segundo a qual a autocontenção seria conveniente (VERÍSSIMO, 2012). No caso específico do controle judicial, o argumento em favor da deferência seria o seguinte. Como a matéria regulatória é tecnicamente complexa, a deferência judicial às decisões das agências reguladoras transmitiria a ideia de respeito judicial a uma instituição comparativamente mais bem adaptada para enfrentá-la (tanto em função da natureza da sua atuação diuturna, como em função do seu maior aparelhamento institucional). Além disso, veicularia a intenção de não prejudicar a coerência e a dinâmica da política regulatória da autoridade administrativa. Dito de outro modo, a justificativa do controle judicial deferente às decisões das agências reguladoras reside, de um lado, na inadequação subjetiva e objetiva dos tribunais para a regulação; de outro, no prejuízo que a sua intervenção pode causar à política regulatória das agências.

É perfeitamente possível acreditar que a Teoria da Deferência poderá ser aplicada para os atos da Autoridade Nacional de Proteção de Dados, porém, será preciso compreender mais profundamente suas atribuições e funcionamento para que se possa ter certeza da similitude dela e das agências, cuja forma de atuação já são bem mais conhecidas no cenário brasileiro contemporâneo dado a experiência histórica já acumulada.

4 JORDÃO, Eduardo. CABRAL JÚNIOR, Renato Toledo. *A Teoria da Deferência e a Prática Judicial: Um Estudo Empírico Sobre O Controle do TJRJ À Agenersa.* Journal of Institutional Studies 2 (2018) Revista Estudos Institucionais, V. 4, N. 2, P.537-571, 2018.

Conclusão

Esses são alguns apontamentos preliminares sobre a LGPD e duas preocupações de ordem prática que ela provoca: que não haja duplicação de autoridades para fiscalizar e aplicar sanções; e, que a especialidade técnica da Autoridade Nacional seja respeitada como já são as agências que atuam nos setores regulados no Brasil.

Nesse sentido, as preocupações aqui expostas são relevantes porque na área de tratamento de dados pessoais, essenciais para atividades econômicas da maior relevância como o setor de seguros, não há tempo a perder com duplicidade de sanções ou, com a falta de reconhecimento das normas aplicáveis porque tudo isso importa em atraso, em equívocos e em perda de produção econômica.

E nesse momento, o Brasil precisa de espaço para criar, inovar, produzir e, gerar renda que possa ser equanimemente distribuída para toda a população para que possam ser cumpridos os objetivos constitucionais de construção de uma sociedade justa, livre e solidária.

Apólices em Excesso ou Apólices a Segundo, Terceiro, Enésimo Risco

WALTER POLIDO
Advogado, Árbitro em Seguros e Resseguros,
Professor universitário, Parecerista

Parece, de pronto, muito simples a teoria inerente a esse tipo de situação de subscrição, mas não tem sido assim no mercado brasileiro, uma vez que algumas inconsistências têm surpreendido os Segurados, sempre que acontecem os sinistros em apólices em excesso uma da outra. Em muitos casos, as apólices de fato não estão sobrepostas de maneira correta, sendo que essa situação gera conflitos diante da expectativa criada quando da contratação dos seguros.

O que vem a ser apólice em excesso ou apólice a primeiro, segundo, terceiro (...) risco?

Em determinados tipos de seguros e por várias razões, apólices se sobrepõem umas às outras, em Seguradoras diferentes. A Companhia com a qual o Segurado mantém relação preferencial na colocação dos seus seguros, pode, por exemplo, para um determinado risco, não aceitar a cobertura para o LMI (limite máximo de indenização) pretendido pelo Segurado, oferecendo apenas uma parte da quantia almejada. Nesse caso, o Corretor de Seguros poderá ofertar o excedente da quantia para outra Seguradora e esta emitirá uma apólice em excesso daquela primeira, integralizando o valor desejado inicialmente

pelo Segurado. Teoricamente, poderiam coexistir mais de duas apólices, ou seja, elas seriam emitidas a primeiro, segundo, terceiro, quarto e mais riscos, sem limitação. Esse modelo, todavia, não constitui o melhor padrão desejável, até porque ele implica em mais controles e trabalhos administrativos sobre os múltiplos contratos de seguros. Na eventualidade de um sinistro, de valor representativo, ele envolveria, simultaneamente, todas as apólices. Interesses financeiros também podem ensejar a repartição dos riscos seguráveis em várias Seguradoras, sem a adoção do sistema de cosseguro. O Segurado deseja atender, por exemplo, as Seguradoras que estão ligadas a bancos e com os quais ele mantém outras linhas de negócios.

Nem todos os ramos de seguros estão sujeitos a esse tipo de estrutura contratual, até porque há outros mecanismos que poderiam impactar negativamente para os Segurados, como a aplicação do rateio nos seguros de propriedades, na hipótese de o seguro da primeira apólice ser contrato com valor inferior aos interesses segurados. O ônus do infraseguro recairá sempre sobre o Segurado e ele participará proporcionalmente dos prejuízos. Os seguros de bens, sendo estabelecidos quase que majoritariamente em bases proporcionais, ou seja, quando há a possibilidade de ser estabelecido o valor real do bem/interesse e admitido este mesmo valor na condição de LMI, não são divisíveis, em tese. Com base nesse aspecto, pode ser indicado que apenas aqueles contratos de seguros comercializados a *risco absoluto* e, portanto, não sujeitos ao rateio, podem ser submetidos à contratação de mais de uma apólice: a primeiro, segundo, terceiro, enésimo risco. São os chamados seguros não proporcionais.

As apólices em excesso, com base nessas premissas, são comercializadas quase que exclusivamente para os Seguros de Responsabilidade Civil, todos eles estabelecidos a primeiro risco absoluto. De forma ampla, os Seguros do ramo RC Geral, Riscos Profissionais (E&O), D&O e Ambiental podem ser objeto de apólices com essa estrutura. Outros ramos de seguros também podem operar na base de risco absoluto e, em princípio, seria então admissível essa forma de repartição da garantia dos riscos segurados através de várias apólices.

Para a adoção desse modelo, algumas regras básicas devem ser observadas e de modo mesmo a não surgirem conflitos posteriores, mormente quando ocorrerem sinistros:

1) O clausulado aplicado na primeira apólice (primeiro risco) deverá ser o mesmo nas demais apólices (segundo, terceiro, enésimo risco). Se cada Seguradora, a partir da segunda apólice emitida em excesso da primeira, aplicar o seu próprio e respectivo clausulado, muito provavelmente ocorrerão conflitos, uma vez que os múltiplos clausulados não serão, necessariamente, semelhantes e garantidores de todas as situações previstas na primeira apólice. A utilização do mesmo e único clausulado pelas diferentes apólices em excesso uma da outra constitui a principal característica desse tipo de estrutura contratual. Não sendo observado esse pressuposto essencial, poderá representar outro tipo de situação, mas não o de apólices em excesso;

2) Usualmente, dependendo do valor do LMI da primeira apólice, o custo do prêmio ou a taxa do seguro a segundo risco será inferior, na medida em que a primeira apólice funcionará na condição de "franquia" para a segunda e assim sucessivamente, na hipótese de outras apólices funcionarem em excesso para o mesmo risco/interesse segurado;

3) As apólices a segundo, terceiro, enésimo risco não terão a aplicação de franquia

ou de participação obrigatória do segurado, na medida em que elas funcionam em excesso, respectivamente, da primeira, da segunda, da terceira .... apólice;

4) As indenizações, sempre que o montante dos prejuízos atingir várias apólices (primeiro, segundo, terceiro ... risco), não são proporcionais entre elas, sendo que cada apólice/Seguradora responderá pela integralidade da respectiva faixa ou LMI contratado e efetivamente atingido pelo sinistro coberto;

5) Primordial, em apólices de RC de forma ampla, que na determinação do LMI por Ocorrência/Sinistro, assim como do LA (Limite Agregado) pelo período anual, todas as apólices mantenham o mesmo padrão de indicação nas respectivas Especificações da Apólice, objetivamente. Se a primeira apólice consignar, por exemplo, o "LMI de $ 10.000.000,00 por Ocorrência/Sinistro" e "Agregado-anual de $15.000.000,00", as demais apólices a segundo, terceiro risco, deverão apresentar a mesma base de indicação (modificando apenas o valor), inclusive em relação ao múltiplo do LA, de forma a estabelecer perfeita simetria entre todos os contratos de seguros vigentes para aquele determinado risco/interesse. Qualquer tipo de divergência nesta demonstração gerará conflitos futuros por sinistro ou no conjunto de sinistros ocorridos durante a vigência dos respectivos contratos;

6) O prazo de cobertura deverá, necessariamente, ser o mesmo em todas as apólices contratadas para o risco/interesse. Em se tratando de seguros da área de RC de forma ampla e envolvendo D&O, E&O e Ambiental é fundamental verificar se a apólice a primeiro risco determina período de cobertura diferenciado, além do prazo de vigência anual em si. Poderá estar consignado, na mencionada apólice, o "período ou a data de retroatividade de cobertura", em se tratando de seguro contratado à base de reclamações *(claims made)*, quando então todas as demais apólices em excesso daquela deverão especificar a mesma data ou período de retroatividade. Qualquer omissão ou divergência neste sentido poderá repercutir em discussões prolongadas, enquanto que as apólices em excesso devem, necessariamente, se apresentar de maneira harmônica. As Seguradoras que se propuserem a operar a partir deste modelo, devem estar preparadas para o ônus que fatalmente recairá sobre elas, ainda que tenham omitido informação crucial nas respectivas Especificações da Apólice. Os princípios técnicos inerentes devem prevalecer sobre a simples forma do contrato, de modo que os legítimos interesses dos Segurados sejam perfeitamente respeitados. Desse modo, não seria cabível, por exemplo, a Seguradora emitir a apólice em excesso de outra e, uma vez ocorrendo o sinistro, pretender alegar que a cobertura para o "período de retroatividade", consignado expressamente na primeira apólice, não fazia parte do referido contrato de seguro. Ainda que seja constatada a omissão deste importante item na apólice a segundo risco, pelo fato de ela ter sido emitida em excesso, deverá prevalecer o pressuposto de que todos os elementos constantes daquela primeira apólice serão aplicados, incondicionalmente, nesta segunda apólice. Do mesmo modo, a apólice em excesso não poderá conter clausulado diferente daquele da primeira apólice e sob a alegação de que a Susep exige o número de registro na apólice do produto da Seguradora emitente. Ora, se essa exigência normativa de fato existir, então ela deverá ser revogada, uma vez que a referida Autarquia estaria impedindo a prática de emissão de apólices em excesso no

Brasil, cujo procedimento é aceito internacionalmente. Esse pretenso impedimento, portanto, colocaria o mercado segurador nacional em desvantagem e de forma completamente injustificável, cabendo às entidades de classe, CNSeg, FenSeg, Fenacor agirem junto à Superintendência Nacional de Seguros, de modo a pleitearem a devida solução para o caso. Os Corretores de Seguros, por sua vez, têm a obrigação profissional de conferir e fazer respeitar todos os princípios inerentes às apólices em excesso, demonstrando as eventuais inexatidões às respectivas Seguradoras envolvidas quando da fase inicial das negociações pertinentes. Para isso, eles são devidamente comissionados, enquanto intermediários dos Segurados junto às Seguradoras. De outra forma, poderão ser instados a responder civilmente por suas respectivas omissões, assim como é devido a qualquer outro prestador de serviço especializado, até porque a compreensão de todo o detalhamento demonstrado neste texto não pode ser um ônus do Segurado, comumente leigo na área securitária;

7) Importante, ainda, que as apólices em excesso contenham expressamente a informação de que toda e qualquer eventual modificação realizada na apólice a primeiro risco deverá ser, concomitantemente, informada às demais Seguradoras envolvidas, sob pena do não reconhecimento da referida alteração que possa onerar as Seguradoras. Assim, por exemplo, se a Seguradora da apólice a primeiro risco emitir um Endosso ampliando determinada cobertura ou incluindo novo local em risco, esses fatos deverão ser prontamente comunicados às respectivas Seguradoras das apólices em excesso, sem exceção;

8) Por último, é importante que nas Especificações da Apólice, de todos os contratos de seguros emitidos (primeiro, segundo, terceiro ... risco), haja a expressa menção no sentido de que não prevalecerão os termos da "Cláusula de Concorrência de Apólices" prevista nas Condições Gerais, uma vez que a apólice foi contratada a primeiro, segundo, terceiro (...) risco, aplicando-se em excesso uma da outra. Importante, ainda, que todas as apólices contenham a indicação dos respectivos LMI/LA em excesso, assim como o nome de cada Seguradora envolvida, considerando-se que os demais elementos contratuais serão idênticos para todas elas e com base na apólice a primeiro risco.

Os Corretores de Seguros devem analisar todas essas situações encontradas nas apólices em excesso, pontualmente, em relação a todos os seus clientes-segurados, buscando a alteração imediata das bases ofertadas pelas Seguradoras, na hipótese de os termos das apólices vigentes não se encontrarem em conformidade à teoria expressa neste texto. Para os novos seguros, a observação de todos os pontos é de crucial importância e de modo a serem evitados conflitos, notadamente quando os sinistros de fato acontecerem, sendo que eles sempre acontecem.

Os Impactos da Lei Geral de Proteção de Dados no Mercado de Seguros e Resseguros

MARCIA CICARELLI BARBOSA DE OLIVEIRA

CAMILA AFFONSO PRADO

LAURA PELEGRINI

DEMAREST

A Lei nº 13.709/18, conhecida como Lei Geral de Proteção de Dados ("LGPD"), causará relevante impacto em diversos setores e indústrias que realizam o tratamento de dados pessoais de indivíduos. Dentre aqueles, o mercado de seguros, resseguros e corretagem será inegavelmente afetado e, portanto, deverá se adaptar às novas disposições da lei até 15/08/2020, quando entrará em vigor.

Em resumo, a LGPD foi inspirada na legislação europeia denominada "General Data Protection Regulation – GDPR" e tem por objetivo proteger a liberdade, a privacidade e o livre desenvolvimento da personalidade dos indivíduos, garantindo-lhes maior controle sobre o uso de suas informações pessoais.

Isso significa que as regras da LGPD deverão ser observadas em todas as operações de tratamento de dados realizadas no Brasil ou, ainda que o tratamento ocorra em território estrangeiro, quando os dados pessoais tiverem sido coletados no Brasil ou pertençam a indivíduo que se encontre no território nacional[1]. Em outras palavras, a LGPD poderá alcançar empresas que não possuem estabelecimento no Brasil, mas que exercem algum tipo de atividade local que envolva o tratamento de dados pessoais, tal como ocorre com os resseguradores eventuais.

A abrangência da LGPD também é evidenciada pela própria definição do que seja o "tratamento de dados pessoais". Segundo o artigo 5º, inciso X, este tratamento abarca "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

Ou seja, qualquer operação com dados pessoais de indivíduos, seja manual ou digital, estará sujeita à LGPD. As poucas exceções estão previstas no artigo 4º[2], que, por sua vez, não se aplica às atividades desenvolvidas pelo mercado segurador, ressegurador e de corretagem.

É importante ressaltar que o tratamento de dados pessoais não pode ser realizado de modo discricionário e irrestrito, sendo autorizado tão somente em dez hipóteses estabelecidas no artigo 7º[3], mediante observância dos princípios elencados no artigo 6º[4], como os da finalidade, adequação, necessidade e transparência.

---

1 Art. 3º "Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. §1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. §2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei".

2 Art. 4º "Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei".

3 Art. 7º "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente".

4 Art. 6º "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações

Assim, os corretores, seguradoras e resseguradores apenas poderão, em geral, acessar, utilizar, armazenar ou transferir os dados pessoais dos proponentes ou segurados pessoas físicas dentro das hipóteses legais elencadas no artigo 7º

Na prática securitária, considerando que o contrato de seguro depende de proposta enviada pelo segurado, há discussões sobre o enquadramento na hipótese do inciso V, que trata da execução do contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, desde que a pedido do titular dos dados. Tratando-se a proposta de uma fase preliminar à formação do contrato e considerando que a lei prevê "o pedido do titular dos dados", fica a dúvida sobre em que medida esse pedido difere do consentimento previsto no inciso I do artigo 7º

Com relação ao consentimento, o "controlador", pessoa natural ou jurídica, será o responsável pelas decisões referentes ao tratamento de dados pessoais, bem como pela obtenção do consentimento do titular (quando aplicável), de acordo com os artigos 5º, VI, e 7º, §5º

Nesse sentido, a solicitação de consentimento deve conter informação clara ao titular sobre a finalidade específica do tratamento dos dados, sendo vedado o tratamento posterior de forma incompatível com a finalidade previamente informada. Deve-se notar que o consentimento genérico será nulo, cabendo às companhias o ônus da prova de que o consentimento foi obtido nos termos da LGPD, em conformidade com os §§ 2º e 4º do artigo 8º

Além disso, deve-se observar que a transferência de dados pessoais para país estrangeiro, que poderá ocorrer quando resseguradores admitidos e eventuais estiverem envolvidos, somente será permitida nas hipóteses do artigo 33[5]. São os casos, por exemplo, de países que proporcionam grau de proteção de dados pessoais adequado à LGPD, tais como os países da União Europeia; quando a autoridade nacional autorizar a transferência; quando o controlador oferecer garantia contratuais de proteção; ou quando o titular tiver fornecido consentimento específico e em destaque para tal transferência, com informação prévia sobre o caráter internacional da operação e distinção clara desta de outras finalidades.

Ainda, não é apenas o tratamento dos dados pessoais que está sujeito à LGPD, como o nome, endereço, número de RG e CPF, ou e-mail[6]. Os dados sensíveis, previstos no artigo 5º, inciso II, tais como

claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

5 Art. 33. "A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos; III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; V - quando a autoridade nacional autorizar a transferência; VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei".

6 Segundo o artigo 5º, I, dado pessoal é a "informação relacionada a pessoa natural identificada ou identificável".

origem racial, convicção religiosa, orientação sexual e informações referentes à saúde, apenas poderão receber tratamento em hipóteses mais específicas, elencadas no artigo 11[7]. Tratando-se do mercado de seguros, resseguros e corretagem, discute-se se esta hipótese dispensaria o consentimento por se enquadrar como exercício regular de um direito no âmbito contratual, por exemplo no seguro saúde; ou, se ainda assim, será necessário que o titular ou responsável legal tenha consentido com o tratamento dos dados sensíveis, inclusive como medida de cautela das companhias.

Obtido o consentimento, deverão ser adotadas medidas de segurança para a proteção dos dados pessoais a fim de evitar acessos não autorizados, destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito, de acordo com o artigo 46.

A Autoridade Nacional de Proteção de Dados, criada pela Medida Provisória nº 869/2018, poderá, inclusive, dispor sobre padrões técnicos mínimos para garantir a segurança dos dados pessoais, principalmente dos dados sensíveis. Nessa linha, é possível que futuramente a SUSEP também defina requisitos específicos a serem seguidos pelo mercado, tal como o fez o Banco Central ao publicar a Resolução nº 4658/2018, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras.

Dessa forma, é recomendável que corretores, seguradoras e resseguradores desenvolvam, desde já, plano de ação para implementar e manter políticas de segurança cibernética, de prevenção e resposta a incidentes. Para tanto, será necessário mapear os tipos de dados, seu fluxo e a finalidade da coleta, bem como os responsáveis pelo tratamento dos dados. As companhias também deverão adaptar suas práticas e documentos a fim de obter consentimento prévio do segurado sempre que necessário, de forma clara e específica, atentando para as situações de transferência dos dados a terceiros.

Ocorrido um incidente de segurança, o controlador responsável deverá comunicar tanto o titular dos dados pessoais como a própria Autoridade Nacional de Proteção de Dados, em prazo razoável a ser por esta definido. A comunicação deverá conter as informações mínimas previstas no §1º do artigo 48[8] e, a depender da gravidade do incidente, a autoridade nacional também poderá determinar ao controlador a ampla divulgação do fato nos meios de comunicação, e a adoção de medidas para reverter ou mitigar os efeitos do incidente, nos termos do artigo 48, §2º

Além disso, o controlador ou o operador poderão ser responsabilizados civilmente pela reparação dos danos materiais ou morais, individuais ou coletivos, causados

7 Art. 11. "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais".

8 Art. 48, §1º "A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo".

aos titulares dos dados violados. A responsabilidade será objetiva e as excludentes serão admitidas em apenas três hipóteses previstas no artigo 43: quando os agentes de tratamento provarem (i) que não realizaram o tratamento de dados pessoais que lhes é atribuído; (ii) que, embora tenham realizado o tratamento de dados pessoais, não houve violação à legislação de proteção de dados; ou (iii) que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Por fim, os agentes de tratamento de dados também estarão sujeitos a sanções administrativas aplicáveis pela autoridade nacional, as quais variam desde advertência; multa de até 2% do faturamento, limitada ao total de cinquenta milhões de reais; e publicização da infração; até o bloqueio ou eliminação dos dados pessoais a que se refere a infração.

Vê-se, portanto, que o atual cenário exige conciliar o dever de proteção de dados e o gerenciamento dos riscos cibernéticos em uma sociedade digital marcada pelas novas tecnologias, fácil acesso e fluxo dinâmico de informações. Neste contexto de riscos de incidentes elevados e incremento das responsabilidades, o seguro de riscos cibernéticos tem se mostrado como um importante instrumento de prevenção e mitigação de danos.

Desde a promulgação da LGPD, houve um aumento de cerca de 116% na demanda por apólices de seguro de riscos cibernéticos[9]. Este aumento parece estar relacionado não apenas à criação de uma série de deveres que visam à proteção e tratamento dos dados pessoais, mas também à obrigação de notificação dos incidentes à Autoridade Nacional de Proteção de Dados e aos titulares dos dados pessoais.

Antes da promulgação da LGPD inexistia previsão expressa sobre o dever de notificação e, consequentemente, a cobertura de responsabilidade civil das apólices de *cyber* raramente era acionada. Com o início de vigência da LGPD, qualquer incidente deverá ser notificado, acarretando em uma maior exposição das empresas que realizam o tratamento de dados justamente diante da responsabilidade pela reparação dos danos causados a terceiros. Esta, ao nosso ver, é uma das causas que inegavelmente tem acarretado no aumento da procura pelo seguro.

Mas, além da cobertura de responsabilidade civil, as apólices também garantem cobertura para os danos sofridos pelo próprio segurado, como por exemplo, os custos de notificação, monitoramento e mitigação de um incidente; de restituição de imagem; e de extorsão na Internet.

O escopo das apólices é ainda mais abrangente, pois, em geral, confere cobertura a um conjunto de serviços e acesso a profissionais especializados em diversas áreas para agir prontamente no momento da ocorrência de um incidente e na mitigação dos danos.

Desta forma, são diversos os impactos da LGPD no mercado segurador, seja em relação às medidas e políticas a serem adotadas com vistas à adaptação dos modelos de negócios às novas regras de proteção e tratamento de dados pessoais, seja quanto ao incremento da demanda pelo seguro de riscos cibernéticos e esperado aumento do número de sinistros em razão do dever de notificação dos incidentes.

O debate em torno destes impactos é recente, razão pela qual este artigo não tem a pretensão de esgotar o tema. As discussões são relevantes e envolvem uma mudança paradigmática de cultura e adaptação às novas regras. Por isso, os corretores, seguradoras e resseguradores devem começar, desde já, a analisar o tema e a desenvolver suas políticas internas de *compliance* mediante integração das diversas áreas como tecnologia da informação, jurídico, marketing e pesquisa e desenvolvimento.

9 Dado divulgado por Willis Tower Watson e publicado no Valor Econômico, em 25/12/2018. Disponível em: https://www.valor.com.br/financas/6037891/procura-por-%3Fseguro-ciber%3F-mais-que-dobra-apos-lei-de-dados. Acesso em 15/04/2019.

Solvency requirements for Insurers in Europe and Brazil – A comparative law analysis

CARSTEN FRANZ OTTO[1]
Foreign Associate DR&A Advogados

As a result of the financial crisis of 2007, the European Union introduced new solvency requirements for the big players on the financial markets: banks, asset managers and insurances. The legislation for the latter was done through the directive 2009/138/EC on the taking-up and pursuit of the business of insurance and reinsurance (hereafter **Solvency II**).

The main goal of the new directive was the protection of the insured and the financial stability of the insurance companies and subsequently of the financial markets. The solvency II directive consists of three pillars:

- Solvency requirements;
- Requirements for governance and risk management of insurers; and
- Disclosure and transparency requirements.

The guidelines follow a risk-based approach, similar to the Basel II regulation,

1 Franz Carsten Otto graduated from the University of St. Gallen (Master of Law and Economics) in 2018 and has completed exchange programs from the Université de Fribourg and the University of California, San Diego. Prior joining DR&A Advogados, Carsten worked in international law firms in Zurich and Prague as well as in a legal department of a Swiss financial service provider.

which is applicable to the international banking system.

As a directive, Solvency II is not directly applicable and must be implemented into the national law of the member states. It sets a minimum standard, but leaves the member states with a certain amount of leeway on how the rules are adopted. As the European Union is the biggest single market in the world, legislation from the EU has an extraterritorial effect on other states that aim to access and participate in the European Market. Therefore, states – as for example Switzerland and Bermuda (both non-EU members) – have already adapted their insurance law in accordance with Solvency II and are deemed as "equal jurisdictions" for reinsurance and group solvency requirements. Insurers from those countries therefore do not have to comply with Solvency II regulation when operating in the European market as long as they fulfil their national solvency requirements. Brazils insurance authorities also seek to receive an equivalence status to Solvency II from the European Insurance and Occupational Pensions Authority (EIOPA), as Brazil has established a risk-based capital assessment mechanism following the Solvency II guidelines.

The following article shall explore the solvency requirements for insurers in the EU directive and compare it with the current legislation of Brazil.

Whereas in Brazil the Conselho Nacional de Seguros Privados (CNSP) and Superintendência de Obras e Serviços Públicos (SUSESP) are supervising insurances, in the European Union, the EIOPA is responsible for Solvency legislation. However, the national supervisory authorities of the member states are responsible for the implementation and the enforcement of the European rules. Moreover, the national supervisory authorities can introduce further rules and requirements but may not go below the minimum standards as set in Solvency II.

Both jurisdictions differentiate between minimal capital requirements (**MCR**) and solvency capital requirements (**SCR**).

In Brazil, insurers must continuously meet the MCR which is the higher value between the base capital and the risk capital. The base capital is composed by a fixed amount depending on the offered insurance (e.g. life insurance, reinsurance) and a surplus depending on the federal states the insurance company operates in. Therefore, the base capital varies between R$ 1,200,00-15,000,000. The risk capital is calculated according to the sum between capital instalments based on the risk of underwriting, credit, operation and market.

In the European Union, legislation solely focuses on the probability of the insurers to meet all their obligation over the following twelve months. Assets and liabilities are assessed according to international accounting standards. The capital requirement therefore depends on the potential risks and the future obligation of the insurers and must meet those with a probability of 85%. Several member states have furthermore introduced sump-lump capital requirements depending on the offered insurance (e.g. Polish life insurers must have a minimum base amount of 3.6 million EUR.). The underlying risk margin is either calculated according the following formula or by using its own internal model approved by the respective Central Bank:

$$RM = CoC \cdot \sum_{t \geq 0} \frac{SCR\,(t)}{(1+r\,(t+1))^{\,t+1}}$$

where:

- CoC denotes the Cost-of-Capital rate;
- the sum covers all integers including zero;
- SCR(t) denotes the Solvency Capital Requirement referred to in Article 38(2) after t years;

- r(t + 1) denotes the basic risk-free interest rate for the maturity of t + 1 years.

The solvency of the assets is calculated according its characteristics (FX Swaps, fixed income bonds, but also denomination, liquidity etc.) following again a complex mathematical model. A deeper explanation of the underlying mathematical assessment is however not done in this article.

In both jurisdictions, the minimal capital requirements and the solvency capital requirements are closely connected. Whereas Solvency II requires that the insurer must be able to meet all its obligations over to following 12 months with a 99,5% probability, Brazilian insurers must meet the highest of the following values:

- Base capital + Risk capital as outlined above;
- 0,2 x total net revenue from premiums; and
- 0,33 x the annual average of total claims of the last 36 month.

As long as Brazil does not obtain an equivalence status, European insurers operating in Brazil have to comply with the Brazilian solvency requirements and vice versa. However, the implementation of the risk-based capital requirement approach in the EU already effects the Brazilian market. As a result, higher overall capital requirements were introduced, and it is likely that insurers adjust their product and business mix in order to optimize their regulatory capital consumption.

Finally, reinsurances, as a regulatory capital management tool, might be used more often in Brazil as it can offer capital reliefs under the new solvency regimes.

Impactos da Lei de Proteção de Dados

(Lei nº 13.709, de 14 de agosto de 2018) nas Atividades de Seguros no Brasil

DANIELLE DJOUKI

Diretora Jurídica e de Compliance na Fairfax Brasil Seguros Corporativos S/A, com MBA em Gestão Empresarial pela FGV-SP e extensão internacional em Stanford Unversity nos EUA em Inovação e Intersecção entre Pessoas e Tecnologia da Informação, pós-graduada pela PUC/SP em Direito das Relações de Consumo, pós-graduada pela FMU/SP em Direito Empresarial, vice presidente da Comissão de Compliance da AIDA Brasil.

LILLIAN CASTILHO MENINI

Advogada, Mestre em Direito Político e Econômico (Universidade Presbiteriana Mackenzie/SP), Pós-Graduada em Gestão de Negócios Bancários (FIA-FEA/USP) e em Direito Empresarial (PUC/SP).

Nos últimos dias 21 e 22 de março de 2019 ocorreu o XIII Congresso Brasileiro de Direito de Seguro e Previdência da AIDA Brasil em Campo Grande – MS, sendo que um dos painéis de discussão no GNT – Direito Regulatório e Compliance, GNT Linhas Financeiras e GNT – Relações de Consumo, foi justamente a Lei de Proteção de Dados.

As discussões foram ricas e as dúvidas e preocupações do mercado nacional brasileiro de seguros foram várias.

O objetivo deste trabalho é comentar as principais questões discutidas no grupo e possíveis soluções.

A Lei de Proteção de Dados (Lei nº 13. 709, de 14/08/2018) entrará em vigor em agosto de 2020, caso a Medida Provisória nº 869/2018, que alterou a vigência desta Lei, de 18 meses para 24 meses, seja convertida em lei até abril de 2019. Caso contrário, em fevereiro de 2020, todo o mercado brasileiro deverá estar adequado aos termos da referida Lei.

Em linhas gerais, a Lei de Proteção de Dados positivou a necessidade da obtenção do consentimento prévio do titular dos dados pessoais para o seu tratamento e

utilização; exige que seja informado ao titular os motivos para os quais os dados serão utilizados; permite a portabilidade dos dados, nos termos da lei; garante o direito à eliminação dos dados por solicitação de seu titular; cria a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

É importante que as seguradoras já nomeiem o encarregado, que estará responsável pelas comunicações entre o controlador (no caso as seguradoras) e a autoridade nacional, bem como o operador (pessoa que realizará o tratamento de dados).

As áreas de tecnologia, jurídico, compliance, segurança da informação e controles internos deverão trabalhar em conjunto nas ações estratégicas e operacionais para a implantação dos controles internos de proteção de dados. As áreas deverão ser mapeadas, objetivando identificar àquelas que têm acesso aos dados pessoais; definir quais dados pessoais dos segurados precisam ser obtidos durante a operação do seguro; quais pessoas (níveis hierárquico e funções) deverão ter acesso aos dados pessoais; para qual finalidade os dados pessoais serão utilizados; definir as soluções tecnológicas para segregar as informações, limitar os acessos, anonimizar dados, inserir cláusulas nos contratos a respeito da proteção de dados, dar treinamentos aos colaboradores, etc.

Como ponto de partida para tal trabalho, discutiu-se a importância de focar nos princípios que norteiam a Proteção de Dados: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Neste aspecto torna-se importante saber quem são as pessoas sujeitas à proteção de dados, quais situações a legislação dispensa o tratamento, como deve ocorrer o consentimento e a responsabilidade de todos os parceiros de negócios e terceirizados envolvidos na operação de seguros.

Sendo assim, da análise do artigo 1º e 5º da Lei de Proteção de Dados, é possível entender que a pessoa natural, o segurado pessoa física, é quem deve ter seus dados pessoais protegidos. O segundo conceito importante para a definição das ações estratégicas na companhia, é que a atividade de tratamento tenha por objetivo a oferta de produtos e/ou serviços. Significa dizer, que toda vez que a empresa abordar um cliente, pessoa física, para a oferta de seus produtos e/ou serviços, utilizando-se de base de dados adquirida em outra ocasião, como exemplo um simples pedido de cotação de seguro, precisa ter a prévia autorização para tal abordagem.

Partindo de tais premissas, o trabalho de adequação na companhia deve levar em consideração as hipóteses em que o tratamento de dados pode ser realizado. Neste aspecto, entende-se por tratamento, conforme previsto na referida Lei "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

A pessoa física que terá seus dados tratados, precisa receber informações claras e precisas sobre o objetivo e finalidade da utilização de tais dados pela seguradora (ora controlador, conforme previsto na Lei de Proteção de Dados). No que se refere às operações de seguro, importante alertar o titular dos dados pessoais, que as informações também poderão ser compartilhadas com congêneres, na cessão de cosseguro, e resseguradores, já que o § 5º artigo 7º da Lei de Proteção de Dados, dispõe sobre a

obrigatoriedade do consentimento, em caso de compartilhamento de dados pessoais com outros controladores.

Quando o consentimento é necessário e dispensável? Há necessidade de tratamento, quando o consentimento não for necessário? Toda vez que houver a utilização dos dados pessoais da pessoa física para a oferta de produtos e/ou serviços, o consentimento é imprescindível, ao passo que não é necessário o consentimento se os dados forem utilizados para o cumprimento de obrigação legal ou regulatória da seguradora; para a execução do contrato de seguro, a exemplo a regulação de sinistro; no exercício regular de direitos em processo judicial, administrativo ou arbitral; para a proteção do crédito; para atender interesses legítimos do controlador ou de terceiro, desde que não infrinja direitos e liberdades fundamentais do titular dos dados pessoais. No entanto, a dispensa do consentimento não dispensa a obrigatoriedade do tratamento, que deverá ser sempre observado.

Outra questão colocada em discussão, é a responsabilidade da seguradora nas apólices coletivas de seguro, em que há a figura do estipulante que mantém o contato com o titular dos dados pessoais, ou mesmo, corretores de seguros intermediando contratações, encampações e transferência de apólices. Como fica a questão do consentimento? O consentimento, mesmos nestas situações, continua sendo necessário para a oferta de produtos e/ou serviços e compartilhamento de informações com outros controladores. A seguradora, sempre que possível, deve obter o consentimento expresso do titular dos dados pessoais, podendo, inclusive, tal consentimento ser dado através de meios eletrônicos. Na pior das hipóteses, em que o consentimento é obtido pelo estipulante ou corretor de seguros, deve a seguradora se resguardar contratualmente no direito de regresso em eventual reparação de danos consequente da ausência de consentimento.

Discutiu-se outro ponto sensível para o mercado segurador: a anonimização dos dados. Quais seriam os meios técnicos razoáveis e disponíveis para tal procedimento? Deve-se anonimizar os dados para uso interno, externo ou ambos? As seguradoras utilizam os dados para estatísticas, fixação de prêmios, estudos de mercado, desenvolvimento de novos produtos. Assim, os limites da anonimização precisam ser definidos para que as seguradoras não percam essa fonte de aprimoramento do mercado de seguros.

A Lei de Proteção de Dados é geral e principiológica e, nesse sentido, previu a necessidade de cada setor se organizar e formular suas próprias regras de boas práticas e de governança que "estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais".

Portanto, o mercado deverá se adequar e rápido, às mudanças trazidas por esta Lei, que representa grande avanço à proteção dos direitos dos consumidores e aos princípios constitucionais da dignidade da pessoa humana e intimidade.

A importância da assistência técnica em perícias atuariais

HEITOR RIGUEIRA
Consultor Atuarial

HR Serviços Atuariais Ltda.

A profissão atuarial ganhou amplitude nos últimos anos, indo além das áreas disciplinadas nos Decreto-Lei nº 806/69 e Decreto nº 66.408/70, atingindo diversas outras, tais como os setores financeiros e de compliance. Da mesma forma, é nítida a interação do atuário com outros profissionais como o contador, o economista, o advogado, e também com atividades do setor social.

A formação acadêmica do atuário, centrada principalmente nas áreas matemática, estatística e de informática, o caracteriza modernamente como um avaliador de riscos não só do ponto de vista quantitativo, mas também do ponto de vista qualitativo, ainda que seu campo de trabalho esteja fortemente centrado nos segmentos de seguros e previdência.

Assim, o trabalho do atuário está basicamente ligado a cálculos, tendo como consequência a formalização contratual, quando interage, como dito, com outros profissionais, particularmente com o advogado. É de relevante significância nos desenhos e apuração do custo dos produtos a perfeita adequação do equilíbrio técnico com o descrito nos regulamentos e/ou condições gerais que compõem os contratos entre as partes, de uma maneira geral classificadas por segurador e segurado, sejam através de contratos individuais ou coletivos.

Em que pese o acordo das partes na contratação, é inevitável que discordâncias

ocorram no curso da vigência do contrato ou mesmo após o seu vencimento, que não podendo ser resolvidas administrativamente desatam numa demanda judicial.

Infelizmente, a judicialização ganhou um porte incomensurável no Brasil, alcançando número superior a cem milhões de processos.

Quando ocorrem demandas contra uma seguradora, entidade de previdência privada e operadora de plano de saúde, muitas das vezes são reclamações de pessoas ou grupos de pessoas que se consideram prejudicadas com o não cumprimento do contrato por parte da contratada, podendo ter reflexos financeiros relevantes sobre o pacto mutualista em que se centra, de uma forma geral, todo este segmento de atividade, podendo até atingir outras situações similares.

Também não é incomum demandas entre pessoas jurídicas, tendo de um lado uma seguradora, entidade de previdência privada ou operadora de plano de saúde e do outro lado empresa contratante para si ou para seus empregados/colaboradores. Nestes casos, estão em conflito discussões de custeio dos produtos contratados que geralmente envolvem matéria de cunho atuarial, importando muita das vezes em valores significativos, sendo algumas destas demandas levadas a procedimento de arbitragem.

Os Tribunais têm verificado o crescimento do número de ações nas atividades de seguros e previdência, que muita das vezes acabam chegando ao STJ (Superior Tribunal de Justiça). Este, ao verificar a ocorrência de temas repetitivos, têm convocado os órgãos associativos (CNSeg e suas federações, Abrapp, Abramge dentre outros) para opinar sobre tema de interesse dos seus filiados. Por entender que a matéria técnica tem relevância na discussão, o STJ também tem convocado o IBA (Instituto Brasileiro de Atuária), órgão de classe dos atuários, como *Amicus Curiae* e solicitado a emissão de parecer sobre questões em que consideram importante à oitiva técnico-atuarial.

Diante de todo este contexto, as partes litigantes em demandas onde se vislumbra que o cerne da discussão é o desequilíbrio de valores entendidos como devido pelas partes, têm, por meio de seus advogados, requerido a instalação de perícias atuariais, o que também pode vir a ser promovido por iniciativa do próprio Juízo quando considera este procedimento imprescindível para solução da demanda.

No passado era muito comum a nomeação de peritos não atuários (principalmente contadores ou economistas) em discussões técnicas cujo fulcro era a matéria atuarial. Atualmente esta questão vem sendo revertida e é frequente a nomeação de atuários para realização de pericias atuariais, como disciplina, aliás, a lei da profissão do atuário (art 5º do Decreto-Lei nº 806/69) a seguir transcrito:

> *Art. 5° Compete, privativamente, ao Atuário:*
>
> .....
>
> *f) a peritagem e a emissão de pareceres sobre assuntos envolvendo problemas de competência exclusivamente do atuário.*

Entretanto, a seguradora, entidade de previdência e operadora de plano de saúde, que têm o dever fiduciário de bem resguardar o equilíbrio financeiro-atuarial de suas atividades, devem ter toda a atenção ao fornecer os elementos técnicos para os seus advogados.

Quando verificado que o tema objeto da demanda tem envolvimento com aspectos atuariais, é importante que seja requerida perícia atuarial ainda na fase de conhecimento do processo, principalmente se as consequências financeiras que possam advir não só naquela ação, mas também em outras subsequentes com o mesmo fato de pedir, são negativas.

É neste momento que os fundamentos técnico-atuariais devem ser objeto de discussão antes de se partir para a etapa dos cálculos.

Definida pelo Juízo a realização da perícia técnica, é importante que o advogado conte com assessoria atuarial já na elaboração da quesitação que deve ser conduzida de modo a que as respostas do perito do Juízo convirjam com a tese defendida.

A assessoria atuarial deverá funcionar como assistência técnica nos autos do processo com o objetivo de interagir com o perito do Juízo fornecendo os subsídios para a resposta aos quesitos das partes, assim como deverá avaliar as perguntas da demandante de modo a se contrapor, total ou parcialmente, conforme a situação.

Infelizmente, o que se verifica hoje é que nem sempre há a cautela por parte da demandada em relação a função do assistente técnico na realização das perícias atuariais, que muitas das vezes se torna um mero fornecedor de informações para o perito, sem a preocupação de tentar esclarecê-lo da questão e ser parte na defesa da posição da demandada. E, em consequência, se observa ao final perdas econômicas significativas para o mutualismo, podendo levar, dependendo da situação, à insolvência das operações.

Nas perícias atuariais, em fase de conhecimento do processo, não são os cálculos atuariais que inicialmente devem ser postos; eles são consequência das discussões técnicas que devem apreciar os fundamentos da questão em debate em relação à parte técnica e aos dispositivos contratuais.

Nos processos judiciais, a disciplina da condução das etapas é sem dúvida alguma dos fundamentos jurídicos; porém, s.m.j., nestas discussões de ordem técnico-atuarial a matéria técnica deve vir logo à tona. Não é prudente deixar a fase pericial só para a liquidação. Ela deve ser tratada, logo de saída, na fase de conhecimento ou instrução, sob pena de que a perícia de liquidação venha a ser apenas para que se proceda os cálculos como sentenciado. Nesta fase, as discussões ficam bem mais restritas e difíceis, pois embora os textos condenatórios, quando envolvam cálculos, nem sempre sejam plenamente descritos, a perda muita das vezes já está consumada e o trabalho se limitará apenas a minimizá-la.

Assim, concluindo, o presente artigo serve como oportunidade para mostrar mais uma atividade onde o atuário pode colaborar com a administração nestes segmentos de atividade securitária, auxiliando os advogados em demandas judiciais onde seja requerida a perícia atuarial.

Planejamento Financeiro e a IFRS17

JOEL GARCIA
Sócio da área de Accountig & Financial Risk da KPMG Brasil e é um dos líderes de projetos de implementação de IFRS17. Possui mais de 23 anos de experiência em seguros tendo atuado em empresas de grande porte dos segmentos de seguros, resseguros e previdência com experiência nas áreas de controle, gestão de preços, atuarial e resseguros. Em IFRS17, Joel lidera projetos de modelagem, classificação de produtos, gerenciamento de dados e simulações de impactos financeiros."

O mercado global de seguros continua avançando com seus desafios no processo de implementação dos requerimentos da IFRS 17 (que diz respeito aos contratos de seguros e que passa a vigorar em 1º de janeiro de 2022). Dentre os grandes temas mais conhecidos e que compõem os projetos de implementação tem-se Pessoal & Treinamento, Processos & Governança, Produtos, Modelos Atuariais, Tecnologia & Dados.

O que para alguns ainda parece ser um tema restrito às áreas de contabilidade e atuarial, tem revelado um espectro bem mais amplo quanto aos impactos numa companhia de seguros. Por outro lado, destaca-se a necessidade de foco para tópicos de gestão, comunicação com o mercado e visão dos stakeholders externos. Novas métricas de performance e base de comparação com indicadores tradicionais do setor, novas informações a serem comunicadas ao mercado, percepção de analistas e agências, assim como efeitos no valor das ações das companhias de seguros constituem um bloco relevante a ser monitorado pela liderança das seguradoras em seus projetos de implementação.

Neste contexto de transformação, um tema chave que será impactado é o processo de orçamentação que geralmente é feito para períodos de 3 a 5 anos, portanto é relevante pensar nisso desde agora, com projeções de resultados baseados em expectativas operacionais de receitas e despesas e resultados financeiros cujo reconhecimento no resultado poderá ser significativamente impactado com a introdução da nova norma. Por exemplo, produtos de longo prazo, principalmente aqueles acima de 3 anos, terão seus resultados apurados considerando o valor presente da expectativa de resultados de todo o período de vigência futura do contrato, o que difere substancialmente do modelo atual.

Tendências do cenário econômico e de negócios deverão ser estimadas e registradas antecipadamente nos balanços

deixando de ser algo a ser reconhecido no resultado de cada ano na visão de curto prazo e isso também será desafiador para todo o mercado. Diante deste cenário, algumas perguntas devem ser feitas nesse momento pelos executivos das seguradoras tentando antecipar os desafios que enfrentarão quando da adoção da norma.

- Como a IFRS17 afetará as métricas e indicadores de performance?
- O que devo divulgar nesse novo mundo?
- Como vou comunicar com analistas e investidores no futuro?
- Como vou comunicar o que a IFRS17 significa para o negócio?
- Como vou treinar minha Administração nessa nova maneira de ver o negócio?
- O que a IFRS17 significa para o resultado e como este irá se comportar num cenário de stress?
- Como vou planejar nessa nova base de apuração?

Algumas seguradoras já iniciaram o diálogo com o mercado e as primeiras reações ao que é apresentado são de apreensão que pode estar relacionado com o baixo nível de compreensão da nova forma de reportar, o que é natural, mas pode gerar incerteza ao analista sobre a adequação das análises feitas no modelo atual de contabilização diante do que se apresenta no novo modelo, o que pode impactar, por exemplo, o preço das ações.

Na visão da KPMG uma abordagem de trabalho para superar esse desafio deve contemplar ao menos os seguintes aspectos:

1. Compreender o que obrigatoriamente deve ser divulgado para estabelecer um baseline como ponto de início das análises;
2. Avaliar o impacto em métricas de desempenho e performance a partir de simulações preliminares. Essa etapa mostrará que:

   Algumas medidas permanecerão como são hoje, a exemplo do caixa real e da cobertura de dividendos;

   Algumas medidas passarão a ser redundantes no futuro gerando oportunidade de ganhos de eficiência, como por exemplo o Embedded Value;

   Outras medidas serão substituídas por novas tais como, o valor de novos negócios, que passará a ser divulgado; e

   Algumas medidas deverão ser ajustadas no novo modelo de apuração e então recalibradas, um exemplo disso, é o Índice Combinado.
3. Acompanhar o andamento desses KPIs e métricas durante o processo de "dry run" da implementação da IFRS17.
4. Realizar o refinamento, aprofundamento e enriquecimento das métricas a partir do conhecimento adquirido durante as etapas do projeto. Uma atividade importante nesse processo é o entendimento de como essas métricas se comportarão diante de cenários de stress, o que permitirá a adoção de medidas de mitigação desses impactos.
5. Por fim, iniciar a etapa de construção, teste e educação dos públicos alvo sobre a nova realidade dos KPIs e métricas de desempenho da sua organização.

Portanto, como se pode perceber a partir do que vimos acima, um dos benefícios ao final dessa jornada será, além do atendimento ao requerimento regulatório, a melhoria nos processos e ferramentas relacionadas à geração e análise de indicadores permitindo a sua utilização para tomada de decisão, planejamento e comunicação com os diversos stakeholders. Essa percepção sobre impactos do normativo deve orientar os executivos na tomada de decisão sobre os seus investimentos nos próximos anos para adequação ao requerimento e também para obter o maior benefício possível dessa jornada.

Comitê de auditoria em seguros: anjo da guarda ou encosto?

ASSIZIO OLIVEIRA
Consultor e membro de Comitês de Auditoria de seguradoras e resseguradoras

LR Assessoria e Consultoria

Introdução

Cada vez mais, segurados, terceiros, beneficiários, fornecedores, parceiros e investidores querem saber mais sobre uma seguradora antes de decidir em quem confiar a proteção dos seus bens, pessoais e materiais. Cada vez mais o regulador considera os níveis de governança e de ambiente de controle das seguradoras e resseguradoras no planejamento de suas fiscalizações.

No entanto, resquícios de tempos idos em que não se falava em governança ainda contribuem para que o mercado de seguros continue a ser uma espécie de charada para seus *stakeholders*, o que leva à necessidade do incremento dos graus de conformidade com relação aos pilares da governança, especialmente os da transparência e da responsabilidade.

Urge, pois, eliminar circunstâncias que podem estar a impedir que as companhias melhorem o seu ambiente de negócios e o externem de forma boa e adequada, de forma a prevenir que terceiros se antecipem, quase sempre com conotações negativas. É premente que a questão da imagem corporativa seja considerada

no contexto da estratégia operacional, mediante a identificação de fraquezas e ameaças que possam prejudicar a reputação empresarial e a adoção de criteriosas formas de, continuamente, manter saudável o ambiente de negócios.

A companhia que, de fato, entende isso como uma missão, têm nos seus Comitês de Auditoria seu mais importante aliado, verdadeiro anjo da guarda. As que assim não agem, tendem a perceber os seus Comitês de Auditoria como um encosto.

Pensadores da Teologia, quanto à ideia do anjo da guarda, atribuem a esse ser a função de preparar a alma dos mortais para a visão do que é divino, cuidando, protegendo e mostrando o caminho mais seguro, porém sem interferir no livre arbítrio do protegido, quem, ao final, decidirá se quer ou não ser cuidado, protegido ou tomar o caminho recomendado. Em uma visão simplista, o encosto age em sentido contrário ao do anjo da guarda.

Por sua vez, os adeptos do movimento Novo Pensamento, sob a égide dos conceitos da Lei da Atração, disseminam que o semelhante atrai semelhante, ou seja, são as próprias pessoas, com atitudes e pensamentos, conscientes ou não, que ditam a sua realidade. Na tradição popular, é o colher o que se plantou.

Acreditemos ou não em anjo da guarda ou encosto, ou na influência de nossos atos e omissões nos resultados que obtemos, é legítimo inferir que, no ambiente corporativo, ter um Comitê de Auditoria proativo, independente e respeitado, ou, ao contrário, um Comitê de Auditoria instituído sem vontade e apenas porque o regulamento oficial obriga, é fruto das atitudes dos acionistas, dos altos administradores e da cultura empresarial e, claro, daquele que aceita fazer parte dele.

Por essa razão, amparado na experiência prática, e tomados os regulamentos vigentes, este artigo objetiva lançar reflexões sobre o Comitê de Auditoria em seguradoras e resseguradoras que atuam no mercado brasileiro.

Linha do tempo

A linha do tempo do órgão interno de governança que se convencionou chamar de Comitê de Auditoria se inicia em 1939, quando a *Bolsa de Valores de Nova York* passou a recomendar, para as empresas listadas, a criação de um comitê especial para apoiar os conselhos de administração na seleção dos seus auditores independentes, recomendação que se tornou obrigação em 1978, reforçada, esta, em 2003, com a adesão da *Nasdaq* e a regulamentação da *SEC*, na esteira do que determinou a *Lei Sarbanes-Oxley* (*SOX*), de 2002.

Desde aquele pontapé inicial, em âmbito global, a instituição do Comitê de Auditoria foi objeto de recomendação e/ou obrigação, entre outros, no *Relatório Cadbury* (Reino Unido, 1992), primeiro código de governança de que se tem notícia, com reflexo nas regras da *Bolsa de Valores de Londres* (1998), no modelo *COSO* (EUA, 1992, 2004 e 2013), na organização multilateral *OCDE* (2004), e nas políticas do *BIS*, o banco central dos bancos centrais (1999). Os modelos de supervisão Basileia (bancos) e Solvência (seguros) também enfatizam a necessidade do Comitê de Auditoria, linha acompanhada pela *IAIS*, que congrega os supervisores de seguros, incluindo o do Brasil.

No cenário interno, desde a primeira versão do guia de boas práticas de governança do *IBGC* (2001), o Comitê de Auditoria vem sendo tratado, sendo que, em 2017, deu-se a edição atualizada do manual "Orientações sobre Comitês de Auditoria". O *CMN / Banco Central do Brasil* e o *CNSP / Susep*, em 2004, editaram as primeiras regras sobre a obrigatoriedade do Comitê de

Auditoria em instituições financeiras e em sociedades do ramo segurador, que vêm sendo atualizadas ao longo do tempo; em 2011, a *CVM* também tratou do tema em instrução normativa. E, em 2016, a *Lei das Estatais* cuidou de obrigar a criação do Comitê de Auditoria para empresas nessa natureza enquadradas.

Em linhas gerais, tomadas em seu conjunto, ditas referências mencionam que o Comitê de Auditoria é órgão de apoio ao conselho de administração, voltado a monitorar e opinar acerca da qualidade dos controles internos e da gestão de riscos, das medidas de prevenção de fraudes, das questões de conflito de interesses, do cumprimento da legislação, dos regulamentos oficiais e das políticas e normas internas (*compliance*), da integridade das demonstrações financeiras, e da qualidade, eficácia e independência das auditorias interna e externa.

Obrigatoriedade

Estão obrigadas a instituir o Comitê de Auditoria, sempre na condição de órgão estatutário subordinado ao conselho de administração, ou, na sua ausência, ao diretor presidente e à assembleia de acionistas, as companhias ou grupos seguradores que, em dois anos seguidos, apresentarem patrimônio líquido superior a R$ 500 milhões ou provisões técnicas acima de R$ 700 milhões.

Podem desfazer o Comitê de Auditoria as companhias que, tendo sido anteriormente enquadradas na obrigação, deixaram de apresentar os valores mínimos de patrimônio líquido e de provisões técnicas, desde que tenham cumprido com todas as exigências pertinentes durante o período em que esteve enquadrada.

Sem embargo, companhias ou grupos que apresentarem montantes de patrimônio líquido e de provisões técnicas inferiores àqueles montantes também podem constituir ou manter o Comitê de Auditoria, opção que raramente é notada no mercado brasileiro.

Cabe às companhias não obrigadas a criar o Comitê de Auditoria fazer uma avaliação sobre a conveniência de tê-lo como um dos seus órgãos internos de governança e, se decidido pela sua instituição, cuidar para que ele seja um anjo da guarda e não um encosto.

Por seu turno, as companhias obrigadas a criá-lo não devem fazê-lo apenas porque o regulador assim o exige, como um encosto, mas sim com a visão estratégica de transformá-lo em seu principal agente de preservação da reputação, como um anjo da guarda. Com efeito, o Comitê de Auditoria, bem organizado e constituído, não só auxilia a incrementar o nível de reputação da empresa, mas também, caso bem escolhidos os seus membros, aportam relevante contribuição ao conselho de administração e à direção em assuntos sob seu âmbito de atuação, funcionando como verdadeira consultoria de alto valor agregado.

Previsão estatutária

Posto que é órgão estatutário, o Comitê de Auditoria e as regras de eleição e destituição de seus membros, bem assim de seu mandato, devem estar expressos no estatuto social da companhia.

Recomendado, em especial, a menos que a governança da companhia estabeleça prazos menores, que o mandato fique estatutariamente estabelecido em três anos, máximo permitido pelo regulamento, o que diminui as formalidades com reeleições mais amiúde e otimiza o custo com registro, publicação e homologação dos correspondentes atos societários.

Número de membros

O Comitê de Auditoria em seguros não pode ter menos de três membros e suas atribuições são indelegáveis; portanto, os membros do Comitê de Auditoria não podem ter suplentes.

Resulta que, quando a companhia opta por eleger o número mínimo obrigatório de membros, não há como contornar imprevistos que impeçam a participação de um dos três membros em reuniões, ou seja, diante do imponderável, não há como obter o quórum mínimo obrigatório, em prejuízo das formalidades e em contraposição ao *compliance* societário.

Essa circunstância é especialmente relevante quando das reuniões de fevereiro e agosto, nas quais se revisam as demonstrações financeiras e se emite o resumo do relatório do Comitê de Auditoria que a elas deve ser juntado, dado que, diferentemente das demais reuniões, que envolvem outros temas das atribuições do Comitê de Auditoria, as reuniões de aprovação das demonstrações financeiras, por comumente ocorrerem nos últimos dez dias daqueles meses, não têm a mesma flexibilidade de mudança de data para que se consiga obter o quórum mínimo obrigatório. Essa situação se agrava em caso de morte, incapacidade, renúncia ou destituição de um membro, vicissitudes que, de forma incontornável, impedem a obtenção do quórum mínimo obrigatório.

Razoável, portanto, que, não sendo flexibilizada a regra vigente, a companhia considere a possibilidade de contar com número de membros superior a três em seu Comitê de Auditoria, de maneira a mitigar a possibilidade de não se obter o quórum mínimo obrigatório.

E, posto que o mandato máximo do membro do Comitê de Auditoria é de cinco anos, um número adequado de membros possibilita um processo de troca paulatino, prudente e consistente, na medida em que membros recém nomeados possam, por alguns meses, conviver com membros mais antigos, para absorver de forma mais eficaz a cultura interna e as atribuições, minimizando, assim, a probabilidade do surgimento de lacunas de desempenho caso a troca de todos os membros seja feita de uma única vez.

Qualificação dos membros

Pelo menos um dos membros do Comitê de Auditoria deve estar qualificado em contabilidade de seguros, auditoria contábil, preparação de demonstrações financeiras e controles internos.

É comum, entretanto, que um *expert* em questões contábeis não domine por completo os temas de controle interno, especialmente de gestão de riscos, das atividades de controle operacional, de *compliance*, da prevenção de fraudes e lavagem de dinheiro, e de auditoria interna. E vice-versa. Nessa mesma esteira, há muito poucos profissionais que dominam, ao mesmo tempo, todos esses assuntos e mais os temas operacionais e atuariais.

De sorte que, ao escolherem os membros de seu Comitê de Auditoria, as companhias devem buscar equilibrar os conhecimentos e experiências de cada um, optando não só por especialistas contábeis e de controle interno, como está obrigada, mas também por conhecedores da operação e da matéria atuarial.

Independência dos membros

O regulador brasileiro exige que todos os membros do Comitê de Auditoria sejam independentes, isto é, sem qualquer vínculo atual ou recente com a administração da companhia, bem assim com seus administradores ou auditores contábeis.

Nesse mesmo contexto, nenhum membro pode receber da companhia remuneração outra que não seja aquela da contrapartida financeira por ser integrante do Comitê de Auditoria.

Como as regras atuais não impedem que integrantes do conselho de administração também possam ser membros do Comitê de Auditoria, a companhia, caso queira lançar mão desse duplo papel, tem de lidar com essa circunstância, fazendo recair a dupla incumbência sobre integrantes do conselho de administração também independentes e remunerando-os apenas e tão somente como membros do Comitê de Auditoria.

O mesmo não se aplica a integrante do conselho fiscal, dado que o regulamento vigente impede o acúmulo de ambas as funções.

Status dos membros

Desde que tomam posse e até o fim do seu mandato, os membros do Comitê de Auditoria estão sujeitos às mesmas responsabilidades legais de qualquer outro componente de qualquer outro órgão estatutário de uma sociedade por ações. E, por consequência, respondem pessoalmente por seus atos e omissões nos termos da legislação e dos regulamentos oficiais que tratam de desvios dos deveres de diligência, lealdade e informação.

Nesse contexto, o tratamento dado aos membros do Comitê de Auditoria deve ser similar àquele que se dá aos demais componentes de outros órgãos internos de governo eleitos estatutariamente, observadas as particularidades da função, especialmente o trabalho *part-time* e a condição de consultor, em razão da qual não toma decisões, mas opina e recomenda medidas para a melhoria das atividades sob o seu âmbito de atuação, com a independência de cobrar a implantação do que recomendou e reportar o que está pendente de ser efetivamente adotado.

Nessa linha, ao membro do Comitê de Auditoria, independentemente da quantidade de reuniões anuais de que participa, deve ser estabelecida remuneração mensal justa, com a inclusão de seu nome no rol de beneficiados por uma eventual apólice de cobertura *D&O*. Na mesma vertente, considerado o seu status como componente de um órgão que está no topo da pirâmide organizacional da companhia, ele deve receber o mesmo tratamento previsto nas políticas internas para qualquer outro dirigente estatutário no que tange à representação, viagens e outros aspectos inerentes.

Regras de funcionamento

A primeira atribuição dos membros do Comitê de Auditoria é formalizar as regras de seu funcionamento, as quais devem ser aprovadas pelo conselho de administração, ou, na sua ausência, pelo diretor presidente; uma vez aprovadas, ditas regras devem ficar à disposição da assembleia de acionistas.

Essa providência redunda na formatação de uma política interna, ou de um regimento ou regulamento, no qual,

observadas pelo menos as normas vigentes, se estabelecem o regime de reuniões, as pautas de cada uma, a elaboração das atas e relatórios, o relacionamento com os diversos níveis da companhia, o suporte logístico e operacional, a realização de avaliações de desempenho periódicas, o tratamento de eventuais conflitos de interesse, etc.

Há casos em que, embora não mandatório, se estabelece regra no sentido de que o Comitê de Auditoria deve ter um coordenador ou presidente, encarregado este de adotar as formalidades necessárias ao seu funcionamento, tais como convocações, condução de reuniões, cumprimento das pautas, voto de minerva, representação, etc.

Desde que não prejudique a independência dos membros, ou seja, que eles fiquem concentrados em opinar e recomendar acerca do que que lhes é exigido por regulamento, as regras de funcionamento, no tocante às atribuições, podem incluir aspectos que vão além do que os regulamentos oficiais determinam, seja porque na governança interna da companhia ou do grupo segurador ficou assim estabelecido, seja porque os acionistas e/ou o conselho de administração requer apoio especializado para temas específicos que tenham afinidade com o âmbito de atuação do Comitê de Auditoria.

Embora não seja exigido, é altamente recomendado que as regras de funcionamento do Comitê de Auditoria sejam revistas e, se necessário, atualizadas, em periodicidade não superior a um ano.

Atribuições gerais

Tomado o foco do âmbito de atuação do Comitê de Auditoria já mencionado, suas atribuições gerais se situam em três momentos, de importância equivalente: monitoramento / avaliação, recomendação e prestação de contas.

Quando exerce o monitoramento / avaliação, o Comitê de Auditoria se vale dos insumos gerados e reportados pelos responsáveis das áreas de gestão estratégica, gestão de riscos, *compliance*, prevenção de fraudes e lavagem de dinheiro, contabilidade, controladoria e ouvidoria, bem como pelos auditores contábeis e atuariais externos e pelos auditores internos. Sempre que a análise dos trabalhos de campo realizados no escopo dessas atividades requerer explicações mais detalhadas, o Comitê de Auditoria tem a prerrogativa de convocar qualquer gestor a dar explicações adicionais e, até, de contratar especialistas externos para apoiar na realização dos exames.

Em adição, o Comitê de Auditoria deve monitorar / avaliar a qualidade dos trabalhos dos auditores externos e internos, desde a elaboração do planejamento de seus trabalhos de campo, até a implementação das medidas de correção e aprimoramento por eles recomendadas, passando pelo alcance e eficácia do resultado de cada um dos trabalhos realizados e da qualidade de seus relatórios, cuidando, em especial, de acompanhar se os recursos humanos, físicos, tecnológicos e de conhecimento são suficientes para levar a bom termo o que deles se exige.

Ainda no terreno da avaliação / monitoramento, o Comitê de Auditoria tem de revisar as demonstrações financeiras antes de sua divulgação, valendo-se do que lhe é fornecido pela administração e pelos auditores contábeis externos, porém com olhar autônomo sobre balanços, demonstrações, variações entre períodos, relatórios da administração, notas explicativas, etc.

O momento da recomendação decorre dos resultados da fase de monitoramento / avaliação e deve resultar em medidas

efetivas do aprimoramento das demonstrações financeiras, dos controles internos, da gestão de riscos, da prevenção de fraudes e da lavagem de dinheiro, e de toda a operação da companhia, no que tange a seus processos, sistemas, rotinas e controles.

Porém, só recomendar não basta: é preciso que o Comitê de Auditoria, além de dar forças para que sejam implementadas as recomendações emitidas pelas áreas de segunda e terceira linhas de defesa, exerça estreito controle de suas próprias recomendações, conheça os planos de ação estabelecidos e acompanhe os prazos de implantação, indicando, sempre que necessário, que os administradores formalizem a assunção de riscos em decorrência da recusa e/ou do atraso da adoção de recomendações relevantes, quais sejam aquelas que envolvem riscos com alto nível de probabilidade e/ou importância relativa.

Nessa linha, se inclui a prerrogativa do Comitê de Auditoria de recomendar a contratação dos auditores contábeis externos ou a sua substituição e, embora o regulamento assim não preveja, essa atribuição deveria ser estendida à auditoria interna e aos titulares das áreas de segunda linha de defesa.

No terceiro conjunto de atribuições do Comitê de Auditoria, o da prestação de contas, é salutar que a possibilidade de reuniões como o conselho de administração prevista no regulamento oficial, por convocação ou iniciativa própria, se transforme em prática comum, ao menos duas vezes por ano, recomendando-se realizá-las tão logo divulgadas as demonstrações financeiras semestrais e o relatório semestral do Comitê de Auditoria, tratado no tópico a seguir. Na ausência do conselho de administração, de se aproveitar a obrigatória reunião semestral com o diretor presidente para o Comitê de Auditoria prestar contas de suas atividades, em paralelo com a abordagem das recomendações relevantes emitidas e ainda não implantadas.

Comunicações obrigatórias

Ademais da elaboração de seus relatórios, o Comitê de Auditoria, em perfeito alinhamento com o responsável pela contabilidade e o auditor contábil externo, está obrigado a reportar ao regulador, no prazo máximo de dez dias contados da comprovação do fato, eventuais desvios da legislação ou dos regulamentos oficiais que possam colocar em risco a continuidade das operações, quaisquer fraudes de autoria de integrantes da administração, fraudes relevantes de autoria de colaboradores internos ou terceiros, e incorreções relevantes nas demonstrações financeiras.

Nesse contexto, a administração da companhia está obrigada a levar ao conhecimento do Comitê de Auditoria, em no máximo vinte e quatro horas contados da identificação, quaisquer eventos que possam ser enquadrados nas condições descritas.

Excetuadas as fraudes praticadas por integrantes da administração, que precisam ser reportadas ao regulador independentemente de sua relevância material, as demais comunicações dependem da definição de um critério de cálculo da relevância, razão pela qual o Comitê de Auditoria precisa definir e documentar tais critérios.

Relatório semestral

O Comitê de Auditoria deve produzir, ao final dos semestres findos em 30 de junho e 31 de dezembro, um relatório de suas

atividades, aqui, para efeitos de melhor compreensão, denominado de "completo". Ele deve ter um conteúdo mínimo, deve ficar à disposição do regulador e dos órgãos de governo interno da companhia por cinco anos, e, a partir dele, se elabora um resumo para ser juntado às demonstrações financeiras.

Vislumbram-se, quanto a essa obrigação, duas circunstâncias, a primeira com relação ao formato do relatório completo e a segunda referente ao seu momento e sua abrangência.

No que toca ao formato do relatório completo, e como, corretamente, o regulamento vigente não estabelece um padrão, a companhia tem a liberdade de formatá-lo como lhe parece mais ajustado com essa exigência, desde que, por óbvio, reste coberto o conteúdo mínimo exigido.

Dessa forma, para formatar o relatório completo, há a opção por organizar um dossiê contendo todas as atas das reuniões do período de abrangência, suportadas pelo material de apoio e pelas evidências do tratamento de todos os temas que formaram a pauta de cada uma, tudo devidamente referenciado, gerando-se, a partir desse dossiê, o resumo do relatório para juntada às demonstrações financeiras.

Outra alternativa é, a partir das atas detalhadas de cada reunião, construir o relatório completo para destacar os principais pontos de cada reunião, e, então, gerar o relatório resumo que deve ser associado às demonstrações financeiras.

Não se descarta, também, a possibilidade de o relatório resumido que deve ser juntado às demonstrações financeiras assumir o caráter de completo, sendo que, nesse caso, ele será bem mais longo e detalhado.

Assim, enquanto perdurar as regras vigentes, a companhia deve eleger a alternativa que lhe parecer mais conveniente, cuidando para evitar redundâncias e retrabalhos, e otimizar custos adicionais com a divulgação e as publicações obrigatórias das demonstrações financeiras.

Quanto ao momento da emissão do relatório completo, e à sua abrangência, e, por consequência, do relatório resumido que se junta às demonstrações financeiras, constata-se certa dificuldade em interpretar o que manda o regulamento vigente, posto que ele crava duas datas bases específicas: 30 de junho e 31 de dezembro.

Ocorre que o vocábulo "semestre" encerra a ideia de um período de seis meses consecutivos, valendo dizer que o conceito de "semestre" não se restringe ao seis primeiros ou aos seis últimos meses de um ano civil, ao final dos quais as companhias devem levantar suas demonstrações financeiras transitórias (data base 30 de junho) e anuais (data base de 31 de dezembro), e ao final dos quais é exigida a emissão do relatório completo do Comitê de Auditoria.

Para agravar, as demonstrações financeiras transitórias e anuais têm prazo para serem fechadas e divulgadas, respectivamente, nos últimos dias úteis de agosto (data base de 30 de junho) e de fevereiro (data base de 31 de dezembro), motivo pelo qual o Comitê de Auditoria só tem condições de opinar sobre elas nos últimos dez dias daqueles meses, ou seja, passados já sessenta dias do encerramento do primeiro e do segundo semestres do ano a que se referem e da data base do relatório completo.

Diante disso, surgem as seguintes dúvidas: o Comitê de Auditoria deve gerar seus dois relatórios completos anuais tão logo encerrados o primeiro e o segundo semestres de cada ano, ou seja, em julho e janeiro, respectivamente? Sendo isso o correto, como neles incluir a aprovação das demonstrações financeiras que só ocorrerá no final dos meses seguintes, isto é, em agosto e fevereiro, de modo que

o relatório resumido delas faça parte? É correto gerar o relatório completo em fevereiro e agosto, considerando as abrangências semestrais de março a agosto e de setembro a fevereiro, que encerram um semestre, de modo que a aprovação das demonstrações financeiras seja nele incluída e se possa gerar o relatório resumido para nelas associá-lo? O relatório completo deve se restringir às atividades de janeiro a junho e de julho a dezembro, com exceção das avaliações das demonstrações financeiras, que acontecerão somente em fevereiro e agosto do semestre seguinte?

Assim, até que os regulamentos vigentes sejam melhorados para bem expressar o que o regulador está a requerer, as companhias precisam se cercar de cuidados e argumentos consistentes sobre a sua opção a respeito do momento da edição e da abrangência dos relatórios completo e resumido do seu Comitê de Auditoria.

Conclusão

Refletindo a respeito das questões aqui abordadas, e adotando as melhores práticas para o funcionamento do Comitê de Auditoria, a companhia fará a opção por contar com um anjo da guarda. Ao contrário...

CROSSOVER CONSULTING & AUDITING CORPORATION

"Movendo as Corporações através do Conhecimento"

GESTÃO DE RISCOS

AUDITORIA INTERNA

CONTROLE INTERNO

GOVERNANÇA

GESTÃO DE NEGÓCIOS

BUSINESS SCHOOL

CROSSOVER
CONSULTING & AUDITING

Somos uma empresa com 10 anos de sólida experiência em Gestão Empresarial, Auditoria Interna, Controles Internos, Riscos e Governança Corporativa. Acreditamos que o sucesso de uma organização está amparado na efetiva gestão de pessoas, processos e produtos, por isso nosso foco é o aperfeiçoamento da governança através do fortalecimento do gerenciamento de riscos, dos processos operacionais e do sistema de controles internos.

Nossos valores são baseados no respeito às melhores práticas de negócio e governança, em valores éticos, respeito à segurança, qualidade e sustentabilidade do ambiente corporativo. Estes são os fundamentos de nossa filosofia de trabalho e comportamento.

Nossa equipe de profissionais é formada por profissionais seniores – consultores e auditores – com experiência na condução e avaliação de negócios no Brasil e exterior.

Nossa missão é oferecer serviços diferenciados, inovadores, confiáveis e de alta qualidade, criando fundamentos adequados para expansão e crescimento sustentável de nossos clientes com base nas melhores práticas de governança.

Internal Control Institute Brasil

Desde 2012, somos uma afiliada do "the Internal Control Institute" responsável pela gestão de suas atividades no Brasil. Oferecemos programas de capacitação e certificação internacional para especialistas em controles internos - CICS Certified Internal Control Specialist.

NO MATTER HOW COMPLEX YOUR BUSINESS NEEDS ARE, WE HAVE THE EXPERIENCE AND CAPABILITIES TO PROVIDE THE BEST SOLUTIONS YOU NEED TO MOVE FORWARD

WWW.CROSSOVERBRAZIL.COM

NORTH AMERICA
CORPORATE OFFICE
FORT LAUDERDALE, FLORIDA
754 2271351
EMAIL: CORPORATEUSA@CROSSOVERBRAZIL.COM

SOUTH AMERICA
SÃO PAULO OFFICE
PHONE 55+11+2599 8360
EMAIL: CONTATO@CROSSOVERBRAZIL.COM
CURITIBA OFFICE
PHONE 55+41+2101 1622
EMAIL: VIVIANE@CROSSOVERBRAZIL.COM
PORTO ALEGRE OFFICE
PHONE 55+51+ 3533 8566
EMAIL: MARLON@CROSSOVERBRAZIL.COM

Análise de Impacto Regulatório (AIR) e Sandbox regulatório no mercado segurador

SIMONE NEGRÃO
Diretora Jurídico e Compliance da Mapfre

MAPFRE

Muito se fala em inovação e, volta e meia, nos deparamos com notícias de *insurtechs* e as profundas 'sacudidas' no mercado segurador. Além de nos despertar para o que deve vir nos próximos anos.

Em atividades reguladas como a securitária, as regras e requisitos regulatórios são vistos, muitas vezes, como obstáculos à inovação e novos entrantes. Mas quanto custa para cada um ficar em conformidade com as regras aplicáveis?

Recentemente o jornal Valor Econômico destacou a seguinte manchete: "Governo prepara 'Janela regulatória' para melhorar o ambiente de negócios". A notícia informa que o executivo prepara um decreto para estabelecer que os órgãos federais só possam editar normas uma ou duas vezes ao mês, para dar mais previsibilidade ao ambiente de negócios do Brasil, reduzindo um dos custos empresariais que é o do acompanhamento das constantes mudanças de normativos.

Neste ponto o Brasil é pródigo. Levantamento feito pelo Instituto Brasileiro de Planejamento e Tributação (IBPT) nos dá conta que desde a promulgação da Constituição Federal, em 4 de outubro de 1988, até 9 se setembro de 2016, União, Estados e municípios editaram mais de 5,4 milhões de normas e leis. Isto representa, em média, 535 normas editadas todos os dias, ou 769 normas editadas por dia útil!

Bom, só de emendas constitucionais estamos chegando à casa das centenas, mas a área de regulação em geral não pode e não deve ficar imune à inovação. O mercado financeiro de forma geral já tem discutido sobre o AIR e as *sandboxes* regulatórias. Será que estamos entrando numa nova era?

AIR (análise de impacto regulatório)

Já temos iniciativa de Projeto de Lei sobre AIR (nº 1.539/2015), que pretende tornar obrigatória a adoção da AIR pelas Agências Reguladoras Federais. Foi publicada também as "Diretrizes Gerais e Guia Orientativo para Elaboração de Avaliação de Impacto Regulatório – AIR" em junho de 2018 como resultado das discussões técnicas coordenadas pela Casa Civil da Presidência da República, em parceria com o Ministério da Fazenda, o Ministério do Planejamento, Desenvolvimento e Gestão e as Agências Reguladoras Federais.

Nos termos do relatório que acompanha o Projeto de Lei "A Análise de Impacto Regulatório (AIR) consiste em uma ferramenta utilizada para examinar e medir os benefícios, os custos e os efeitos prováveis no contexto da atuação regulatória. Compreende um conjunto de procedimentos que antecede e subsidia o processo de tomada de decisão, disponibilizando dados empíricos, a partir dos quais os tomadores de decisão podem avaliar tanto as opções existentes quanto as possíveis consequências".

Ora, é de todo recomendável que os atores que deverão implementar uma nova norma tenham antes da sua edição, a análise dos impactos, custos, alternativas e principalmente tenham a oportunidade de dialogar por meio dos instrumentos adequados com o órgão que está regulamentando o assunto. Diferentes visões se são difíceis de se compatibilizar por um lado, por outro enriquecem o debate e sem dúvida contribuem para o aperfeiçoamento da regulação.

Não menos importante é que o AIR deve sempre observar o princípio da proporcionalidade, o que significa dizer que os recursos, esforços e tempo empregados em toda análise devem ser proporcionais à relevância do problema investigado e dos possíveis impactos da intervenção governamental.

Sandbox regulatório

Conforme artigo "*Sandbox*, o futuro da regulação" escrito pelo especialista Bruno Feigelson[1] , "*Sandbox* é um ambiente que vai permitir que *startups* de *fintech*, ou até mesmo instituições financeiras, possam oferecer seus produtos e serviços ao público, por um período limitado, sem as restrições impostas pela regulamentação vigente. A ideia é estimular a experimentação, para que o regulador possa acompanhar de perto as inovações e avaliar o impacto que elas terão na experiência do usuário, o quanto isto facilita a vida das pessoas e, em contrapartida, os riscos reais decorrentes de sua implementação".

1 https://www.ab2l.org.br/sandbox-o-futuro-da-regulacao/

Como será que o nosso mercado está se preparando para isso? A meu ver, caminhando muito bem!

A SUSEP como uma das convidadas do evento *Insurtech* 2018, trouxe a notícia que em dezembro de 2017, foi lançado o 4º Grupo de Trabalho do Laboratório de Inovação Financeira (LAB) com representantes da Comissão de Valores Mobiliários (CVM), da Superintendência Nacional de Previdência Complementar (Previc) e a SUSEP.O LAB, patrocinado pelo Banco Interamericano de Desenvolvimento (BID), já estuda uma *sandbox* regulatória para as *insurtechs* testarem soluções inovadoras sob a supervisão dos órgãos reguladores.

De fato o assunto já esteve na pauta das reuniões da Comissão Especial de Inovação e *Insurtech* da SUSEP.

E para que ninguém tenha dúvida de que as inovações regulatórias já estão entre nós, a CVM publicou portaria em 19/03/2019 (portaria CVM/PTE 48/2019) que disciplina o processo de normatização da própria CVM incorporando tanto a AIR quanto à possibilidade dos *sandboxes* regulatórios.

A AIR passa a ser uma das fases do processo de normatização que é composto pelas seguintes fases: (i) abertura e catalogação; (ii) análise de impacto regulatório – AIR; (iii) pré-audiência pública; (iv) audiência pública; (v) pós audiência pública. Importante salientar que há algumas hipóteses previstas na Circular de dispensa de AIR.

Já as *Sandboxes* são previstas da Circular como a possibilidade de criação de um ambiente regulatório experimental na fase de pré-audiência pública em que poderão ser editados instrumentos normativos de caráter temporário a partir dos quais se buscará avaliar empiricamente os benefícios e os procedimentos mais adequados para a implementação da solução preconizada.

Ao que tudo indica estamos no caminho da reconciliação entre *compliance* e inovação e seguindo para uma maior racionalidade no processo de regulamentação. De fato, a inovação se desenvolve com a rapidez habitual dos negócios deixando a reboque a regulamentação que não está tão habituada a esta velocidade.

Distribuição de seguros

THOMAZ KASTRUP, KAREN SCHIAVON E ANDRÉ H. JAHARA
Thomaz Kastrup é sócio, Karen Schiavon e André H. Jahara são associados do Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

MATTOS FILHO >
Mattos Filho, Veiga Filho,
Marrey Jr e Quiroga Advogados

Introdução

A legislação acerca da comercialização de seguros no Brasil comporta contratação direta ou indireta (com intermediação). Apesar disso, devido às práticas do mercado local, a maioria dos seguros são colocados junto ao público indiretamente. São de tal forma arraigadas essas práticas no mercado que – não raro – algumas seguradoras não contam com canais diretos para a comercialização de seus produtos, de modo que grande parte das contratações acabam sendo feitas mediante intermediação.

Em linhas gerais, as formas de intermediação de seguros praticadas no Brasil são a corretagem e a distribuição de seguros, cada uma com lógica, características e normas próprias. Os contratos de distribuição de seguros têm por objetivo regular a relação entre uma seguradora e as entidades capazes de oferecer, promover, distribuir e comercializar produtos securitários por meio de seus canais de distribuição.

Os contratos de distribuição agregam valor às seguradoras porque lhes asseguram espaço no balcão dos distribuidores, ampliando (em muito) sua base de segurados: esse é um dos motivos (se não o principal)

pelos quais tais arranjos, em regra, não são tão utilizados pelas seguradoras ligadas a grupos financeiros, cuja natural capilaridade com agências bancárias espalhadas em diversas localidades lhes franqueia condições de crescimento similares, sem necessidade de firmar parcerias fora do seu grupo.

Ao amparo da regulamentação em vigor, a distribuição de seguros pode ser feita sob a forma de (i) estipulação, ou (ii) representação de seguros. Apesar de algumas semelhanças, tais institutos possuem profundas diferenças entre si, pautadas principalmente pelas diferentes relações entre seguradora, distribuidor (estipulante ou representante) e proponente.

Enquanto nas operações de representação de seguros – nas quais o representante não possui vínculo pré-existente com o proponente – o primeiro é considerado representante da seguradora; na estipulação, por sua vez, o distribuidor atua como representante do grupo segurado, uma vez que tem relação prévia com os membros do referido grupo segurado de apólices coletivas (por exemplo, empregador e empregado). Enfim, tamanha é a diferença entre tais institutos que não convém abordar ambos nesta publicação, motivo pelo qual – a partir daqui – nos debruçaremos somente sobre a representação de seguros.

Criada por meio da Resolução CNSP nº 297/13, a representação de seguros tem suscitado grande interesse no mercado segurador, mostrando-se meio hábil a garantir o seu crescimento e lucratividade. Desde a sua criação, inúmeras foram as parcerias celebradas entre seguradoras e grupos diversos, envolvendo valores expressivos que revelam o grande interesse por arranjos dessa natureza. Somente no último ano:

- A Zurich Minas Brasil Seguros S.A. fechou contrato de representação de seguros com a rede varejista Havan Lojas de Departamentos Ltda., pagando R$ 200 milhões pelo direito de distribuir seus produtos securitários com exclusividade nos canais de venda físicos e online das lojas 'Havan' e com metas de distribuição de seguros no valor de R$ 2,8 bilhões, a serem cumpridas pela Havan Lojas de Departamentos Ltda. nos próximos 5 (cinco) anos[1];
- A Zurich Minas Brasil Seguros S.A. estendeu sua parceria com a Via Varejo S.A., controladora das lojas "Casas Bahia" e "Ponto Frio", por mais 5 (cinco), pagando R$ 825 milhões pelo direito de distribuir seus produtos securitários com exclusividade nos canais de venda físicos e online das lojas "Casas Bahia" e "Ponto Frio" e com metas de distribuição de seguros acordada[2]; e
- A seguradora francesa CNP Assurances renovou sua parceria para distribuição de seguros com a Caixa Seguridade (braço de seguros da Caixa Econômica Federal) até 2041, comprometendo-se a pagar um valor que passa dos R$ 4 bilhões pelo direito de distribuição[3].

Representação de Seguros

A representação de seguros consiste na distribuição de seguros pelo representante à conta e ordem da seguradora parceira, em caráter não eventual, mas sem vínculo de dependência, com território delimitado. Ela pode ser exclusiva ou não, podendo ou não

1 https://latinlawyer.com/article/1189026/zurich-and-havan-sign-insurance-deal-in-brazil, verificado em 15 de abril de 2019, às 21:30.
2 https://latinlawyer.com/article/1177464/mattos-filho-and-themudo-lessa-renegotiate-zurich-distribution-contracts, verificado em 15 de abril de 2019, às 21:30.
3 https://latinlawyer.com/article/1173715/french-insurer-cnp-enters-billion-dollar-jv-with-caixa, verificado em 15 de abril de 2019, às 21:30.

contar com a participação de corretora de seguros. Por este serviço, os representantes de seguros fazem jus a uma comissão, via de regra calculada com base no valor dos prêmios angariados junto aos segurados em favor da seguradora.

Na qualidade de representante da seguradora, cabe ao distribuidor a recepção de propostas de seguro, podendo emitir os bilhetes, certificados ou apólices individuais diretamente aos segurados e orientá-los no que diz respeito aos termos e condições dos produtos de seguros por ele comercializados, recolher os prêmios, receber os avisos de sinistros e realizar o pagamento das indenizações aos segurados.

Por expressa disposição legal, as seguradoras respondem solidariamente com o representante de seguros por quaisquer atos praticados por este último em desacordo com a regulamentação em vigor perante a Superintendência de Seguros Privados – SUSEP ("SUSEP").

A representação de seguros pode ser utilizada para os seguintes ramos de seguro:

i. Riscos Diversos;

ii. Garantia Estendida/Extensão de Garantia – Bens em Geral;

iii. Garantia Estendida/Extensão de Garantia Auto;

iv. Funeral;

v. Viagem;

vi. Prestamista;

vii. Desemprego/Perda de Renda;

viii. Eventos Aleatórios;

ix. Animais;

x. Microsseguro de Pessoas;

xi. Microsseguro de Danos;

xii. Microsseguro/Previdência; e

xiii. Assistência e outras coberturas – Auto.

Essa limitação foi intencional, pois atinge o mercado de *affinity*/massificado, onde tais coberturas têm grande demanda.

Frequentemente as operações de representação de seguros têm aspectos financeiros para os distribuidores de seguros: no início da relação, as seguradoras lhes proporcionam liquidez financeira na forma do chamado "*upfront*", a ser quitado paulatinamente pelo representante ao longo da relação por meio do cumprimento das metas de distribuição de seguros contratualmente acordadas.

O interesse por tais arranjos decorre do fato de que a tão necessária capilaridade fornecida pelos distribuidores e almejada pelas seguradoras somente pode ser atingida por meio de vultuosos investimentos: basta pensar nas sociedades varejistas, com milhares de lojas espalhadas pelo Brasil afora. Isso requer investimentos e capital de giro. Essa, sem dúvida, foi a destinação dada pela Via Varejo S.A. e pela Havan Lojas de Departamentos Ltda. a, pelo menos, parte do *upfront* pago pela Zurich Minas Brasil Seguros S.A. no bojo dos contratos acima mencionados.

Aliás, tamanha é a representatividade dos varejistas entre os representantes de seguros que a Circular SUSEP nº 480/13 foi emitida especificamente para regular essas operações. Em resposta aos inúmeros problemas associados ao inerente conflito de interesses existente entre o representante de seguros (no caso, os varejistas) e seus clientes, tal normativo trouxe vedação expressa à distribuição de seguros por varejistas por meio da modalidade de estipulação. Assim, salvo exceções previstas na regulamentação aplicável, a distribuição de seguros pelo setor varejista é permitida somente na modalidade de "representação de seguros".

Em vista da expansão do consumo por meio virtual (comércio eletrônico), é importante mencionar que o paradigma da ampliação da capilaridade das organizações varejistas por meio da ampliação da sua infraestrutura física não se manterá

ad aeternum. Em um cenário de domínio dos *marketplaces* como principal canal de comercialização de produtos, as seguradoras e, consequentemente, os contratos de representação de seguros provavelmente gravitarão em torno dos distribuidores cujas plataformas virtuais tenham mais acessos pelo público, a despeito do número dos seus estabelecimentos e lojas físicas.

Com relação ao cumprimento das metas de venda de seguro, caso venham a ser descumpridas, deve o representante de seguros devolver à seguradora a parcela não amortizada do *upfront* corrigido pelo índice convencionado entre as partes ou estender a vigência do contrato de representação até que a meta originalmente acordada seja atingida. Para salvaguardar essa devolução, as seguradoras exigem robustas garantias dos representantes, sendo a mais comum a carta de fiança bancária por conta de sua blindagem jurídica até mesmo em cenários de liquidação/recuperação judicial ou extrajudicial do distribuidor.

Conclusão

A proliferação de operações de representação de seguros revela o acentuado grau de interesse pelo instituto na atualidade. Além de garantir o crescimento continuado das seguradoras em meio à crescente concentração do mercado e à crescente evolução tecnológica, arranjos desse tipo aproximam o seguro da população e, consequentemente, contribuem para a difusão em meio ao público da cultura de contratação de seguro, ainda bastante incipiente no Brasil quando comparado com outros países.

Essas condições têm feito nascer nos representantes, seguradoras e escritórios de advocacia uma gama de profissionais especializados nesses tipos de operações, contribuindo sobremaneira para o desenvolvimento desse negócio, cuja versatilidade comporta estruturas contratuais sofisticadas e aptas a lidar, simultaneamente, com as necessidades dos distribuidores e das seguradoras, garantido segurança jurídica a todos os envolvidos.

Diante da ampliação da comercialização de seguros no Brasil por meio de representação de seguros, estamos certos de que esse *know-how* permitirá ao setor securitário superar os desafios impostos pelas novas tecnologias que se apresentam ao mercado, permitindo-lhe extrair o máximo proveito das oportunidades que, na verdade, representam.

Princípios e Regras de Direito Aplicáveis ao Contrato de Resseguro Internacional – *PRICL*

SERGIO RUY BARROSO DE MELLO
Vice Presidente da AIDA Internacional

Pellon & Associados
ADVOCACIA

1. Introdução

É uma grande alegria elaborar estas notas sobre tema da mais alta relevância ao Setor de Seguro e Resseguro para a prestigiada Revista Eletrônica *Opinião.Seg*, dirigida pela festejada *Editora Roncarati*, a quem o Mercado de Seguros no Brasil tanto deve por sua dedicação intelectual ininterrupta a essa atividade empresarial ao longo de tantos anos.

Coube a mim tratar dos Princípios e Regras de Direito aplicáveis ao contrato de resseguro (conhecido como *PRICL*), que passará a ser fonte de direito para solução dos litígios que envolvam os contratos de resseguro, em nível global, especialmente mediante procedimentos arbitrais, já que a maioria absoluta desse tipo contratual apresenta cláusula compromissória de arbitragem.

O projeto surgiu por meio de apoio fornecido pela Universidade de Zurique, do

Swiss National Funds, da *Austrian Science Funds* e do *German Research Foundation*, que criaram grupo de especialistas em nível internacional, para elaboração de tais princípios. O Projeto foi denominado ***PRICL***, por ser a abreviatura de *Principles of Reinsurance Contract Law,* razão pela qual permitimo-nos utilizar essa expressão ao longo dessas linhas.

2. Significado do *PRICL*

O ***PRICL*** é um conjunto de regras e princípios de direito privado aplicáveis ao contrato de resseguro, não vinculativas. Pode ser qualificado como *soft law* (lei branda).

O objetivo é prover o Setor de Seguro e Resseguro mundial de elementos técnicos e jurídicos capazes de garantir segurança aos contratantes de um resseguro.

O uso do ***PRICL*** poderá ser feito por meio de cláusulas compromissórias de arbitragem inseridas nos contratos de resseguro, nas quais se estabeleça a sua utilização como norma de solução das disputas submetidas à arbitragem.

O ***PRICL*** não pretende reinventar a lei de resseguros. Pode ser considerdo como espécie de codificação privada ou "atualização" do direito de resseguro global existente, porque incorpa boa parte dos usos e costumes internacionais consagrados em termos de resseguro. O ***PRICL*** tem por objetivo reafirmar as normas atuais de resseguro, sem alterá-las.

3. O que o *PRICL* não é

O ***PRICL*** não será redigido para servir de lei modelo e não necessita de qualquer legislação para a sua utilização. Basta que as partes optem pelo ***PRICL*** como a lei que rege o contrato de resseguro, inserindo tal premissa em cláusula compromissória de arbitragem.

Justo porque os mercados de resseguro são absolutamente globais, o direito aplicável aos contratos de resseguro não pode ser tratado apenas em nível regional. Neste sentido, regras como as do ***PRICL*** preveem sempre um conjunto de normas uniformes em nível global, sem impedir o desenvolvimento do direito dos contratos de resseguro.

O ***PRICL*** não será jamais imposto às partes no contrato. Elas o aplicarão apenas quando escolhê-lo como a "lei" que rege o seu contrato. Mesmo que as partes optem pelo regime do ***PRICL***, estarão livres para excluir certos princípios do âmbito de aplicação, bem como alterá-los ou mesmo variar os seus efeitos.

Devido à sua natureza inteiramente não vinculativa, o ***PRICL*** não interfere com os produtos oferecidos nem com as cláusulas tradicionais usadas nos mercados internacionais de resseguros. Ao contrário, o ***PRICL*** deverá facilitar a oferta internacional de produtos de resseguro, bem como a utilização de cláusulas modelo, porque fornecerá um conjunto harmonizado de regras gerais de produtos e cláusulas modelo. Na medida em que as regras do ***PRICL*** tenham por base a experiência técnica e jurídica consagradas no resseguro internacional, haverá consequente previsibilidade de resultados, independente da jurisdição a que o contrato de seguro está intimamente relacionado.

4. Por que escolher o *PRICL*?

A escolha adequada da lei e dos princípios que regem o contrato de resseguro é a

melhor maneira de criar segurança jurídica às partes na solução dos conflitos. Isto porque se trata de tipo contratual cujas cláusulas podem ter interpretações das mais diversas, dependendo do local e do direito aplicável (Exemplo: *civil law* – países latinos ou *comun law* – países anglos saxônicos).

Em virtude do caráter internacional das operações de resseguro, várias jurisdições podem se envolvidas na solução do litígio e, consequentemente, a análise aprofundada de cada lei aplicável não seria juridicamente viável.

Por outro lado, esse impacto não pode ser totalmente evitado através da incorporação de cláusulas modelo, por várias razões. Mas a principal é a falta de abrangência das regras modelo, o que lhe retira a garantia jurídica suficiente à interpretação justa, correta e uniforme por diferentes Tribunais de arbitragem ou ordinários.

Mesmo que as partes se comprometam vincular e se submeter à determinada lei, encontrarão dificuldades em estabelecer o seu conteúdo para aplicação à atividade de resseguro. Isto porque é comum se deparar com a ausência de fontes de direito no campo do próprio resseguro.

Já a jurisprudência dos Tribunais, tanto no Brasil quanto no exterior, não serve de guia seguro, porque não abordou as grandes questões jurídicas surgidas nas controvérsias de resseguro ou o fez apenas em certos aspectos, sem se aprofundar no estudo e decisão sobre principais institutos oriundos das cláusulas, sempre criativas. A jurisprudência existente é considerada como "enviesada", porque se relaciona preferencialmente com o resseguro facultativo, ignorando os tratados de resseguro, além de, predominantemente, abranger os casos que envolvam perdas da cauda longa.

Ademais, em países cujo direito segue prioritariamente os pricípios da lei civil, como o Brasil (*civil law*), é comum a ausência de lei específica para contratos de resseguro ou normas gerais com dispositivos sobre esse instituto jurídico.

Assim, é importante ter à disposição regras e princípios de direito aplicáveis aos contratos de resseguro, como o ***PRICL***, proporcionando quadro uniforme dentro do qual as cláusulas modelo podem ser acordadas com absoluta segurança jurídica pelas partes, afinal, será possível conhecer o seu sentido muito antes da celebração e formalização do resseguro.

O ***PRICL*** surge como eficiente opção às partes do negócio de resseguro, porque se reveste de conjunto uniforme de regras e princípios técnicos e de direito, inclusive normas gerais relativas ao direito das obrigações e dos contratos em geral. O ***PRICL*** se apresenta como norma abrangente, relativamente suave e uniforme em termos de resseguro, acompanhada por comentários que explicam os princípios e ilustram a sua aplicação a casos típicos.

Assim, se torna muito mais previsível o resultado dos debates jurídicos sobre o significado dos termos do contrato de resseguro, na medida em que as partes elegeram o ***PRICL*** como a lei aplicável aos contratos de resseguro.

5. Limites inerentes à eficácia do *PRICL*

O ***PRICL*** será eficaz na medida em que as partes venham a aproveitar e usar a sua autonomia para inseri-lo no contrato de resseguro. Pelo menos para os contratos que contenham cláusula compromissória de arbitragem essa autonomia é irrestrita, a teor da Lei de Arbitragem (nº 9.307/96) que permite às partes escolher "regras de direito", como a lei que regerá o contrato.

Considerando que o termo "regras de direito" abrange também o direito fora das leis

tradicionais, o ***PRICL*** se apresentará como conjunto qualificado de regras e princípios que podem ser escolhidos pelas partes.

No entanto, mesmo no âmbito da arbitragem que confere às partes máxima liberdade, há limites para a escolha da lei. Em outras palavras, a aplicação do direito especial não pode violar a ordem pública, razão pela qual a eficácia do ***PRICL*** no fornecimento de quadro uniforme de princípios e regras de resseguro é limitada ao respeito à lei local.

A legislação nacional sempre terá importânica na resolução dos litígios de resseguro, embora quase sempre seja limitada ao contrato de seguro. Porém a sua aplicação se dará de forma muito restritiva ao contrato de resseguro, especialmente naqueles regidos pelo ***PRICL*** como um conjunto uniforme de regras de direito. Para evitar esse problema, será sempre recomendável que as partes indiquem claramente na sua cláusula de eleição de lei o uso obrigatório e único dos princípios e regras oriundas do ***PRICL*** como a lei aplicável e prevalente.

O âmbito de aplicação do ***PRICL*** não se limita aos contratos «internacionais» de resseguro. Embora os contratos de resseguro sejam frequentemente contratos internacionais, no Brasil isso não é regra, afinal, contratos entre seguradoras brasileiras e ressegurador local são eminentemente nacionais.

A escolha do ***PRICL*** usufrui de elevado grau de liberdade contratual das partes, motivo pelo qual pode e deve ser inserido aos termos do contrato como norma prevalente. Além disso, às vezes um contrato nacional de resseguro fará parte integrante de um sistema de resseguro internacional. Nessas situações a utilização do ***PRICL*** se reveste de maior importânica.

O ***PRICL*** só será aplicável quando as partes no contrato, ou seja, o ressegurador e o segurador, assim acordarem, jamais por imposição.

6. Casos em que as partes não escolheram o *PRICL*

Mesmo nas hipóteses nas quais as partes não tenham escolhido a aplicação e utilização das regras e princípios do ***PRICL***, os árbitros ou juízes, conforme o caso, podem optar pelo seu uso, como útil referência em situações que considerem adequadas.

Mas o ***PRICL*** não serve como lei modelo para legislaturas nacionais, internacionais ou supranacionais, são apenas regras e princípios do direito de resseguro para utilização como fonte de interpretação dos contratos de resseguro.

7. Exclusão ou modificação do *PRICL*

A liberdade das partes norteia a elaboração desse projeto, de forma que as partes podem excluir a aplicação do ***PRICL*** ou mesmo modificar o efeito de qualquer das suas disposições, para adaptar à situação local, seja por conta dos usos e costumes distintos ou mesmo de lei específica.

Em outras palavras, o ***PRICL*** é altamente maleável como fonte de direito de resseguro.

8. O *PRICL* fornece conjunto de regras inteiramente não obrigatórias

Se as partes optarem pelo ***PRICL***, não precisam aceitá-lo em sua integralidade, podem alterá-lo na parte em que lhes interessar, no próprio contrato de resseguro. Isto se deve à natureza inteiramente não obrigatória do ***PRICL.***

Ademais, o próprio ***PRICL*** permite essa liberdade de alteração pelas partes, ao prever tal direito em seu preâmbulo.

O estilo objetivo do ***PRICL*** quanto a seu funcionamento e existênica se justifica, porque não há razões políticas para restringir a liberdade contratual das partes em operações de resseguro, razão pela qual também não há espaço para regras obrigatórias em favor de uma delas.

Ao mesmo tempo, não existem preocupações de interesse público que necessitem de proteção por regras de resseguro obrigatórias, como se vê, por exemplo, nos contratos de seguro onde o segurado se encontra protegido por normas específicas, como o Código de Defesa do Consumidor.

9. Exclusão ou modificação do *PRICL*

Qualquer exclusão ou modificação do ***PRICL*** pode ser expressa ou implícita.

É possível as partes acordarem expressamente sobre as cláusulas contratuais incompatíveis com as disposições do ***PRICL*** e excluir ponto específico de seus princípios e regras que entenderam necessário, justo pelo princípio constitucional da autonomia da vontade contratual.

As partes podem excluir certas partes do ***PRICL*** simplesmente escolhendo ou incorporando no contrato partes específicas, distintas da original.

10. Usos e costumes

Seguindo o princípio da liberdade contratual, as partes podem acordar na aplicação de qualquer utilização particular. Neste sentido, os usos ou costumes podem ser aplicados ao contrato independentemente de saber se está em conformidade com o ***PRICL***, porque este garante e reconhece como soberana a vontade contratual das partes.

Sempre que as partes não concordarem com a aplicação de determinado uso ou costume, o ***PRICL*** reconhecerá tal intenção e vedará a sua utilização.

Isto porque o ***PRICL*** não prioriza os usos e costumes em geral, destina-se a funcionar como reafirmação do uso do resseguro internacional e fornecer condições de reconhecimento dos usos e costumes utilizados em qualquer país onde tenha sido celebrado o contrato de resseguro, desde que as partes assim o queiram.

Ao utilizarem-se os critérios do ***PRICL***, assegura-se a sua aplicação uniforme e, consequentemente, a ausência de necessidade e motivação para o desenvolvimento de leis de resseguro.

11. Relevância da disposição do *PRICL*

Em geral, o resseguro encontra poucas regras de uso obrigatório aos contratos, mas podem existir, como é o caso daquelas incorporadas na Resolução nº 168, de 2007, do Conselho Nacional de Seguros Privados – CNSP.

Portanto, a escolha em favor do ***PRICL*** não pode impedir a aplicação do direito de supervisão e de outras disposições de direito público. Essas regras podem ter forte impacto sobre o contrato de resseguro e se aplicam prioritariamente ao ***PRICL***.

12. Interpretação e Suplementação do *PRICL*

O ***PRICL*** deve ser interpretado à luz do seu texto, contexto, finalidade e caráter

internacional. Em particular, tem como objetivo a promoção da boa fé contratual no sector de resseguro, a segurança jurídica nas relações contratuais e a uniformidade de aplicação de seus princípios e regras.

As questões abrangidas pelo âmbito de aplicação do ***PRICL***, porém não expressamente resolvidas por ele são, tanto quanto possível, resolvidas em conformidade com os princípios do direito local aplicável ou a intenção das partes contratantes.

13. Ausência de regra ou princípio específico no *PRICL*

Podem ocorrer situações nas quais certas questões se apresentam previstas no âmbito de aplicação do ***PRICL***, mas não são expressamente resolvidas por ele. Tais questões devem ser resolvidas por aplicação analógica das normas explícitas constantes no ***PRICL***. Se não for possível, a solução deverá ser encontrada com base nos princípios de formulação geral do ***PRICL***.

14. Conclusão

Cumprindo a sua meta inicial, o Grupo responsável pela elaboração do ***PRICL*** terminou a primeira fase do projeto no final de 2018, cujo texto será objeto de grande divulgação em nível internacional, bem como utilizado por seguradoras e resseguradoras importantes que participaram ativamente de sua construção ao longo desse período.

Neste momento o Grupo inicia a elaboração da segunda parte do **PRICL**, ao abordar elementos técnicos mais específicos dos usos e costumes do negócio de resseguro, ao mesmo tempo em que as instituições representativas do seor, em nível internacional, iniciam sua ampla divulgação, para que todos os participantes desse tipo de negócio jurídico possam conhecer e melhor decidir sobre a sua aplicação como fonte secundária de interpretação.

Desejamos boa sorte a todos, na certeza de que o trabalho está no caminho correto, ao mesmo tempo em que destacamos que a participação do Brasil nesse projeto, significa a possibilidade de conhecer previamente os desafios e colaborar de maneira efetiva na busca das soluções para a necessária harmonia contratual e a tão desejada segurança jurídica, fundamental em termos de investimento e operação de resseguro.

Por isso, sinto-me honrado em participar desse seleto grupo de profissionais responsáveis pela elaboração do ***PRICL***, na qualidade de representante da América Latina e na certeza de que o trabalho será significativamente facilitado pelo precioso apoio recebido do mercado de seguro e resseguro da região.

É hora de ter calma

ANTONIO PENTEADO MENDONÇA

PENTEADO MENDONÇA E CHAR
ADVOCACIA

O Brasil atravessa um momento delicado. As expectativas da nação quanto ao governo Bolsonaro vão derretendo e se a reforma da Previdência Social não passar com força, ou seja, pouco desidratada, as coisas tendem a ficar pretas rapidamente.

Como até agora a coordenação política do governo não mostrou para que veio, o grande vencedor da primeira batalha da reforma da Previdência foi o presidente da Câmara, deputado Rodrigo Maia. Acontece que o deputado não é subordinado ao presidente, nem tem alinhamento automático com as teses defendidas pelo executivo. Ao contrário, Rodrigo Maia é zeloso em manter sua independência e deixa isso claro cada vez que fala sobre o tema.

De outro lado, o bate cabeça entre as principais lideranças do executivo não faz bem a ninguém. A verdade é que até agora o governo não teve oposição séria feita pelos partidos políticos a esquerda e que perderam a eleição. PT e companhia estão mudos, se limitando a fazer barulho nas votações no Congresso. No entanto, o governo atrapalha o governo e as consequências vão desde o aumento do desemprego, até a queda de popularidade do presidente da república.

Neste cenário é extremamente difícil planejar seja lá o que for. O resultado é que a iniciativa privada está em compasso de espera e os investimentos previstos para agora estão suspensos até que a situação fique mais clara.

Ninguém vai investir sem ter certeza de que o país voltará a crescer. E aí temos um complicador a mais. Quer gostem, quer não gostem, o governo Michel Temer deixou o país organizado e na rota da retomada do crescimento. Mas as previsões para os números do primeiro trimestre do governo Bolsonaro apontam uma reversão do quadro, inclusive com a possibilidade concreta de crescimento negativo.

Os analistas econômicos reduzem semana depois de semana as expectativas para o PIB de 2019. O fechamento de postos de trabalho com carteira assinada cresce. Mais de 13 milhões de pessoas estão sem emprego. Mais de 40 milhões de brasileiros estão fora do mercado de trabalho. A renda média nacional não chega a R$ 2.500,00 mensais. As vendas estão estagnadas. O consumo das famílias está num dos níveis mais baixos dos últimos anos.

É esta a realidade a frente do executivo de uma seguradora que tem que planejar o futuro da companhia. No mínimo, é uma tarefa muito complicada. Exige conhecimento do país e das tendências. Exige conhecimento do jogo político, das manobras do Congresso, das necessidades dos governadores, das carências do país. Parte destes dados não fazem parte da rotina dos executivos. Mas, agora, se não forem consideradas e bem ponderadas, o desconhecimento pode levar a uma leitura equivocada do cenário, com consequências graves para o resultado da companhia.

O setor de seguros administra mais de um trilhão e duzentos bilhões de reais. Todavia a ordem de grandeza não é percebida pelas autoridades que dão ao segmento uma importância muito menor do que seria o correto. E este cenário não vai mudar rapidamente.

A inciativa privada, bem como a maior parte da sociedade, está cortando na carne para reduzir ao máximo os seus custos. Isso significa que as vendas seguem em patamar muito baixo. E sem vendas e novos negócios não há seguros para serem feitos.

O curto prazo com certeza não será uma festa para ninguém, muito menos para as seguradoras. Mas elas não precisam necessariamente se darem mal dentro da situação.

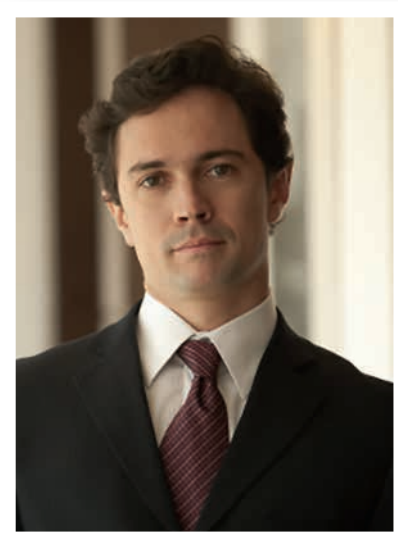
Com gestão, ponderação, bom senso, cautela e parcimônia não há porque uma companhia não navegar com relativo sucesso pelas águas agitadas do oceano brasileiro.

Mais importante do que isso, uma das alternativas possíveis é a reforma da Previdência Social passar com a consistência necessária para fazer a diferença e aí o Brasil retoma seu crescimento rapidamente. A partir de 2020 as incertezas desaparecem, a economia ganha corpo, os negócios se aceleram e o quadro atual se modifica completamente.

Se isso acontecer, o setor de seguros pode dobrar de tamanho em cinco anos, trabalhando apenas com os riscos atualmente seguráveis. O país é sub segurado. Aumentado a capilaridade e consequentemente os canais comerciais, as seguradoras e os corretores de seguros têm potencial para crescer de forma rápida e consistente, trabalhando apenas os segurados potenciais que atualmente não têm uma gama de seguros que estão aí, mas não são contratados.

Quem fizer a leitura correta do momento e das potencialidades de sua empresa tem tudo para, seja qual for o cenário, seguir em frente com solidez e perspectiva positiva para o futuro.

Seguro Garantia Judicial: Uma evolução legislativa e jurisprudencial em benefício de todos



DIÓGENES GONÇALVES
Sócio de Pinheiro Neto Advogados

GIANVITO ARDITO
Associado de Pinheiro Neto Advogados

RAÍSSA LILAVATI BARBOSA ABBAS CAMPELO
Associada de Pinheiro Neto Advogados

PINHEIRONETO
ADVOGADOS

Há uma notável crescente utilização do seguro garantia judicial em processos judiciais, seja para garantir o juízo, seja para substituir a constrição judicial sobre bens dos executados.

Esse aumento da emissão de seguros garantias judiciais está diretamente relacionado às mudanças legislativas, disponibilização de novos produtos pelas seguradoras e suas vantagens frente a outras formas de garantia, tais como a fiança bancária.

O Seguro Garantia tem por finalidade assegurar o fiel cumprimento de obrigações legais ou contratuais assumidas pelo tomador perante o segurado. O contrato de Seguro Garantia é tripartite, na medida em que envolve (i) o tomador do seguro, que

é o devedor da obrigação garantida pela apólice; (ii) o segurado (ou beneficiário), que é o credor da obrigação garantida – e no caso do seguro garantia judicial, o Poder Judiciário – e, finalmente, (iii) a companhia seguradora, que é a garantidora da obrigação.

Desde a década de 60, o seguro garantia já vinha sendo utilizado pelo mercado, o que ficou evidenciado no art. 20, 'e' e 'f' do Decreto-Lei nº 73/1966 que em sua redação original já previa a obrigatoriedade da contratação de seguro para "garantia do cumprimento das obrigações do incorporador e construtor de imóveis" e "garantia do pagamento a cargo de mutuário da construção civil, inclusive obrigação imobiliária".

Nas décadas de 1980/90, o Seguro Garantia foi previsto como forma de garantia ao Poder Público em contratos de compra e venda, fornecimento, construção, prestação de serviços, etc. e como forma de assegurar o cumprimento de propostas apresentadas pelos concorrentes de uma licitação (art. 46, §1º, III do Decreto-Lei 2.348/1987; e arts. 6º, VI, 31, III, 56, §1º, II da Lei 8.666/1993). Essa sistemática foi ainda mais fomentada com o advento dos dois modelos de Seguro Garantia, um para contratos privados e outro para contratos públicos, auxiliando especialmente nas garantias às concessões da década de 90 (Circulares SUSEP nºs 4 e 5/97).

Com o decorrer do tempo o produto seguro garantia passou a ser aperfeiçoado, culminando com a edição da Circular SUSEP nº232/2003 para regulamentos várias modalidades de seguro garantia. Uma dessas novas modalidades foi o Seguro Garantia Judicial, que é contratado pelo devedor perante uma seguradora para assegurar em Juízo o valor de obrigação que lhe é demandada, resguardando o seu interesse legítimo e/ou evitar constrições patrimoniais decorrentes de atos de penhora determinados no curso de procedimentos judiciais. Atualmente, o seguro garantia é regulamentado pela Circular SUSEP nº 477/2013.

São requisitos para o oferecimento do seguro garantia, especialmente em procedimentos administrativos e judiciais: (a) valor da garantia ser igual e, em alguns casos, ser 30% (trinta por cento) maior do que o valor do débito e corrigido pelo mesmo índice de atualização da dívida garantida; (b) regularidade da seguradora quanto à sua solvabilidade, retenção de risco e permissão governamental para oferecer tal garantia, sempre sob supervisão da Superintendência de Seguros Privados - SUSEP; (c) possibilidade de renovação da vigência da garantia até o final do litígio; (d) impossibilidade de cancelamento do seguro por inadimplência de prêmio; e (e) liquidez e aptidão para efeitos imediatos em caso de pedido de indenização nos termos da correspondente apólice.

A liquidez das garantias prestadas por seguradoras é assegurada pela observância necessária de uma série de requisitos, tais como capital mínimo, reservas técnicas atuariais, resseguro e cosseguro, prévia análise de risco para emissão de apólice, obrigatoriedade de prestação de contragarantia, entre outros, conforme regras e fiscalização pela SUSEP.

A certeza da exigibilidade do seguro garantia deriva de prévia aprovação do modelo básico desse tipo de garantia via normas da SUSEP de longa data, que, sob rigorosa fiscalização, avalia para aprovação os produtos de cada seguradora e de eventuais clausulados especiais a respeito.

Do ponto de vista econômico, a garantia representada pelo seguro garantia é tão líquida quanto a fiança bancária, é prestada por seguradora devidamente autorizada a atuar como instituição financeira, inclusive sujeita a normas de solvência derivadas do Acordo da Basiléia tal como ocorre com os bancos, e tem como vantagens o menor

custo cobrado do tomador e fato de não consumir limites de crédito bancário do devedor. A resiliência e solvabilidade do sistema de seguro garantia é, ainda, potencializada pela obrigatoriedade do resseguro de porções relevantes dos riscos, gerando maior capilaridade e pulverização de riscos, evitando que as partes estejam sujeitas a eventuais questões de liquidez da seguradora.

Quando esse produto surgiu, houve grande resistência do Poder Judiciário em aceitá-lo.

O primeiro passo para combater essa resistência veio com a Lei nº 11.382/2006, que alterou o Código de Processo Civil de 1973 para prever a possibilidade de substituir a penhora judicial por seguro garantia ou por fiança bancária (art. 656, § 2º, do Código de Processo Civil de 1973). [1]

Porém, os Tribunais ainda permaneciam resistentes à utilização do seguro garantia judicial, pois (i) a lei estabelecia apenas a possibilidade de substituição de penhora por seguro garantia, (ii) o dinheiro ainda tinha preferência legal sobre o seguro garantia e (iii) especificamente no âmbito das execuções fiscais, a Lei nº 6.830/1980 não dispunha sobre o seguro garantia.

Pouco a pouco, o Poder Judiciário passou a aceitar o seguro garantia judicial como forma regular de garantia, assemelhada à fiança bancária. Porém, isso ainda não era o bastante.

Assim, o segundo passo para evolução na aceitação do seguro garantia pelo Poder Judiciário veio com tanto por atos normativos da própria Procuradoria Geral da Fazenda Nacional[2] quanto pela Lei nº 13.043/2014, que admitiu expressamente a possibilidade de a execução fiscal ser garantida por meio de seguro (art. 7º, II, da Lei nº 6.830/1980).[3]

A terceira e provavelmente mais importante medida veio com o Novo Código de Processo Civil que (i) manteve a possibilidade de substituição de penhora por seguro garantia e fiança bancária – e, sim, o seguro garantia vem mencionado antes mesmo da fiança bancária no texto legal – e (ii) inovou ao dispor que o seguro garantia judicial se equipara a dinheiro (art. 835, § 2º, do Código de Processo Civil de 2015).[4]

É inegável que o legislador poderia ter ido além para deixar claro que o seguro garantia judicial pode ser a primeira garantia apresentada em juízo, não se limitando a sua utilização para a substituição de uma penhora.

Todavia, o silêncio do legislador a esse respeito não afasta a possibilidade de o seguro garantia ser a primeira garantia a ser apresentada em juízo, pois a lei expressamente equipara o seguro garantia a dinheiro. Além disso, a admissão do seguro garantia apenas para casos de substituição resultaria na prática de atos processuais desnecessários, à medida que primeiro seriam praticados atos de penhora para posteriormente se estabelecer a substituição.

A jurisprudência do Superior Tribunal de Justiça evoluiu de forma gradativa a ponto de conferir maior segurança para a utilização do seguro garantia judicial.

---

1 "Art. 656. § 2º A penhora pode ser substituída por fiança bancária ou seguro garantia judicial, em valor não inferior ao do débito constante da inicial, mais 30% (trinta por cento)."

2 O oferecimento de seguro como forma de garantia judicial foi ainda incrementado pela Portaria PGFN nº 1.153/09, que regulamenta a apresentação desta forma de caução nos autos de processos judiciais e procedimentos administrativos referentes a tributos federais (débitos inscritos na Dívida Ativa da União).

3 "Art. 7º - O despacho do Juiz que deferir a inicial importa em ordem para:
II - penhora, se não for paga a dívida, nem garantida a execução, por meio de depósito, fiança ou seguro garantia."

4 "Art. 835. § 2º Para fins de substituição da penhora, equiparam-se a dinheiro a fiança bancária e o seguro garantia judicial, desde que em valor não inferior ao do débito constante da inicial, acrescido de trinta por cento."

Existem posicionamentos conflitantes entre turmas daquela Corte Superior quanto a diversos pontos que circundam o seguro garantia judicial, notadamente acerca da possibilidade ou não de substituição de dinheiro depositado por seguro garantia, mesmo após o Novo Código de Processo Civil. Nesse particular, apenas um julgado vinculante é que teria o condão de pacificar o assunto.

A despeito de inexistir um precedente com essa vinculação, é inegável a constatação de que um paradigma vem sendo quebrado gradativamente para assegurar aos jurisdicionados a utilização do seguro garantia.

Para evidenciar o que foi dito até agora, destaca-se trecho do acórdão do Recurso Especial nº 1.691.748, em qual o Min. Ricardo Villas Bôas Cueva da 3ª Turma foi categórico ao reconhecer a importância econômica e jurídica do seguro garantia judicial:

> "9. No cumprimento de sentença, a fiança bancária e o seguro garantia judicial são as opções mais eficientes sob o prisma da análise econômica do direito, visto que reduzem os efeitos prejudiciais da penhora ao desonerar os ativos de sociedades empresárias submetidas ao processo de execução, além de assegurar, com eficiência equiparada ao dinheiro, que o exequente receberá a soma pretendida quando obter êxito ao final da demanda.
>
> 10. Dentro do sistema de execução, a fiança bancária e o seguro garantia judicial produzem os mesmos efeitos jurídicos que o dinheiro para fins de garantir o juízo, não podendo o exequente rejeitar a indicação, salvo por insuficiência, defeito formal ou inidoneidade da salvaguarda oferecida.
>
> 11. Por serem automaticamente conversíveis em dinheiro ao final do feito executivo, a fiança bancária e o seguro garantia judicial acarretam a harmonização entre o princípio da máxima eficácia da execução para o credor e o princípio da menor onerosidade para o executado, a aprimorar consideravelmente as bases do sistema de penhora judicial e a ordem de gradação legal de bens penhoráveis, conferindo maior proporcionalidade aos meios de satisfação do crédito ao exequente.
>
> 12. No caso, após a definição dos valores a serem pagos a título de perdas e danos e de astreintes, nova penhora poderá ser feita, devendo ser autorizado, nesse instante, o oferecimento de seguro garantia judicial pelo devedor, desde que cubra a integralidade do débito e contenha o acréscimo de 30% (trinta por cento), pois, com a entrada em vigor do CPC/2015, equiparou-se a dinheiro."
>
> (STJ - REsp 1691748/PR, Rel. Min. RICARDO VILLAS BÔAS CUEVA, 3ª Turma, j. 7.11.2017, DJe 17.11.2017)

Conclui-se, assim, que o seguro garantia judicial é uma garantia válida, eficaz e suficientemente idônea para assegurar o Juízo para eventual satisfação de débitos em litígio. Além disso, de uma perspectiva econômica, é garantia mais vantajosa do que modalidades semelhantes, tais como a fiança bancária.

A auditoria atuarial e de benefícios para as Entidades supervisionadas pela PREVIC

Instrumento complementar às atividades de fiscalização e ampliação dos mecanismos de defesa e proteção dos direitos dos participantes dos fundos de pensão

MARCO PONTES
Atuário, sócio líder da área de Serviços Atuariais da RSM ACAL.

A nova economia, ancorada nos paradigmas atuais, tem passado, ao longo das últimas décadas, por profundas modificações em diversos sentidos: social, econômico, comportamental e tecnológico, apenas para citar algumas. Não se pode negar o impacto que o processo de globalização causou sobre as diversas atividades de serviço. As atividades contábil e atuarial, cada vez mais complementares, não estão imunes a esses processos e têm a obrigação de se atualizar nas mais variadas formas, de modo a cumprirem seu papel, sob pena de serem corroídas pelo célere processo de desenvolvimento de negócios e acabarem por serem incapazes de acompanhar e traduzir as mudanças frequentes no ambiente empresarial, em que políticas arrojadas, adotadas por executivos, práticas lesivas aos interesses de uma corporação, possam vir a carecer de uma divulgação adequada. Por isso, as

práticas contábeis e atuariais devem estar comprometidas e em perfeita sintonia com o complexo e ágil mundo corporativo atual, especialmente em alguns setores-chaves, como é o setor de previdência complementar.

Com a introdução do IFRS no Brasil, os critérios de preparação de relatórios financeiros divulgados ao público passaram a ter um nível de exigência maior. A Superintendência Nacional de Previdência Complementar – PREVIC tem dado mostras de caminhar no sentido de imprimir mais transparência às Demonstrações Financeiras. Em 2018, colocou em audiência pública a CPC 49, que estabelece os princípios aplicados nas demonstrações contábeis de planos de aposentadoria. A norma tem vigência para os exercícios sociais que se iniciarem a partir de 1º de janeiro de 2019.

Esse importante passo para o setor se constitui em um marco, em vista do fato de a previdência complementar ser a principal formadora de poupança no país. Ainda nos encontramos aquém da capacidade que o país possui comparativamente às principais economias do mundo. Daí a necessidade de tornar os relatórios mais transparentes e inteligíveis, de modo que os usuários interessados e, em última instância, a sociedade, sejam capazes de auferir a credibilidade necessária as nossas atividades. Entendemos que a contabilidade, em sua essência pura, seja capaz de traduzir o que ocorre nas corporações, até mesmo naquelas mais complexas, como é o setor de previdência complementar. Por acreditarmos que é imperativa a reformulação constante do papel do auditor, não se pode deixar de exigir a reformulação de determinados conceitos básicos, entre outros, sua postura, no que tange às provisões estimadas pelo atuário e outras provisões que compõem, em maior parte, o estoque do passivo de uma organização que lida com risco, como o caso das seguradoras, os fundos de pensão e operadoras de saúde.

As Entidades de Previdência Complementar e as seguradoras são as principais investidoras institucionais e serão as forças motrizes do desenvolvimento da economia brasileira para os próximos anos, especialmente no atual momento em que se discute a necessidade de reformar o sistema de previdência com a introdução do pilar de capitalização. Por essa razão, uma corporação que possui grande estoque de compromisso de natureza atuarial não pode ser tratada de forma segregada, mas, fundamentalmente, de forma orgânica, como qualquer outra empresa. Isso ficou claro por ocasião do primeiro ciclo de privatizações que teve início nos dois mandatos dos governos FHC. Naquela ocasião, os compradores e investidores interessados na aquisição de empresas estatais detectaram déficits elevados nos planos de aposentadoria das empresas estatais que foram privatizadas. Observamos, com certo pesar, uma falha grave no sistema, pois os auditores independentes tinham como prática dividir opinião com os atuários. Essa postura contribuiu fortemente para detecção de déficits com os programas de aposentadoria dos empregados de empresas estatais. Posteriormente, tal procedimento foi corrigido, quando as denominadas Big Four passaram a possuir, em seus quadros, profissionais atuários.

A situação melhorou a partir do instante em que as quatro grandes firmas de auditoria passaram a não mais dividir opinião com os atuários responsáveis pelas informações que compunham a coluna do passivo das DF´s. Tal fato ocorreu a partir da inclusão de metodologias adicionais ao rol de procedimentos nos trabalhos de auditoria das demonstrações financeiras, no que tange aos compromissos de natureza atuarial que compõem os balanços de uma entidade de previdência ou seguradora.

Provavelmente, se houvesse regulamentação suficiente para proteger os participantes e procedimentos de auditoria que compreendesse os passivos atuariais, situações como a que ocorreu com o fundo de aposentadoria dos funcionários do Banerj não teriam ocorrido. Engana-se quem acredita que, durante o governo FHC, foi a primeira vez que o sistema foi colocado à prova.

Se voltarmos mais no tempo, nos depararemos com uma situação mais dramática. Quem não se lembra da ação nefasta dos Montepios, que culminou por lesar um grande contingente da população brasileira que se viu desprovida de qualquer proteção quando precisou? A ausência de uma legislação específica causou um efeito nefasto à população e contribuiu decisivamente para criar uma grande barreira psicológica para o desenvolvimento da previdência complementar, segundo o modelo aberto no país.

Tal fato ocorreu por diversas razões, dentre às quais podemos destacar: (i) a ausência de uma legislação que regulasse a matéria, como já afirmamos; (ii) aos efeitos maléficos da inflação, e (iii) pela ação temerária e má gestão de empresários que atuavam no setor. Contudo, os tempos são outros, houve um avanço significativo dos órgãos de supervisão ao longo das últimas décadas, os quais contribuíram decisivamente para proteger o consumidor final.

Em 2014, por exemplo, a Susep saiu na frente da Previc ao exigir das empresas por ela supervisionada a auditoria atuarial anual concomitantemente com a auditoria contábil. Tal exigência, sem dúvida, deu mais credibilidade ao sistema. Agora, a PREVIC tem uma grande oportunidade de corrigir uma distorção no sistema de previdência complementar fechado, apoiando o trabalho realizado pelo Comitê de Pronunciamento Atuariais do Instituto Brasileiro de Atuária – IBA, refletido no CPA 017, que trata da auditoria atuarial e de benefícios para as supervisionadas pela PREVIC.

O documento dispõe sobre procedimentos específicos para a realização de auditoria atuarial e de benefícios, cujo conteúdo deve ser observado pelos atuários que vierem exercer esta atividade junto às Entidades supervisionadas pela Previc. Tal documento é fruto de um profundo trabalho realizado pelo IBA, se constituindo em mais um elemento para melhorar a gestão e governança das Entidades Fechadas, aumentando a abrangência que se faz necessária e que na atualidade não é atingida pelo trabalho de auditoria contábil das demonstrações financeiras realizadas pelas firmas de auditoria.

O aumento da tecnicidade exigida pelos órgãos de supervisão no Brasil nos últimos anos é uma realidade e deve se consolidar no país, visto que os órgãos reguladores têm buscado o aprimoramento contínuo da transparência das informações financeiras. Negligenciar esse fato é ir contra um princípio fundamental da contabilidade e da atuária: a transparência e a independência. Exemplo deste aprimoramento regulatório foi a publicação da Resolução CGPAR 09/2016, que estabeleceu a realização de auditoria interna periódica para as empresas estatais federais que patrocinam fundos de pensão, sendo os resultados dessa auditoria submetidos diretamente ao Conselho de Administração dessas empresas e, mais recentemente, à Resolução CGPAR 25/2018, que estabelece diretrizes e parâmetros para as empresas estatais federais quanto ao patrocínio planos de benefícios de previdência complementar.

No caso da CGPAR 09/2016, entre as diversas áreas que a auditoria interna precisa se manifestar, estão os aspectos relacionados à metodologia utilizada no cálculo atuarial, custeio, consistência dos dados e aderência das hipóteses. Nesse sentido, o Comitê

de Pronunciamentos Atuariais - CPA 17 vem ao encontro dessa Resolução, fornecendo subsídios para a condução dos procedimentos necessários para a emissão de uma opinião sobre o quadrante atuarial. Não obstante, como bem citado no guia de Melhores Práticas da Previc, recomenda-se a realização da auditoria atuarial periodicamente, sendo instrumento de gestão e busca de aprimoramento das práticas de governança por todos os fundos de pensão.

As responsabilidades das referidas provisões de natureza atuarial devem ser revistas, de modo que a administração do Fundo de Pensão, seus atuários e auditores, independentemente da natureza ou grau de complexidade que possa existir, assumam suas responsabilidades no grau e nível que couber, e todo o esforço nesse sentido deve ser empregado.

Embora exista alguma resistência de certos profissionais do setor que tem um ponto de vista contrário à realização da auditoria atuarial e de benefícios por entender que representará mais custos para a Entidade, não há dúvidas de que os ganhos advindos de sua adoção podem gerar valor para todos os stakeholders do setor de fundos de pensão e contribuir de forma decisiva para os órgãos de fiscalização, especialmente no que tange à situação de solvência e equilíbrio econômico, financeiro e atuarial dos planos e como mecanismo de defesa e proteção dos direitos dos participantes dos fundos de pensão para que situações como a que ocorreu com o fundo de pensão do Banerj não venham a acontecer novamente.

Essa postura não afeta de modo algum o conceito de prudência, conservadorismo ou independência e deve ser vigorosamente incentivada. Por uma questão de segurança, princípios e de compromisso com a transparência, a contabilidade e a atuária devem seguir cumprindo o seu papel fundamental de informar correta e suficientemente aos investidores, credores, órgãos reguladores o que ocorre nas corporações, independentemente do ramo de atividade, setor ou indústria a que pertença.

O sistema de previdência complementar tem um grande desafio para os próximos anos e precisa de regras claras, que propiciem maior segurança e transparência para o setor, especialmente neste momento em que se discute a reforma da previdência, como já destacamos no preâmbulo deste artigo.

CURSOS DE CAPACITAÇÃO PARA PROFISSIONAIS DO MERCADO DE SEGUROS

SÃO PAULO DE 06 A 14 DE AGOSTO

Seguro RCP - Advogados

Explicação dos riscos inerentes à atividade jurídica. Análise dos limites adequados para mitigação do risco. Ponderação de franquia e participação obrigatória de acordo com as particularidades do escritório. Exercício de sinistros de uma falha no contencioso e no consultivo.

Seguro RCP - Engenharia e RC Obras

Explanação da diferença do risco coberto de cada produto. Qual o trigger de cada um e o período de proteção do segurado/exposição da seguradora. Discussão sobre as principais coberturas das apólices.

Seguro RCP - Médicos e Hospitais

Aspectos de cobertura dos produtos para proteção de falha profissional dos profissionais da área da saúde. Diferença entre dano e risco estético. Dano moral puro. Alcance da definição de ato médico. Sinistro em prestação de serviço continuado (quando é caracterizada a falha). Relação dos profissionais e prestadores a quem se destina o produto.

Seguro RCP - Miscellaneous Avançado

Explicação do risco coberto e de todas as extensões de cobertura do produto – o que são e qual a aplicação delas na prática. Análise do riscos excluídos que reduzem a proteção para o segurado. Discussão acerca da colocação do risco em cosseguro e resseguro –quais as vantagens e desvantagens de cada procedimento. Tipos de profissionais que podem contratar a apólice e quais seus riscos.

Seguro D&O - Entenda o risco

Qual o tamando do risco dos gestores de acordo com as leis de falência, ambiental, código de defesa do consumidor, trabalhista, código penal, anticorrupção, etc. Análise prática do caso Brumadinho no seguro D&O; todos os envolvidos são segurados? E se forem processados por homícidio das vítimas, está coberto?

Seguro D&O - Avançado

Apresentação das principais definições da apólice, tais como: ação social, ato de gestão, entidade externa, perda e segurado. Como é aplicado os conceitos de reclamações conexas, limite agregado e limite máximo de indenização. Vantagens e desvantagens entre resseguro e cosseguro. Explicação de todas as extensões de cobertura do produto – o que são e qual a aplicação delas na prática. Em quais situações e o que acontece com o Run-off em falência, recuperação

ASSINANTE RONCARATI TEM 15% DESCONTO!

INSCREVA-SE JÁ

SAIBA MAIS EM: cursos.linhasfinanceiras.com

LF cursos
EXPERT EM SEGUROS

RONCARATI
EDITORA

A Lei Geral de Proteção de Dados

Parte I – Antecedentes e elementos para sua interpretação

JOÃO MARCELO RICARDO MÁXIMO DOS SANTOS
Sócio fundador do escritório
Santos Bevilaqua Advogados

GÉSSIKA SAMPAIO DA FONSECA
Advogada do escritório
Santos Bevilaqua Advogados

I. Introdução

Historicamente, o Brasil sempre se diferenciou de outros países por não ter uma legislação de proteção da privacidade e da confidencialidade de dados pessoais.

Nesse sentido, as normas que de alguma forma se aplicavam ao tratamento de dados pessoais obtidos por empresas eram, principalmente, o Código Civil, o Código do Consumidor e a Constituição. A exceção a essa regra é o sigilo bancário, objeto da Lei Complementar nº 105/2001.

No tocante à utilização de dados pelo setor público, tampouco existiam regras específicas, tornando-se necessária a aplicação analógica do Código Civil e do Código do Consumidor.

Ocorre que a disponibilidade e o tráfego de informações se ampliaram de formas antes inimagináveis, como também se multiplicaram os métodos para a obtenção, utilização e transferência e dessas informações. Tudo isso com uma redução exponencial de custos para a realização dessas atividades.

Ou seja, mesmo países nos quais já existia uma legislação para o tratamento de informações pessoais viram-se obrigados a

desenvolver novas regras e a impor novas responsabilidades e sanções relacionadas ao tema.

No caso do Brasil, pulamos a etapa das normas sobre privacidade, confidencialidade e dados pessoais pré-internet e editamos a Lei nº. 13.709/2018 - a Lei Geral de Proteção de Dados - já em uma realidade na qual a digitalização já havia avançado e avança mais, com velocidade exponencial, em todos os aspectos da vida e das relações.

Outro desafio a ser enfrentando pelo novo paradigma da digitalização é a natureza transnacional do tratamento das informações pessoais, a qual obriga os legisladores nacionais a repensarem as formas como interferem nos seus ordenamentos jurídicos, sob pena de editarem regras com pouco ou nenhum efeito prático relevante.

Nesse sentido, a impossibilidade de os legisladores confinarem nas suas jurisdições o trânsito dos dados pessoais, juntamente com a atual transitoriedade estrutural das coisas, geraram a edição de normas de eficácia extraterritorial e com maior grau de indeterminação, focadas na imputação de responsabilidade pela construção de estruturas de controle.

Essa tendência, aliás, tem sido evidente desde a edição das regras tratando da prevenção ao tráfico de drogas, à corrupção e à lavagem de dinheiro. Mas a extraterritorialidade era inicialmente uma iniciativa principalmente norte-americana, e foi consagrada como padrão global, com a edição das regras sobre recepção e tratamento de dados pessoais pela União Europeia, a *General Data Protection Rule* – GDPR.

A extraterritorialidade é um elemento extremamente importante da GDPR e criou a necessidade prática, para todas as empresas multinacionais com operações na União Europeia e todas as empresas que têm relações negociais com elas (ou seja, uma parte relevante de qualquer ambiente de negócios do mundo) de adaptarem suas operações, para estarem em conformidade com a GDPR.

Esse é o contexto no qual escrevemos esse estudo, em duas partes.

Nosso objetivo, nessa primeira parte, é tratarmos (i) da necessidade de proteção de dados pessoais de forma geral, do (ii) estado geral de desenvolvimento das regras de diferentes jurisdições sobre dados pessoais, com especial foco nas principais características da GDPR, e (iii) das normas brasileiras que, antes da edição da Lei nº. 13.709/2018, regulavam, em algum aspecto, o tratamento de dados pessoais.

Na segunda parte, a ser publicada em complemento a esta, faremos comentários sobre a Lei nº. 13.709, de 14 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados – LGPD, a qual foi alterada pela Medida Provisória nº. 869, de 27 de dezembro de 2018.

II. Do Contexto Atual e da Necessidade de Regulamentar a Proteção de Dados Pessoais

Apesar de a repercussão midiática do uso indevido de dados ser bastante recente, a preocupação com o respeito pelos direitos e liberdades fundamentais, e especialmente pelo direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal, antecede os anos 2000. Em 1981 foi estabelecido pelo Conselho Europeu o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados: a Convenção 108.

A Convenção tinha como objetivo proteger o indivíduo contra os abusos que

podem acompanhar a coleta e o processamento de dados pessoais, além de regular o fluxo dessas informações entre países. Ademais, proibiu o processamento de dados sensíveis, ou seja, dados referentes a raça, posicionamento político, saúde, religião, vida sexual, registro criminal, entre outros, na ausência de salvaguardas legais[1].

Seu objetivo primordial era tratar as informações relativas aos indivíduos com mais transparência e incluí-los na tomada de decisão sobre o uso dos seus dados. Para isso, as organizações deveriam orientar-se por princípios como a minimização da especificação do propósito, além de garantir os direitos à portabilidade, retificação e esquecimento.

Contudo, além da necessidade do estabelecimento de limites para o tratamento dos dados pelas próprias organizações, era preciso também exigir que estas tomassem providências para proteger os dados sob seu poder, a todo momento sob ameaças externas.

Vivemos hoje na sociedade da informação e do conhecimento. Com o desenvolvimento da internet e da digitalização das informações em geral, as interações entre pessoas naturais e jurídicas passaram a ser predominantemente digitais e muito mais globais, o que viabilizou o uso, processamento e aquisição de informações de forma mais disseminada e intensa. Ao mesmo tempo em que a informação em geral, da perspectiva das pessoas, ficou muito mais disponível, as informações pessoais passaram a ser um recurso estratégico das empresas.

Segundo o professor Luís Manuel Borges Gouveia, *"a Sociedade da informação está baseada nas tecnologias de informação e comunicação que envolvem a aquisição, o armazenamento, o processamento e a distribuição da informação por meios electrónicos, como a rádio, a televisão, telefone e computadores, entre outros. Estas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, económicos e políticos, criando uma nova comunidade local e global: a Sociedade da Informação.*[2]".

Nesse novo paradigma, não somente a maior quantidade e o maior fluxo de informações pessoas como a inteligência artificial e a internet das coisas vão cada vez mais influenciar a forma como as pessoas veem e são vistas pelo mundo.

A inteligência artificial relaciona-se com a capacidade de máquinas serem capazes de aprender, raciocinar, deliberar e tomar decisões de forma racional e inteligente, o que se dá por meio da criação de algorítimos que interpretam dados.

Por outro lado, a internet das coisas reside na conexão à internet de todo o tipo de objeto físico, desde torradeiras de pão a turbinas de avião. Conectados, esses dispositivos coletam dados e podem se comunicar entre si, tornando o mundo físico e o digital cada vez mais intrincados.

E as duas coisas estão cada vez mais interligadas: *"epitomized by the advent of autonomous and connected vehicles (ACV's), the merger of AI with the IoT holds a vast potential to reshape the boundaries of public and private spheres, and to transform human interactions with their immediate environment, for better or worse3".*

1 Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal. Ministério Público. Disponível em <http://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_protecao_pessoas_tratamento_automatizado_dados_caracter_pessoal.pdf>. Acesso em 15 de maio de 2018.

2 Gouveia, Luís Manuel Borges. *Sociedade da Informação: Notas de contribuição para uma definição operacional.* 2004. Disponível em <http://homepage.ufp.pt/lmbg/reserva/lbg_socinformacao04.pdf>. Acesso em 19 de maio de 2018.

3 Hacker, Philipp. Personal data, exploitative contracts, and algorithmic fairness: autonomous vehicles meet

Nesse contexto, não podemos deixar de mencionar o *blockchain*, que tornará cada vez mais confiáveis e completas as informações pessoais recebidas.

E, com isso, os *smart contracs*, pelos quais obrigações das partes são executadas sem a intervenção de pessoas, ocuparão espaço cada vez maior, o que, em um círculo virtuoso, vai aumentar a necessidade de prestação e a utilidade prática das informações pessoais.

Imagine-se, por exemplo, a hipótese de um proprietário de um automóvel que sofre um acidente. Os danos ao carro podem ser imediatamente identificados por um software nele embarcado e informados a uma seguradora, a qual imediatamente identifica a espécie de dano e sua cobertura, um transporte para o segurado, um reboque para o automóvel e uma oficina, aos quais solicita imediatamente um orçamento, o qual pode ser imediatamente pré-aprovado. Feito isso tudo, o segurado, logo após o acidente, é orientado sobre como deve agir.

Note-se, para além da possibilidade prática e condição tecnológica da situação acima, a quantidade e a relevância das trocas de informações que antecedem e sucedem o evento é muito grande. E, dependendo do exemplo, pode implicar em fluxo de informações transnacional.

Além dos riscos oferecidos pelas próprias organizações no uso e tratamento de dados, como o desvio da finalidade ou a manipulação de informações, por exemplo, há também ameaças externas constantes de que esses dados sejam violados, por meio dos chamados ciberataques.

Ciberataque pode ser definido como a tentativa de invadir sistemas e máquinas para se apoderar de determinadas informações. Esses ataques usam da criptografia – técnica que transforma informação inteligível em algo que um agente externo seja incapaz de compreender – para capturar dados e fazer com que as empresas tenham que pagar para tê-las de volta. Geralmente, o ciberataque vem associado a um objetivo financeiro, mas também pode ser utilizado para apagar informações existentes[4].

De acordo com uma pesquisa realizada pela Trend Micro, empresa de segurança da informação, 51% das companhias brasileiras sofreram ataques *ransomware* (ações em que os hackers criptografam ou bloqueiam o sistema de computador de uma organização e, em seguida, exigem resgate para descriptografá-lo ou liberá-lo) em 2016. Esse mesmo estudo constatou que 56% das empresas não possuem tecnologia para detectar comportamento suspeito[5].

Além disso, entre março de 2016 e março de 2017, esse tipo de ataque aumentou cinco vezes, segundo especialistas em segurança cibernética da Kaspersky Lab[6], o que demonstra o crescimento exponencial do risco cibernético. Assim, além de investir na segurança dos seus sistemas, nas políticas de *compliance* e em uma mudança estrutural interna, as organizações devem estar preparadas para lidar com ciberataques e como gerenciar os riscos daí decorrentes.

Em 2016, por exemplo, a Uber sofreu um cyberataque que expôs dados de 57 milhões de pessoas, dentre os quais, 196 mil eram brasileiros[7]. Segundo a Companhia, os dados expostos foram nome, endereço

---

the internet of things. *International Data Privacy Law*, Volume 7, Issue 4, 1 November 2017, Pages 266–286. Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3007780. Acesso em 18 de maio de 2018.

4 O que é um ciberataque? http://www.cartaeducacao.com.br/carta-explica/o-que-e-um-ciberataque/

5 http://www.revistacobertura.com.br/2017/03/21/aumento-de-ciberataques-eleva-busca-por-seguros-cyber-risks/

6 Idem.

7 Vazamento de dados da Uber atingiu 196 mil brasileiros. Tecmundo. Disponível em <https://www.tecmundo.com.br/seguranca/129236-vazamento-dados-uber-atingiu-196-mil-brasileiros.htm>. Acesso em 08 de maio de 2018.

de email e telefone celular dos usuários[8]. Para agravar a situação, a empresa omitiu o ataque, que somente foi divulgado em novembro de 2017[9].

No Brasil, o Ministério Público do Distrito Federal e Territórios – MPDFT instaurou inquérito civil para averiguar o ocorrido.

Outro exemplo de repercussão mundial foi a obtenção e vazamento de dados de mais de 50 milhões de usuários do Facebook. No começo de 2014, o pesquisador russo Aleksandr Kogan lançou no Facebook um teste de personalidade, aparentemente inofensivo. Por meio desse teste, conseguiu recolher informações de 50 milhões de pessoas.

Esses dados foram repassados para a empresa Cambridge Analytica, que logo percebeu que tais informações poderiam ser utilizadas de forma estratégica. Um funcionário da empresa divulgou o ocorrido e expôs que, analisando todos os dados aos quais teve acesso, a empresa descobriu padrões como, por exemplo, que pessoas que odiavam Israel, gostavam de uma determinada marca de chocolate.

O uso, manipulação e interpretação desses dados, por meio de algoritmos, foi apontado como tendo sido utilizado na campanha do atual presidente dos Estados Unidos, Donald Trump, que tinha como chefe de marketing Steve Bannon, um dos fundadores da Cambridge Analytica[10].

O alvo dos roubos e do uso indevido de dados, entretanto, não se limita a empresas que prestam serviços por meios tecnológicos, como o Uber e o Facebook.

Um exemplo disso, foi a invasão realizada em computadores de 7.998 professores de 320 universidades em todo o mundo, nos últimos 5 anos, realizado por nove iranianos que trabalhavam em nome do Corpo dos Guardas da Revolução. De 2013 até 2018, os hackers roubaram 31,5 terabytes de documentos e dados, incluindo pesquisas científicas, periódicos e dissertações, de acordo com a acusação. Seus alvos também incluíram as Nações Unidas, 30 empresas dos EUA e cinco agências do governo dos EUA[11].

Outro caso, foi a violação de segurança que comprometeu informações pessoais e financeiras dos compradores das redes de lojas de departamento americanas Saks Fifth Avenue e Lord & Taylor. Em abril deste ano, hackers obtiveram informações de mais de cinco milhões de cartões de crédito e de débito em poder das lojas e liberaram para venda em fóruns na internet, de acordo com a Gemini Advisory LLC, uma empresa de segurança cibernética de Nova York, nos Estados Unidos[12].

Também em abril, no Brasil, o Ministério Público do Distrito Federal e Territórios (MPDFT) instaurou inquérito civil público para apurar o uso indevido de dados de aproximadamente 73 milhões de usuários da Vivo. Segundo o MP, a empresa utilizou as informações para a venda de espaço

8 Vazamento da Uber expôs nome, telefone e email de 156 mil usuários brasileiros. Folha Uol. Disponível em < https://www1.folha.uol.com.br/mercado/2018/04/vazamento-da-uber-expos-nome-telefone-e-email-de-156-mil-usuarios-brasileiros.shtml>. Acesso em 08 de maio de 2018.

9 Uber omitiu ciberataque que expôs dados de 57 milhões de pessoas. Tecmundo. Disponível em <https://www.tecmundo.com.br/seguranca/124408-uber-omitiu-ciberataque-expos-dados-57-milhoes-pessoas.htm?utm_source=tecmundo.com.br&utm_medium=referral&utm_campaign=circulacao>. Acesso em 09 de maio de 2018.

10 Zuckerberg reconhece que erros no Facebook permitiram roubo de dados. Mais de 50 milhões de usuários foram afetados. Testes da rede social forneceram informações pessoais a seus desenvolvedores. Disponível em <http://g1.globo.com/jornal-nacional/noticia/2018/03/zuckerberg-reconhece-que-erros-no-facebook-permitiram-roubo-de-dados.html>. Acesso em 10 de maio de 2018.

11 Massive cyberhack by Iran allegedly stole research from 320 universities, governments, and companies. Sciencemag. Disponível em <http://www.sciencemag.org/news/2018/03/massive-cyber-hack-iran-allegedly-stole-research-320-universities-governments-and>. Acesso em 10 de maio de 2018.

12 Hackers roubam dados de milhões de cartões nos EUA. Veja. Disponível em <https://veja.abril.com.br/mundo/hackers-roubam-dados-de-milhoes-de-cartoes-nos-eua/>. Acesso em 11 de maio de 2018.

publicitário. No caso, seria possível identificar, por exemplo, usuários em tratamento médico, a partir do mapeamento da circulação em clínicas e hospitais[13], e assim oferecer publicidade específica e direcionada a pessoas com esse perfil.

Outro ponto relevante a ser considerado é a dificuldade em tratar os temas acima como problemas de uma jurisdição.

Com efeito, a extraterritorialidade tem sido um dos instrumentos cuja utilização se tornou frequente, de modo a tentar evitar que a nova dinâmica de localização geográfica de empresas, atividades e clientes reduza a efetividade das regras editadas pelos estados nacionais.

De fato, a extraterritorialidade de determinadas regras de sanções econômicas pode estar sujeita a maior controvérsia.

De qualquer forma, independentemente de se concordar com o monismo a que induz, a extraterritorialidade pode ser considerada, em cada caso concreto, boa ou ruim, dependendo da visão política em relação ao tema regulado. Por exemplo, dificilmente se pode discutir o mérito das regras globais de combate ao terrorismo, tráfico de drogas e corrupção e lavagem de dinheiro em geral, as quais têm, inclusive, impulsionado a criação de regras mais efetivas em ordenamentos jurídico nacionais.

De qualquer modo, a crescente extraterritorialidade nas normas decorre de um problema prático com que os Estados nacionais têm que lidar, qual seja, a globalização das atividades econômicas e empresas, somada à extrema "portabilidade" das estruturas produtivas e atividades entre diferentes países.

13 Vivo é investigada por uso indevido de dados de 73 milhões de usuários: Segundo Ministério Público, informações permitiam direcionamento de publicidade. O Globo. Disponível em <https://oglobo.globo.com/economia/defesa-do-consumidor/vivo-investigada-por-uso-indevido-de-dados-de-73-milhoes-de-usuarios-22553219>. Acesso em 11 de maio de 2018.

No caso concreto da obtenção, manutenção e tratamento de informações pessoais, estas podem ser organizadas em blocos cuja transferência e manipulação são fáceis e potencialmente muito danosas para as pessoas envolvidas. Por isso, uma legislação que não tivesse efeitos extraterritoriais teria a eficácia enfraquecida pela possibilidade de transferências de informações para entidades localizadas em outros países, onde seriam possivelmente tratadas sem que a norma local alcançasse tais pessoas e tratamentos.

Por outro lado, a possibilidade de toda essa informação disponível e plenamente gerenciável ser utilizada para criar um ambiente hostil, discriminatório, permeado por manipulação e exploração abusiva de vulnerabilidades é mais um elemento a ser considerado no estabelecimento das regras em questão.

Parece, de fato, necessário o estabelecimento de regras ao mesmo tempo efetivas para proteger a privacidade e a construção de um ambiente econômico e social ético e que, ao mesmo tempo, não dificultem a conquista de novos espaços e a realização de todas as nossas potencialidades.

Em outras palavras, temos que organizar um novo sistema de obrigações e responsabilidades que torne suportáveis os enormes riscos emergentes de novas tecnologias aplicadas à obtenção e tratamento de dados pessoais.

III. O Regulamento Geral de Proteção de Dados da União Europeia

A necessidade de, mesmo em um ambiente de mudanças desafiadoras, tornar efetiva a proteção de dados e de garantir a

harmonização legislativa entre os Estados-Membros suscitou a revisão das regras de proteção de dados pessoais na União Europeia. Como resultado, o parlamento europeu e o Conselho da União Europeia publicaram, em 4 de maio de 2016, o Regulamento Geral de Proteção de Dados, *"General Data Privacy Regulation"* - GDPR.

A nova norma, vigente desde o dia 25 de maio de 2018, é aplicável a todas as organizações europeias e suas filiais e subsidiárias (inclusive no Brasil), assim como às organizações sediadas fora da União Europeia, mas que que exportam produtos ou serviços para o grupo econômico, que realizem processamento de dados pessoais de titulares residentes em território europeu, independentemente de sua nacionalidade. Assim, tal norma demanda a preocupação de virtualmente todas as grandes empresas do mundo e da maioria das empresas em geral.

Veja-se, a esse respeito, alguns "Considerandos" do REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016, a GDPR, que falam por si:

> (5) A integração económica e social resultante do funcionamento do mercado interno provocou um aumento significativo dos fluxos transfronteiriços de dados pessoais. O intercâmbio de dados entre intervenientes públicos e privados, incluindo as pessoas singulares, as associações e as empresas, intensificou-se na União Europeia. As autoridades nacionais dos Estados-Membros são chamadas, por força do direito da União, a colaborar e a trocar dados pessoais entre si, a fim de poderem desempenhar as suas funções ou executar funções por conta de uma autoridade de outro Estado-Membro.
>
> (...)
>
> (73) O direito da União ou dos Estados-Membros podem impor restrições relativas a princípios específicos e aos direitos de informação, acesso e retificação ou apagamento de dados pessoais e ao direito à portabilidade dos dados, ao direito de oposição, às decisões baseadas na definição de perfis, bem como à comunicação de uma violação de dados pessoais ao titular dos dados, e a determinadas obrigações conexas dos responsáveis pelo tratamento, na medida em que sejam necessárias e proporcionadas numa sociedade democrática para garantir a segurança pública, incluindo a proteção da vida humana, especialmente em resposta a catástrofes naturais ou provocadas pelo homem, para a prevenção, a investigação e a repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública ou violações da deontologia de profissões regulamentadas, para outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, para a conservação de registos públicos por motivos de interesse público geral, para posterior tratamento de dados pessoais arquivados para a prestação de informações específicas relacionadas com o comportamento político no âmbito de antigos regimes totalitários ou para efeitos de defesa do titular dos dados ou dos direitos e liberdades de terceiros, incluindo a proteção social, a saúde pública e os fins humanitários. Essas restrições deverão respeitar as exigências estabelecidas na Carta e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (...)
>
> (103) A Comissão pode decidir, com efeitos no conjunto da União, que um país terceiro, um território ou um setor determinado de um país terceiro, ou uma organização internacional, oferece um nível adequado de proteção de dados

adequado, garantindo assim a segurança jurídica e a uniformidade ao nível da União relativamente ao país terceiro ou à organização internacional que seja considerado apto a assegurar tal nível de proteção. Nestes casos, podem realizar-se transferências de dados pessoais para esse país ou organização internacional sem que para tal seja necessária mais nenhuma autorização. A Comissão pode igualmente decidir, após enviar ao país terceiro ou organização internacional uma notificação e uma declaração completa dos motivos, revogar essa decisão.

(...)

(107) A Comissão pode reconhecer que um país terceiro, um território ou um setor específico de um país terceiro, ou uma organização internacional, deixou de assegurar um nível adequado de proteção de dados. Por conseguinte, deverá ser proibida a transferência de dados pessoais para esse país terceiro ou organização internacional, a menos que sejam cumpridos os requisitos constantes do presente regulamento relativos a transferências sujeitas a garantias adequadas, incluindo regras vinculativas aplicáveis às empresas, e derrogações para situações específicas. Nesse caso, deverão ser tomadas medidas que visem uma consulta entre a Comissão e esse país terceiro ou organização internacional. A Comissão deverá, em tempo útil, informar o país terceiro ou a organização internacional das razões da proibição e iniciar consultas com o país ou organização em causa, a fim de corrigir a situação.

De fato, como antecipado nos seus Considerandos, a União Europeia adotou, na GDPR, uma abordagem principiológica, transnacional e criadora de responsabilidade das pessoas e entidades pela organização de sistemas de controle do tratamento de dados pessoais.

Segundo o artigo 4º do Regulamento, dados pessoais são qualquer *"informação relativa a uma pessoa singular identificada ou identificável (titular dos dados)"*, sendo que, *"é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular"*.

Estabelecido esse conceito, o tratamento de qualquer dado relativo a uma pessoa física (dados relativos à saúde, biométricos, genéticos, profissionais, familiares, entre outras), seja por qualquer forma de suporte (áudio, vídeo, foto, texto), está sujeito à GDPR.

Tratamento, por sua vez, segundo o regulamento é *"uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição"*.

Na prática, qualquer utilização de dado pessoal de cidadão europeu por parte de qualquer organização atrairá a aplicação da GDPR.

Para que seja lícito, o tratamento de dados pessoais, segundo a GDPR, deverá atender a alguns requisitos (artigo 6º), sendo a maioria destes relativos ao consentimento do sujeito titular das informações tratadas.

Existe certo ceticismo entre os especialistas sobre a efetiva tutela dos indivíduos, que, de acordo com a GDPR, se concretizaria pelo simples fato de estes darem o seu consentimento.

Isso porque, um número considerável de estudos sugere que os avisos de privacidade quase nunca são lidos e o consentimento é quase sempre concedido[14]. Segundo Philipp Hacker, *"in the current state of the digital economy, consent is ubiquitous, and its consequences are rarely understood15".*

Não concordamos com esse ponto de vista, que retira das pessoas a responsabilidade pelos seus próprios atos, protegendo-as delas mesmas com base na visão de terceiros sobre o que pensam ou devem pensar. De qualquer modo, essa preocupação deve ser elemento a fundamentar a garantia da maior transparência possível no que se refere a quais informações pessoais serão obtidas e o que será feito com elas.

Independentemente da eficácia ou não da tutela pretendida com o novo regulamento, certo é que esse impõe às organizações inúmeras regras de conduta que deverão ser adotadas, sob pena de aplicação de severas sanções, bem como traz uma série de direitos aos sujeitos titulares dos dados pessoais, em seu capítulo III (artigos 12 ao 23).

Dentre esses direitos, está o direito de acesso, segundo o qual o titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar aos seus dados pessoais e às seguintes informações: *a) As finalidades do tratamento dos dados; b) As categorias dos dados pessoais em questão; c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais,* dentre outras.

Destacam-se também, o direito ao apagamento dos dados ("*direito a ser esquecido*"), o direito à limitação do tratamento dos dados, o direito de portabilidade dos dados, segundo o qual o titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, em um formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir e o direito de oposição ao tratamento de dados.

É, por fim, interessante ressaltar o direito de retificação, segundo o qual *o* titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, inclusive por meio de uma declaração adicional.

A GDPR determina, ainda, que as organizações, públicas e privadas devem nomear um encarregado de proteção de dados (artigo 37), que pode ser um funcionário da entidade, um representante para um grupo de organizações ou um consultor externo.

Esta nomeação é obrigatória para as autoridades e organismos públicos (exceto tribunais no exercício de sua função jurisdicional), e para as entidades privadas que atendam pelo menos uma das seguintes condições: (i) suas atividades principais consistam em processamento de dados que necessitam de monitorização regular e sistemática dos indivíduos em larga escala; (ii) suas atividades principais consistam

14 Hacker, Philipp. Personal data, exploitative contracts, and algorithmic fairness: autonomous vehicles meet the internet of things. *International Data Privacy Law*, Volume 7, Issue 4, 1 November 2017, Pages 266–286. Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3007780. Acesso em 18 de maio de 2018.

15 *Idem.*

em tratamento em larga escala de dados de categorias especiais, definidos no artigo 9 da GDPR, como raça ou etnia, dados de saúde, dados genéticos ou biométricos, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, orientação sexual e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º[16].

A necessidade de indicação de um responsável pelas atividades elencadas na GDPR é uma espécie de expansão da lógica das atividades reguladas, como o mercado financeiro e de seguros.

Nesse contexto, tal qual normalmente ocorre em atividades reguladas, o encarregado da proteção de dados deve ser designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções descritas no regulamento[17].

Cada Estado-membro terá ainda uma autoridade de controle, que terá, entre outras, as seguintes atribuições: (i) controlar e executar a aplicação do GDPR; (ii) aconselhar, em conformidade com o direito do Estado-Membro, o Parlamento nacional, o Governo e outras instituições e organismos a respeito das medidas legislativas e administrativas relacionadas com a defesa dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento; (iii) promover a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos do regulamento; (iv) se lhe for solicitado, prestar informações a qualquer titular de dados sobre o exercício dos seus direitos e, se necessário, cooperar com as autoridades de controle de outros Estados-Membros para esse efeito; (v) tratar as reclamações apresentadas por qualquer titular de dados, ou organismo, organização ou associação, e investigar, na medida do necessário, o conteúdo da reclamação e informar o autor da reclamação do andamento e do resultado da investigação num prazo razoável, em especial se forem necessárias operações de investigação ou de coordenação complementares com outra autoridade de controlo; (vi) conduzir investigações sobre a aplicação do regulamento, inclusive com base em informações recebidas de outra autoridade de controle ou outra autoridade pública; (vi) acompanhar fatos novos relevantes, na medida em que tenham incidência na proteção de dados pessoais, como, notadamente a evolução a nível das tecnologias da informação

16 Artigo 10º: Tratamento de dados pessoais relacionados com condenações penais e infrações: O tratamento de dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas com base no artigo 6.o, n.o 1, só é efetuado sob o controle de uma autoridade pública ou se o tratamento for autorizado por disposições do direito da União ou de um Estado-Membro que prevejam garantias adequadas para os direitos e liberdades dos titulares dos dados. Os registos completos das condenações penais só são conservados sob o controle das autoridades públicas.

17 Artigo 39: Funções do encarregado da proteção de dados
1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções:
a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;
b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;
c) Presta aconselhamento, quando tal lhe for solicitado, no que refere à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35.o;
d) Coopera com a autoridade de controle;
e) Ponto de contato para a autoridade de controle sobre questões relacionadas ao tratamento, incluindo a consulta prévia a que se refere o artigo 36.o, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.
2. No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

e das comunicações e das práticas comerciais; (vii) se necessário, proceder a uma revisão periódica das certificações emitidas[18]; (viii) conservar registros internos de violações do presente regulamento e das medidas tomadas; (ix) desempenhar quaisquer outras tarefas relacionadas com a proteção de dados pessoais.

Interessante notar que a necessidade da existência de uma autoridade de controle pode ser vista como, para além da governança que isso envolve no que se refere a cada país, a consequência da estrutura particular da União Europeia.

As autoridades de controle disporão também de poderes de investigação e (i) poderão exigir que as organizações públicas ou privadas responsáveis pelo tratamento de dados lhe forneçam informações; (ii) realizarão investigações sob a forma de auditorias sobre a proteção de dados; (iii) notificarão o responsável pelo tratamento ou o subcontratante de alegadas violações do regulamento; (iv) terão acesso a todas as instalações do responsável pelo tratamento e do subcontratante, incluindo os equipamentos e meios de tratamento de dados, em conformidade com o direito processual da União ou dos Estados-Membros.

Além disso, as mencionadas autoridades de controle poderão (i) aplicar advertências ao responsável pelo tratamento de dados; (ii) fazer repreensões ao responsável pelo tratamento ou ao subcontratante sempre que as operações de tratamento tiverem violado as disposições do regulamento; (iii) ordenar ao responsável pelo tratamento ou ao subcontratante que satisfaça os pedidos de exercício de direitos apresentados pelo titular dos dados nos termos do regulamento; (iv) impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição; (v) ordenar a retificação ou o apagamento de dados pessoais ou a limitação do tratamento, bem como a notificação dessas medidas aos destinatários a quem tenham sido divulgados os dados pessoais; (vi) retirar a certificação ou ordenar ao organismo de certificação que retire uma certificação emitida, ou ordenar ao organismo de certificação que não emita uma certificação se os requisitos de certificação não estiverem ou deixarem de estar cumpridos.

Ademais das sanções administrativas, poderão ser impostas às organizações que descumprirem o regulamento sanções pecuniárias, que podem variar de € 10 milhões a € 20 milhões ou de 2% a 4% do faturamento anual da empresa.

De fato, o novo regulamento impõe uma mudança cultural nas organizações que tratam dados pessoais, inclusive no Brasil.

Isso porque, todo o canal de suprimento das organizações, desde a forma como a informação é recolhida, até seu armazenamento e eventual transferência para organizações terceirizadas ou até mesmo transferências internas, internacionais ou não, deverá estar preparado para aplicar as normas da GDPR, sabendo inclusive reconhecer os problemas que o tratamento indevido dos dados pode gerar, tanto para a própria organização quanto para o titular dos dados.

E isso deverá ocorrer em organizações do mundo todo, pois, como já dito, a abrangência territorial do regulamento é extremamente ampla, uma vez que é aplicado (i) ao tratamento de dados pessoais efetuado no contexto das atividades de organizações situadas no território da União

18 Artigo 42, 1: Os Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem, em especial ao nível da União, a criação de procedimentos certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o presente regulamento. Serão tidas em conta as necessidades específicas das micro, pequenas e médias empresas;

Europeia, independentemente de o tratamento ocorrer dentro ou fora da Europa; e (ii) ao tratamento de dados pessoais de titulares residentes no território europeu, realizado por organizações não estabelecidas na União Europeia e que ofertem bens ou serviços a esses titulares, independente da exigência de pagamento.

Pensemos, por exemplo, nos brasileiros que possuem dupla cidadania e são cidadãos brasileiros e europeus ao mesmo tempo. Esses indivíduos, ao se hospedarem em hotéis no Brasil ou ao adquirirem cartões fidelidade de varejistas, também em território brasileiro, estão fornecendo dados de cidadãos europeus a empresas brasileiras, que não necessariamente tenham relação com a União Europeia. Nesses casos, a GDPR deverá ser cumprida por essas organizações, sob pena de serem aplicadas as sanções previstas na norma.

Ou ainda, quaisquer empresas multinacionais que atuem no Brasil e que possuam em sua base dados de milhares de segurados, de diversas nacionalidades, incluindo europeus, foram afetadas diretamente pela GDPR.

IV. O "Cloud Act" Norte Americano

Paralelamente à entrada em vigor da GDPR, foi aprovada nos Estados Unidos o "*Clarifying Overseas Use of Data (CLOUD) Act*". Trata-se basicamente de uma atualização do Ato de Privacidade de Comunicações Eletrônicas americana (*Eletronic Communications Privacy Act "ECPA"*), de 1986, lei que regulava questões de privacidade e segurança na esfera digital.

Embora sejam contemporâneas, as normas apontam para direções diametralmente opostas: enquanto a regulação da União Europeia busca proporcionar maior segurança e privacidade aos dados pessoais, a lei dos Estados Unidos obriga as organizações americanas a fornecerem dados de seus usuários de forma irrestrita às autoridades americanas.

A origem do "Cloud Act" deu-se seis anos atrás, em 2013, quando o Departamento de Justiça Americano requereu à Microsoft que esta entregasse dados de um de seus consumidores, pois o mesmo estava sendo investigado por atividades ilícitas. O consumidor, no entanto, era um cidadão irlandês, que morava na Irlanda e seus dados estavam armazenados em um servidor também na Irlanda[19].

A empresa negou-se a cumprir a ordem e recorreu à Suprema Corte dos Estados Unidos, que, em 2016, invalidou o mandado do Departamento de Justiça, sob o argumento de que o "ECPA" não exigia o fornecimento de dados armazenados em território externo, às autoridades americanas.

Em 2017, o Departamento de Justiça americano pediu a revisão do caso na Suprema Corte, ocasião em que os Ministros sugeriram que a lei deveria ser revista no Congresso. No ano seguinte, foi então aprovado o "*CLOUD Act*".

Com a aprovação da Lei, autoridades americanas podem forçar organizações americanas a fornecerem dados de seus usuários, independentemente do país em que essas informações estejam armazenadas. Além disso, a nova lei também oferece a possibilidade de o poder executivo dos Estados Unidos celebrar acordos com países estrangeiros, com o objetivo

19 The CLOUD Act Is Up For Vote and What It Means For Consumers. Forbes. Disponível em < https://www.forbes.com/sites/stevepociask/2018/03/22/the-cloud-act-is-up-for-vote-and-what-it-means-for-consumers/#2a7150a92ccf>. Acesso em 04 de junho de 2018.

de adquirir informações, sem que haja a necessidade de aprovação do Senado americano.

Os países que realizarem tal acordo poderão obter dados diretamente de companhias americanas, desde que esses dados não pertençam a um cidadão americano ou residente americano.

Antes da aprovação da lei, os Estados Unidos podiam ter acesso aos dados requeridos apenas por meio de tratados de assistência mútua, chamados de "*mutual legal-assistance treaties (MLAT's)",* que permitiam que dois ou mais países negociassem os termos exatos dessa troca de informações no âmbito de investigações criminais. Esses tratados, embora nem sempre muito eficazes, respeitavam as leis de proteção de dados dos países envolvidos, inclusive do país em que os dados eram armazenados.

O Brasil celebrou o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, promulgado por meio do decreto nº 2.810 de 2001[20]. No entanto, segundo o Ofício nº 965/2018 expedido pelo Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, *"em relação aos casos que envolvem pedidos de cooperação jurídica voltados à obtenção de dados e quebra de sigilo telemático nos EUA, a utilização do MLAT não vem apresentando resultados satisfatórios, seja quanto ao índice de pedidos cumpridos, seja em relação ao tempo para as respostas positivas, causadas na maior parte por conta das limitações da lei norte-americana Stored Communication Act (...)21".*

O Tratado brasileiro é, inclusive, objeto de Ação Declaratória de Constitucionalidade em trâmite no Supremo Tribunal Federal (ADC nº 51)[22], proposta pela Federação das Associações das Empresas de Tecnologia da Informação. O pedido é que a constitucionalidade da norma de cooperação jurídica internacional entre autoridades judiciárias brasileiras e estrangeiras seja declarada, para que os tribunais brasileiros apliquem o *Mutual Legal Assistance Treaty - MLAT.*

Agora, porém, com o *CLOUD Act,* um governo estrangeiro, como o brasileiro, por exemplo, pode requerer à uma companhia americana dados sob sua guarda, desde que não pertençam a um cidadão americano e nem a um residente americano, sem necessidade de cumprir leis americanas sobre proteção de dados.

Por outro lado, qualquer governo estrangeiro poderá obter, sem restrições, informações sobre cidadãos brasileiros, ao realizar o mencionado acordo executivo com o governo americano. Nesse cenário, ainda que o Brasil venha a ter uma lei sobre proteção de dados, esta não será respeitada, restando, inclusive, esvaziada a questão central da ADI nº 51.

Além disso, os "acordos executivos" para fornecimento de dados podem se tornar ferramentas políticas, de modo que o governo americano não recusará conceder informações para países cujos governos não respeitem os direitos humanos e liberdades civis, por exemplo, para evitar desgaste com um governo que possa vir a ser seu aliado político[23].

Diferentemente da GDPR, o *CLOUD Act* considera o direito à segurança, permanentemente, superior ao direito à privacidade e à proteção de dados pessoais. Entidades norte-americanas de proteção à

20 http://www.planalto.gov.br/ccivil_03/decreto/2001/d3810.htm

21 https://www.jota.info/wp-content/uploads/2018/04/stf-ineficacia-do-mlat-ministerio-da-justica.pdf

22 http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379

23 TENNANT, Fraser. The CLOUD Act: law enforcer or global privacy threat? Financier WorldWide, issue 186, june 2018.

privacidade, inclusive, enxergam o *CLOUD Act* como uma grave ameaça aos direitos individuais[24].

V. No Brasil

a) Normas Vigentes

A Constituição Federal prevê em seu artigo 5º, inciso X que *"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"*. Nesse contexto, o direito à proteção e privacidade de dados integraria a vida privada do indivíduo, sendo abrangido, assim, pela tutela constitucional.

Também segundo a Constituição Federal, é inviolável o sigilo de dados e das comunicações, conforme previsão do artigo 5º, inciso XII: *"é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal."*.

A ideia do texto constitucional, ao excetuar a inviolabilidade do sigilo em algumas hipóteses, é que as restrições à privacidade devam sempre ser necessárias e proporcionais, ao atender finalidades como investigações criminais, por exemplo. Algumas decisões do STF[25] caminhavam no sentido de exigir ordem judicial mesmo para a coleta de dados cadastrais — como nome, sobrenome e endereço — de usuários por delegados de polícia e pelo Ministério Público, mas algumas leis mais recentes trataram do tema de forma diferente.

É o caso da Lei das Organizações Criminosas (Lei 12.850/2013) e da Lei 12.683/2012, que alterou a Lei de Lavagem de Dinheiro. Essas normas facultam a autoridades policiais e ao Ministério Público o acesso a dados cadastrais de investigados, independentemente de autorização judicial, perante a Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito[26]. Interpretações extensivas dessas

---

24 https://www.aclu.org/letter/coalition-letter-cloud-act

25 RECURSO EXTRAORDINÁRIO. DIREITO PROCESSUAL PENAL. MANDADO DE SEGURANÇA. INQUÉRITO POLICIAL. REQUISIÇÃO DIRETA DE DADOS CADASTRAIS TELEFÔNICOS PELO DELEGADO DE POLÍCIA FEDERAL. DEBATE SOBRE A NECESSIDADE DE AUTORIZAÇÃO JUDICIAL. PERDA SUPERVENIENTE DE BJETO. ARQUIVAMENTO DO INQUÉRITO A REQUERIMENTO DO PARQUET. PREJUÍZO DO RECURSO EXTRAORDINÁRIO.
Decisão: Trata-se de Recurso Extraordinário interposto com base no art. 102, inc. III, alínea a, da Constituição da República contra acórdão da Oitava Turma do Tribunal Regional Federal da 4ª Região, que negou provimento à apelação da União, mediante os seguintes fundamentos
APELAÇÃO. MANDADO DE SEGURANÇA. PROCESSUAL PENAL. EMPRESA DE TELEFONIA. DADOS CADASTRAIS DE CLIENTES. REQUISIÇÃO. AUTORIDADE POLICIAL. ART. 5º, XII, DA CF. SIGILO. QUEBRA. AUTORIZAÇÃO JUDICIAL. NECESSIDADE.
1. Tem legitimidade para impetrar o mandamus a companhia telefônica que, ao reputar ilegal a ordem emanada pela Polícia Federal, para que forneça dados cadastrais de seus clientes, pretende ver reconhecido perante o Poder Judiciário seu direito líquido e certo de não prestar as informações solicitadas.
2. O sigilo telefônico incide não apenas sobre as comunicações telefônicas propriamente ditas (regulamentada pela Lei nº 9.296/96) mas também sobre os respectivos dados e registros, constituindo projeção específica do direito à privacidade garantido na Lei Maior.
3. Referido direito fundamental não pode ser tido como absoluto, tendo em vista a natural restrição resultante do princípio da convivência das liberdades.
4. Para evitar possíveis abusos por parte dos órgãos estatais, a quebra de sigilo deve ser feita com observância do procedimento legalmente estabelecido, ou seja, mediante autorização judicial devidamente fundamentada, sendo demonstrada a efetiva necessidade da medida restritiva.
5. Portanto, a determinação da autoridade policial para que sejam revelados dados sigilosos afigura-se ilegal, uma vez que a produção das provas pretendidas dependeria da competente autorização judicial."
(STF – RE: 716795, Relator Min. Luiz Fux, Data de Julgamento: 31/10/2012, Data de Publicação: Dje – 6/11/2012).

26 Brasil. Lei 12.850/2013. Art. 15. *O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito.*
Lei 12.683/2012 Art. 17-B. *A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de*

competências têm defendido que elas são aplicáveis a todo tipo de investigação criminal, e não apenas em casos de desmantelamento de organizações criminosas e lavagem de dinheiro.

No caso das empresas de telefonia fixa e móvel, há também o entendimento de que os delegados de polícia e os promotores e procuradores de justiça podem ter acesso, sem autorização judicial, aos registros de identificação dos terminais de origem e de destino das ligações telefônicas, para garantir a eficácia das investigações criminais. Alguns delegados chegam a pedir até a localização dos aparelhos celulares, às empresas de telefonia móvel, sem autorização judicial.

Importante mencionar que a Lei 9.472/1997, que dispõe sobre a organização dos serviços de telecomunicações, tem disposição expressa no sentido de que a privacidade da comunicação é um direito que deve ser garantido ao usuário:

> *Art. 3° O usuário de serviços de telecomunicações tem direito:*
>
> *(...)*
>
> *V - à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucional e legalmente previstas;*
>
> *(...)*
>
> *IX - ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço;*

Nesse cenário, o alcance dos dados a que as autoridades públicas podem ter acesso é bastante controvertido, e, inclusive está sendo questionado na Ação Direta de Inconstitucionalidade 5063, que aguarda julgamento no Supremo Tribunal Federal desde 2013.

O Código de Defesa do Consumidor (Lei 8.078/90) possui disposições sobre os dados dos consumidores. Em seu artigo 43, trata da questão do acesso do consumidor aos seus dados pessoais que estejam arquivados: "o *consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes*", além de prever que, sempre que encontrar inexatidão nos seus dados e cadastros, o consumidor poderá exigir sua imediata correção.

Essa talvez tenha sido a primeira regra mais específica tratando da utilização de dados pessoais por entidades brasileiras, embora tenha alcance, aos olhos do intérprete atual, bastante limitado. Não trata, por exemplo, do consentimento para a obtenção, gerenciamento e uso dos dados pessoais, limitando-se a garantir, o consumidor, acesso aos dados a ele referentes. Ademais, tal regra tem a sua aplicabilidade limitada às relações de consumo, embora o conceito de consumidor venha sendo repetidamente ampliado pelos nossos Tribunais.

Já o direito de acesso às informações mantidas pelo Estado a seu respeito pode ser garantido pelo *habeas data,* previsto no artigo 5º, inciso LXXII da Constituição Federal. O mencionado inciso preceitua que, para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, e para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo, o instrumento processual adequado será o *habeas data.*

Esse instrumento constitucional, porém, ao protagonizar importante precedente no Supremo Tribunal Federal, teve seu

autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.

uso restringido. Em um *habeas data*[27], o STF definiu que tal ação constitucional presta-se a três funções: acesso a registros públicos, retificação desses registros e complementação deles.

Diante disso, foi consolidada a limitação do uso do instrumento. No entendimento do agora Ministro Luis Roberto Barroso, o remédio constitucional passou a ter "valia essencialmente simbólica" , como afirmado [28], 20 anos atrás.

No caso da internet, a proteção aos dados dos usuários é um pouco maior desde a promulgação do Marco Civil da Internet (Lei 12.965/2014). A referida lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e impõe que a proteção da privacidade e dos dados pessoais, na forma da lei[29], seja princípio norteador do uso da internet no Brasil.

Além disso, a Lei estabeleceu que é assegurado ao usuário da internet o direito, entre outros, (i) à inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; (ii) à inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; (iii) à inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; (iv) ao não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; (v) à informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: (a) justifiquem sua coleta; (b) não sejam vedadas pela legislação; e (c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; (vi) ao consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; e (vii) à exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei.

Interessante notar que, no momento em que essa lei foi editada, quando passamos a ter alguns dispositivos isolados tratando da proteção à privacidade, no caso da Europa, já havia uma lei que tratava dos dados pessoais e direito à privacidade, a qual foi substituída por uma outra, mais adaptada à modernização das comunicações e dos métodos de gerenciamento de informações pessoais.

A Lei também estabeleceu alguns conceitos, mas a definição de dados pessoais foi dada posteriormente, pelo Decreto 8.771/2016, que regulamentou o Marco Civil da Internet, como "*dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa*". Essa conceituação é bastante abrangente e similar à da regulação europeia, e coloca sob proteção, por exemplo,

---

27 RE 742701, Relator(a): Min. CELSO DE MELLO, julgado em 11/06/2013, publicado em PROCESSO ELETRÔNICO DJe-115 DIVULG 17/06/2013 PUBLIC 18/06/2013.

28 http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/viewFile/47206/45406

29 Art. 3o A disciplina do uso da internet no Brasil tem os seguintes princípios:
I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;
IV - preservação e garantia da neutralidade de rede;
V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
VII - preservação da natureza participativa da rede;
VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

dados gerados pela navegação que, embora não sejam propriamente conteúdo de comunicação, permitem uma identificação das pessoas. É o caso de data e hora da navegação e localização do terminal de acesso, por exemplo.

O Decreto também estabeleceu, em seu artigo 10, que autoridades administrativas competentes poderão, independente de autorização judicial, obter apenas dados de filiação (nome dos pais), endereço, e a qualificação pessoal do usuário (nome, prenome, estado civil e profissão), quando as organizações privadas tiverem essas informações.

O Marco Civil da Internet, dispôs ainda, de forma genérica, sobre a proteção aos dados pessoais:

> *Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.*
>
> *Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.*
>
> *Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:*
>
> *I - advertência, com indicação de prazo para adoção de medidas corretivas;*
>
> *II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;*
>
> *III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou*
>
> *IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.*
>
> *Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o* caput sua filial, sucursal, escritório ou estabelecimento situado no País.

Os dispositivos mencionados, entretanto, não são suficientes para garantir a proteção de dados pessoais, pois tratam de forma generalista as obrigações em relação a estes, limitando-se a estabelecer que sua coleta, armazenamento, guarda, disponibilização e tratamento, deverão atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

Ademais, na linha das normas legais que regulamenta, o foco da referida norma não são os dados pessoais em si, mas sim os dados que sejam obtidos no âmbito de *registros de conexão e de acesso a aplicações de internet.*

Em 2013, estrou em vigor a Lei nº Lei nº 12.737/2012, conhecida como lei dos delitos cibernéticos, que acrescentou os artigos 154-A e 154-B ao código penal brasileiro, tipificando a conduta de "*invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".*

A referida lei representou um avanço bastante significativo na legislação penal e representou uma inovação no ordenamento jurídico brasileiro. No entanto, a sua natureza penal, estritamente associada, portanto, a atos dolosos, estabelece âmbito muito mais restrito do que uma norma que trate diretamente das formas legítimas de obtenção, gerenciamento e tratamento de dados pessoais e, geram e no âmbito da internet e mesmo de "dispositivos informáticos", expressão que pode eventualmente ser interpretada de forma mais restrita do que "dispositivo eletrônico", excluindo do seu âmbito de aplicação dispositivos como os *smartphones*, por exemplo.

Já no que se refere ao setor financeiro brasileiro, há uma preocupação maior e histórica com a proteção de dados. A Lei Complementar nº. 105/2001, por exemplo, ainda que não disponha especificamente sobre a proteção de dados pessoais, dispõe sobre o sigilo bancário e está vigente desde 2001.

Talvez a eficácia desta Lei seja atribuível à excelência operacional das instituições financeiras e ao respeito, pelas instituições brasileiras em geral, ao Banco Central do Brasil e ao papel que exerce relativamente ao Sistema Financeiro Nacional em geral e às instituições financeiras em especial.

A Lei Complementar, de qualquer modo, foi antecedida, no que se refere ao sigilo bancário, da Lei nº 7.492/1986, a qual define os crimes contra o sistema financeiro nacional e estabelece, em seu artigo 18, que a violação do sigilo de uma operação ou serviço oferecido por uma instituição financeira sujeita o agente à pena de prisão de um a quatro anos e multa, exceto se as informações forem exigidas por autoridades policiais e membros do Ministério Público.

Importante comentar ainda a Lei 12.683 de 2012, que alterou a lei de lavagem de dinheiro, especifica que o setor financeiro deve: (i) identificar seus clientes e manter registros atualizados sobre eles; (ii) manter um registro de todas as transações financeiras que ultrapassem o limite permitido; (iii) responder corretamente a todas as solicitações feitas pelo COAF (o Conselho Brasileiro de Controle de Atividades Financeiras) ou um outro regulador adequado, de maneira que este conselho seja responsável por manter o sigilo sobre as respostas enviadas; (iv) prestar atenção especial a qualquer transação que evidencie seriamente a constituição de crime, comunicando o fato, em segredo, ao COAF no prazo de 24 horas; sob pena de, nos termos do artigo 12 da lei, serem aplicadas as sanções de advertência, multa pecuniária, cassação ou suspensão da autorização para o exercício de atividade, operação ou funcionamento.

Mais uma vez, temos uma lei que se refere à coleta de dados pessoais mas que pretende regular um aspecto específico de sua utilização. No caso, o objetivo é tratar dos controles para a prevenção da lavagem de dinheiro.

De qualquer modo, considerando a quantidade e a sensibilidade das informações coletadas e gerenciadas por seus membros, em abril de 2016 a Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA[30], publicou um guia de segurança cibernética[31] sugerindo práticas para garantir a segurança de dados de seus associados (bancos, gestoras, corretoras, distribuidoras e administradoras), em razão do aumento de incidentes de segurança cibernética no Brasil.

Pouco tempo depois, em julho de 2017, a Comissão de Valores Mobiliários , entidade vinculada ao Ministério da Fazenda e

30 http://www.anbima.com.br/pt_br/institucional/a-anbima/posicionamento.htm

31 http://www.anbima.com.br/data/files/60/01/28/F8/1593E5106D60FCD5A8A80AC2/ANBIMA%20DEBATE%20CYBERSECURITY%2031082017.pdf

criada com o objetivo de fiscalizar, normatizar, disciplinar e desenvolver o mercado de valores mobiliários no Brasil[32], publicou um estudo sobre a "Percepção de riscos cibernéticos nas atividades de administradores fiduciários e intermediários". Nesse estudo, foram apresentados os *"resultados de um questionário conduzido com alguns participantes do mercado de capitais brasileiro, com o objetivo de se obter, de forma exploratória, a percepção dos jurisdicionados da CVM em relação a riscos cibernéticos em suas atividades, bem como alguns contornos das práticas vigentes de gerenciamento de riscos cibernéticos.33".*

Por sua vez, em abril de 2018, o Banco Central publicou a Resolução nº. 4.658/2018, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

A norma se divide em duas partes principais: (i) uma que trata da política de segurança cibernética, subdividida em implementação, divulgação e plano de ação e resposta a incidentes; e (ii) outra que dispõe sobre a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

No tocante à política de segurança cibernética, esta deve ser adequada a fatores como porte e modelo de negócio da instituição, natureza das operações, complexidade dos produtos e a sensibilidade dos dados em questão. Em linhas gerais, a política deverá estabelecer como um de seus objetivos a capacidade de a instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados ao ambiente cibernético.

A Resolução ainda prevê a necessidade de divulgação ao público de um resumo contendo as linhas gerais da política de segurança cibernética.

A norma exige também a instituição de um plano de ação e resposta a incidentes. Este deve disciplinar as medidas a serem desenvolvidas pelas instituições financeiras para se adequarem aos princípios e diretrizes da política de segurança cibernética, além de abranger as rotinas, procedimentos, controles e tecnologias destinados à prevenção e resposta a incidentes.

Note-se, no que se refere a tal norma, o objetivo foi tratar de aspectos operacionais das instituições que atuam sob a supervisão do Banco Central do Brasil e não da relação entre tais entidades e seus clientes.

Nesse aspecto, de forma similar à regulação europeia e a entidades atuantes em mercados tipicamente regulados, o artigo 7º da Resolução exige que as instituições financeiras designem diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes, que poderá exercer outras funções, desde que não haja conflito de interesses.

O artigo 11º da Resolução dispõe que as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, devem assegurar que suas políticas, estratégias e estruturas para gerenciamento de riscos, especificamente no tocante aos critérios de decisão quanto à terceirização de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País ou no exterior. A instituição

32 http://www.cvm.gov.br/menu/acesso_informacao/institucional/sobre/cvm.html

33 http://www.cvm.gov.br/export/sites/cvm/menu/acesso_informacao/serieshistoricas/estudos/anexos/Percepcao_de_riscos_ciberneticos_nas_atividades_de_administradores_fiduciarios_e_intermediarios.pdf

contratante será responsável pela confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos serviços contratados.

A contratação desses serviços deverá ser comunicada ao Banco Central com antecedência mínima de sessenta dias da efetiva contratação. Para casos de contratação no exterior, devem ser observados os seguintes requisitos: (i) existência de convênio para troca de informações entre o Banco Central e as autoridades supervisoras dos países onde os serviços poderão ser prestados (ou, inexistindo convênio, solicitar autorização do Banco Central); (ii) a instituição contratante deve assegurar que a prestação dos serviços não causará prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central; (iii) a instituição deve definir previamente os países e regiões onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e (iv) a instituição contratante deve prever alternativas para a continuidade dos negócios no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

De fato, a Resolução 4.658/2018 do Banco Central pode ser considerada um avanço na proteção de dados no Brasil, mas se limita a tratar de aspectos operacionais das instituições financeiras e não tem como foco as relações delas com os seus clientes.

b) Responsabilidade em caso de tratamento e uso inadequados de dados pessoais.

Ainda que não tenha uma legislação específica no Brasil sobre privacidade de dados, as organizações públicas e privadas possuem responsabilidade sobre eventuais danos causados a terceiros cujos dados pessoais estejam sob sua guarda.

Face a ausência de um órgão regulador e fiscalizador próprio, o Ministério Público tem assumido papel central nessa questão, atuando em prol da tutela da privacidade, intimidade e de dados dos consumidores.

No início deste ano de 2018, por exemplo, o Ministério Público Federal propôs ação em face da Microsoft para impedir que seu sistema operacional, o Windows 10, continue coletando dados pessoais sem autorização dos usuários. Segundo os procuradores de justiça, atualmente, a opção padrão de instalação e atualização do Windows 10 permite que a empresa obtenha diversas informações sobre os consumidores, como geolocalização, conteúdo de emails, hábitos de navegação e histórico de buscas na internet[34].

Como já mencionado, ainda que insuficiente, o Marco Civil da Internet possui previsão de que, caso ocorra operação de coleta, armazenamento, guarda e tratamento de registros de dados pessoais em território nacional, que não respeitem os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, sem prejuízo de demais sanções cíveis, criminais ou administrativas, serão aplicadas sanções de (i) advertência, com indicação de prazo para adoção de medidas corretivas; (ii) multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; (iii) suspensão temporária das atividades mencionadas; e/ou (iv) proibição de exercício dessas atividades.

Interessante notar, contudo, que o Marco Civil da Internet traz uma exclusão de

34 https://tecnologia.uol.com.br/noticias/reuters/2018/04/26/ministerio-publico-processa-microsoft-por-coleta-de-dados-no-windows-10.htm

responsabilidade de intermediários por danos decorrentes de conteúdo gerado por terceiros. Vejamos:

> *Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.*
>
> *Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.*

O assunto foi tratado no Recurso Especial nº 1.306.157-SP, interposto pelo Google Brasil[35]. Ainda que a matéria impugnada no recurso tenha se restringido à obrigação de retirar o conteúdo da internet no prazo de 24 horas, sob pena de multa, em sede de tutela antecipada, o Ministro Relator Luís Felipe Salomão expôs sua opinião de que conteúdos ofensivos, como por exemplo discurso de ódio e mensagens racistas e difamantes não são abarcados pela proteção da liberdade de expressão, de modo que sua publicação acarretaria a responsabilidade civil do intermediador.

Segundo o Ministro, *"no caso de sites de hospedagem de vídeos, eventuais ofensas à honra de pessoas não podem ser consideradas atos exclusivamente praticados por terceiros (usuários)*. Além disso, entendeu também o Ministro que "*não há como afirmar acertadamente que, por exemplo, o discurso de ódio, mensagens racistas e difamantes, pornografia infantil, anúncios servis a tráfico de entorpecentes - como os que noticiam a imprensa brasileira existirem em rede social da ora recorrente - possam fazer parte do âmbito normativo de proteção da liberdade de manifestação do pensamento".*

VI. Da Lei Geral de Proteção de Dados Pessoais – LGPD

A edição da Lei nº 13.709/2018, nossa Lei Geral de Proteção de Dados Pessoais – LGPD , deu-se com base nos precedentes e fundamentos acima expostos.

A compreensão desse fato é fundamental para que se interprete e aplique a LGPD de forma correta e em consonância com seus objetivos.

Na segunda parte desse estudo, discutiremos especificamente a LGPD e suas regras.

35 Direito civil. Obrigação de fazer e não fazer. Vídeos divulgados em site de compartilhamento (youtube). Contratação a envolver a marca e material publicitário dos autores. Ofensa à imagem e ao nome das partes. Dever de retirada. Indicação de URL's. Desnecessidade. Individualização precisa do conteúdo do vídeo e do nome a ele atribuído. Multa. Reforma. Prazo para a retirada dos vídeos (24 h). Manutenção.
REsp nº 1.306.157 - SP (2011/0231550-1). Relator Ministro Luis Felipe Salomão, publicado 24/03/2014.

Previdência Privada:
as entidades do "Sistema S" e a paridade contributiva

PAULO SOGAYAR

SOGAYAR
SOCIEDADE DE ADVOGADOS

I – Introdução

Recentemente muito se tem falado em cortar recursos do "Sistema S", que considera entidades como Senai, Sesi e Sesc. Por não haver um conceito legal específico, a doutrina considera que tais entidades são integrantes do denominado "Terceiro Setor" e classificadas como "serviços sociais autônomos".

Ocorre que algumas dessas entidades oferecem planos de previdência privada e podem existir planos deficitários.

Se eventualmente o governo decidir cortar recursos do "Sistema S", rogamos para que não faltem recursos com os quais tais entidades possam honrar seus compromissos perante os planos de previdência privada, de modo a não onerar ainda mais os participantes e assistidos.

O presente traz à lume argumentos no sentido de demonstrar que tais entidades não estão sujeitas à paridade contributiva prevista no §3º do artigo 202[1] da Constituição Federal (CF), conforme redação da

1 "§ 3º É vedado o aporte de recursos a entidade de previdência privada pela União, Estados, Distrito Federal e Municípios, suas autarquias, fundações, empresas públicas, sociedades de economia mista e outras entidades públicas, salvo na qualidade de patrocinador, situação na qual, em hipótese alguma, sua contribuição normal poderá exceder a do segurado."

Emenda Constitucional 20 de 1998 (EC 20/98), ponderando que é a Lei Complementar 108/01 (LC 108/01) que disciplina a relação entre a União, Estados, Distrito Federal ou Municípios, inclusive suas autarquias, fundações, sociedades de economia mista e empresas controladas direta ou indiretamente, enquanto patrocinadoras de entidades fechadas de previdência complementar (EFPC), e suas respectivas EFPC.

Conforme o artigo 27 da LC 108/01, as EFPC patrocinadas por entidades públicas, inclusive empresas públicas e sociedades de economia mista, deveriam ter revisto, no prazo de dois anos, a contar de 16 de dezembro de 1998, seus planos de benefícios e serviços, de modo a ajustá-los atuarialmente a seus ativos, sob pena de intervenção, sendo seus dirigentes e seus respectivos patrocinadores responsáveis civil e criminalmente pelo descumprimento do disposto em tal artigo.

Já se passaram mais de 18 anos e ainda não há uma posição do Supremo Tribunal Federal (STF) sobre se as entidades do "Sistema S" estão enquadradas na expressão "outras entidades públicas", nos termos do §3º do artigo 202 da CF.

Aqueles que defendem que as entidades do "Sistema S" estão enquadradas na expressão "outras entidades públicas" e a elas deveria ser aplicada a regra da paridade contributiva, consideram que:

a) tais entidades prestam serviços de interesse público;

b) elas são mantidas, em grande parte, por recursos públicos, conforme artigo 149[2] da CF;

c) o artigo 202 da CF visa controlar gastos públicos; e

d) várias normas do regime jurídico administrativo são aplicáveis às entidades do "Sistema S"[3].

Mas será que tais entidades deveriam ser enquadradas nos termos do §3º do artigo 202 da CF?

II – Interpretação da expressão "outras entidades públicas"

Embora um processo interpretativo possa ter supremacia sobre outros, para determinar o sentido e alcance da norma, os diversos processos interpretativos não se excluem reciprocamente[4], mas se completam, na busca do sentido e alcance da norma, pois o espírito da norma apenas pode ser alcançado ao final do processo de interpretação, com a aplicação de todos os processos interpretativos[5].

Os processos interpretativos são: gramatical, lógico, sistemático, histórico e sociológico ou teleológico[6].

De acordo com o processo gramatical, embora seja atrativo o argumento de que o §3º em tela, ao mencionar explicitamente a "União, Estados, Distrito Federal e municípios, suas autarquias, fundações, empresas públicas e sociedades de economia mista" tenha "esgotado" as figuras da administração pública direta e indireta e, consequentemente, "outras entidades públicas"

2 "Art. 149. Compete exclusivamente à União instituir contribuições sociais, de intervenção no domínio econômico e de interesse das categorias profissionais ou econômicas, como instrumento de sua atuação nas respectivas áreas, observado o disposto nos arts. 146, III, e 150, I e III, e sem prejuízo do previsto no art. 195, § 6º, relativamente às contribuições a que alude o dispositivo. (…)".

3 Nesse sentido, por exemplo: o artigo 70 da Constituição Federal, que determina a prestação de contas ao TCU; Lei 4.711/1965, que regula a Ação Popular; Lei 8.429/1992, que trata da Improbidade Administrativa.

4 Cfr. Diniz, Maria Helena, "Compêndio de Introdução à Ciência do Direito", São Paulo, Saraiva, 1991, p.381.

5 Ascensão, José de Oliveira, "Introdução à Ciência do Direito", Rio-São Paulo-Recife, Renovar, 2005, p.504.

6 Cfr. Diniz, Maria Helena, "Curso de Direito Civil Brasileiro", 1ª vol. Teoria Geral do direito Civil, São Paulo, Saraiva, 1997, ps. 58/60.

se refira a quaisquer outras entidades que, de alguma forma, possam ser consideradas como "públicas", também é possível se interpretar a expressão "outras entidades públicas" como "outras entidades de direito público", excluindo, consequentemente, entidades de direito privado, como as do "Sistema S".

A aludida expressão também poderia ser interpretada como "outras entidades efetivamente públicas que venham a ser criadas".

No processo lógico, considerando que realmente a intenção do legislador na época foi controlar gastos públicos, é bastante convidativo entender que a expressão "outras entidades públicas" seja interpretada de forma ampla, abrangendo todas as entidades que recebem recursos públicos.

As entidades do "Sistema S", por determinação legal, devem aplicar os recursos que recebem com o objetivo de atender a missão para a qual foram instituídas.

As receitas que recebem por força dos artigos 149 e 240[7] da CF (consideradas como contribuição parafiscal) são oriundas de categoria de contribuinte para o próprio benefício do segmento que se pretende fomentar, sendo certo que tais contribuições, em nenhum momento, integram o patrimônio público, não tendo uma destinação orçamentária típica de receita pública, a elas não se aplicando o artigo 165[8] da CF.

Assim, referidas contribuições são receitas privadas e próprias das entidades do "Sistema S", embora elas tenham que prestar contas[9] da aplicação dessas receitas, de forma finalística, ao TCU. Além disso, suas despesas também são de natureza privada.

As entidades do "Sistema S" têm autonomia administrativa e, reitere-se, estão sujeitas apenas ao controle finalístico pelo TCU, o que inclusive já foi reconhecido pelo STF no RE 789.874[10] (jul. 17/09/2014).

No aludido RE, o STF considerou que as entidades do "Sistema S" são patrocinadas "basicamente por recursos recolhidos do próprio setor produtivo beneficiado" e que não integram a administração pública. Na

7 "Art. 240. Ficam ressalvadas do disposto no art. 195 as atuais contribuições compulsórias dos empregadores sobre a folha de salários, destinadas às entidades privadas de serviço social e de formação profissional vinculadas ao sistema sindical."

8 "Art. 165. Leis de iniciativa do Poder Executivo estabelecerão:
I – o plano plurianual; II – as diretrizes orçamentárias; III – os orçamentos anuais. (...)."

9 Cfr. Parágrafo único do artigo 70 da Constituição Federal:
"Art. 70. A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder. Parágrafo único. Prestará contas qualquer pessoa física ou jurídica, pública ou privada, que utilize, arrecade, guarde, gerencie ou administre dinheiros, bens e valores públicos ou pelos quais a União responda, ou que, em nome desta, assuma obrigações de natureza pecuniária."
E do artigo 183 do Decreto-lei 200/67:
"Art. 183. As entidades e organizações em geral, dotadas de personalidade jurídica de direito privado, que recebem contribuições parafiscais e prestam serviços de interesse público ou social, estão sujeitas à fiscalização do Estado nos termos e condições estabelecidas na legislação pertinente a cada uma."

10 "EMENTA: ADMINISTRATIVO E CONSTITUCIONAL. SERVIÇOS SOCIAIS AUTÔNOMOS VINCULADOS A ENTIDADES SINDICAIS. SISTEMA "S". AUTONOMIA ADMINISTRATIVA. RECRUTAMENTO DE PESSOAL. REGIME JURÍDICO DEFINIDO NA LEGISLAÇÃO INSTITUIDORA. SERVIÇO SOCIAL DO TRANSPORTE. NÃO SUBMISSÃO AO PRINCÍPIO DO CONCURSO PÚBLICO (ART. 37, II, DA CF). 1. Os serviços sociais autônomos integrantes do denominado Sistema "S", vinculados a entidades patronais de grau superior e patrocinados basicamente por recursos recolhidos do próprio setor produtivo beneficiado, ostentam natureza de pessoa jurídica de direito privado e não integram a Administração Pública, embora colaborem com ela na execução de atividades de relevante significado social. Tanto a Constituição Federal de 1988, como a correspondente legislação de regência (como a Lei 8.706/93, que criou o Serviço Social do Trabalho – SEST) asseguram autonomia administrativa a essas entidades, sujeitas, formalmente, apenas ao controle finalístico, pelo Tribunal de Contas, da aplicação dos recursos recebidos. Presentes essas características, não estão submetidas à exigência de concurso público para a contratação de pessoal, nos moldes do art. 37, II, da Constituição Federal. Precedente: ADI 1864, Rel. Min. Joaquim Barbosa, DJe de 2/5/2008. 2. Recurso extraordinário a que se nega provimento."

mesma oportunidade, o STF, embora tenha analisado especificamente o Serviço Social do Trabalho – SEST, também entendeu, com base na CF e na legislação de regência, que tais entidades têm autonomia administrativa e estão sujeitas, apenas, ao controle finalístico pelo TCU da aplicação dos recursos recebidos.

Tendo as entidades do "Sistema S" autonomia administrativa, não integrando a administração pública e utilizando-se basicamente de recursos recolhidos do próprio setor produtivo beneficiado, não é lógico que elas sejam incluídas na expressão "outras entidades públicas".

Sob o ponto de vista do processo sistemático, considerando que a expressão "outras entidades públicas" não é mencionada no §4º[11], mas apenas no §3º do artigo 202 da CF, pode-se interpretá-la como substituta da expressão "empresas controladas direta ou indiretamente", adotada no citado §4º

Embora não seja possível se interpretar a Constituição Federal com base em leis, uma lei pode integrar a sua vontade, complementando-a. Essa possibilidade ocorre quando a norma maior permite que o tema seja disciplinado, por exemplo, via lei complementar, exatamente o que determinou o §4º do artigo 202.

Lembramos que a lei complementar que regulamenta os §§ 3º, 4º, 5º e 6º do artigo 202 da CF é a LC 108/01.

Comprovação disso é o seu artigo 1º[12]. Aliás, assim como o §4º do artigo 202 da Constituição Federal nada menciona sobre "outras entidades públicas", o artigo 1º da LC 108/01 é claro em especificar quem seriam os "patrocinadores públicos", a saber: a União, os Estados, o Distrito Federal e os Municípios, inclusive suas autarquias, fundações, sociedades de economia mista e empresas controladas direta ou indiretamente.

Considerando que a LC 108/01 regulamenta os §§3º, 4º, 5º e 6º do artigo 202 da Constituição Federal e nada menciona sobre "outras entidades públicas" é forçoso concluir que "outras entidades públicas" mencionado no §3º refere-se efetivamente a "empresas controladas direta ou indiretamente".

A exposição de motivos da LC 108/01 corrobora que a intenção do legislador estava relacionada a "patrocinadores vinculados à administração pública":

> "(...) 4. As regras e princípios gerais do regime de previdência complementar, previstos no projeto de lei complementar que disciplina o caput do art. 202 da Constituição Federal, são imperativos para todo o regime, aplicando-se aos planos de benefícios e a todas as entidades de previdência complementar. Além daquelas regras e princípios, disposições especificas previstas nesta proposta lei complementar, elaborada para regulamentar, igualmente, os §§§ 3º, 5º e 6º do art. 202 da Constituição Federal, deverão ser observadas pelas entidades cujos patrocinadores estejam vinculados à administração pública."

No que concerne a interpretação histórica, antes da EC 20/98, a relação dos "patrocinadores públicos" e as entidades de previdência, no âmbito da administração pública federal, era regida pela Lei 8.020/90 e pelo Decreto 606/92.

Tais diplomas legais expressamente previam quem poderia ser "patrocinador

11 "§ 4º Lei complementar disciplinará a relação entre a União, Estados, Distrito Federal ou Municípios, inclusive suas autarquias, fundações, sociedades de economia mista e empresas controladas direta ou indiretamente, enquanto patrocinadoras de entidades fechadas de previdência privada, e suas respectivas entidades fechadas de previdência privada."

12 Art. 1o A relação entre a União, os Estados, o Distrito Federal e os Municípios, inclusive suas autarquias, fundações, sociedades de economia mista e empresas controladas direta ou indiretamente, enquanto patrocinadores de entidades fechadas de previdência complementar, e suas respectivas entidades fechadas, a que se referem os §§ 3º, 4º, 5º e 6º do art. 202 da Constituição Federal, será disciplinada pelo disposto nesta Lei Complementar.

público": as autarquias, as fundações, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União[13].

Na época já existiam as entidades do "Sistema S", as quais não se enquadravam no rol acima mencionado, ou seja, historicamente nunca foram consideradas "patrocinadoras públicas".

A EC 20/98 não teve a intenção de assim as considerar, pois da análise da PEC 33/1995 (que resultou na EC 20/98) não se discutiu essa ampliação.

Corrobora com essa ideia o §5º do artigo 202[14] da CF, pois quando se pretendeu inovar ou ampliar a aplicação dos preceitos trazidos pela EC 20/98, notadamente a paridade contributiva, o legislador assim o fez de forma expressa e clara, ao prever a aplicação da lei complementar do §4º (posteriormente a LC 108/01), no que couber, às empresas privadas permissionárias ou concessionárias de prestação de serviços públicos.

Assim, sob o processo histórico, também não parece ter o legislador tido a intenção de aplicar a paridade contributiva às entidades do "Sistema S".

Em relação ao aspecto teleológico, entendemos que a finalidade da norma foi evitar gastos públicos, porém de entes efetivamente relacionados à administração pública.

Nesse aspecto, reitere-se o entendimento do STF no RE citado, no sentido de que as entidades do "Sistema S" têm autonomia administrativa, utilizam-se basicamente de recursos recolhidos do próprio setor produtivo beneficiado e não integram a administração pública, motivo pelo qual a elas não seria aplicado o §3º do artigo 202 da CF, ou seja, a elas não seria aplicada a paridade contributiva.

III – Conclusão

Em que pese o tema ser complexo e ainda não ter sido apreciado pelo STF, entendemos que as entidades do "Sistema S" não estão sujeitas ao §3º do artigo 202 da Constituição Federal, ou seja, não estão sujeitas à regra da paridade contributiva.

Por: Paulo Sogayar Junior, sócio do escritório Sogayar Sociedade de Advogados, com 25 anos de experiência na assessoria a clientes em matérias relacionadas à área de saúde, seguros, previdência complementar e capitalização, com atuação no consultivo e contencioso (administrativo e judicial). Graduado pela USP (1993). Mestre em Direito Comercial com foco em seguros pela Universidade de Bristol, Inglaterra (1997/1998). MBA Executivo em Seguros pela FUNENSEG/IBMEC (2002/2003). Membro da Associação Internacional de Direito de Seguro – AIDA Brasil. Colaborador da ABRH-SP – Associação Brasileira de Recursos Humanos, na área da saúde. Palestrante de diversos seminários na área da saúde. Autor de diversos artigos na área.

---

13 Lei 8.020/90:
"Art. 1º Para os fins desta lei consideram-se: I – patrocinadoras: as autarquias, as fundações, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União; II – entidades: as entidades fechadas de previdência privada patrocinadas pelas pessoas jurídicas referidas no inciso anterior."
Decreto 606/1992:
"Art. 1º Para os fins deste decreto, consideram-se: I – patrocinadoras: as autarquias, as fundações, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União; II – entidades: as entidades fechadas de previdência privada, patrocinadas pelas pessoas jurídicas referidas no inciso anterior."

14 "§ 5º A lei complementar de que trata o parágrafo anterior aplicar-se-á, no que couber, às empresas privadas permissionárias ou concessionárias de prestação de serviços públicos, quando patrocinadoras de entidades fechadas de previdência privada."

LGPD e (Re) Seguros

BÁRBARA BASSANI

Sócia da área de seguros e resseguros de TozziniFreire Advogados, com atuação em consultoria, regulatório-SUSEP e contencioso estratégico (administrativo e judicial). Doutora e Mestre em Direito Civil pela Universidade de São Paulo – USP. Graduada pela Universidade Presbiteriana Mackenzie. Professora do MBA de Gestão Jurídica do Seguro e Resseguro da Escola Nacional de Seguros (Funenseg) e de diversos cursos de Seguros em outras instituições de ensino superior. Autora de diversos artigos e livros, com destaque para Seguros: Beneficiários e suas Implicações, publicado pela Editora Roncarati.

CARLA DO COUTO HELLU BATTILANA

Sócia da área de Privacidade de Dados de TozziniFreire Advogados com ampla dedicação em assessorar empresas de tecnologia em assuntos corporativos e transações diversas, assim como na preparação e revisão de termos de uso e políticas de privacidade. Mestre pela University of Chicago, EUA. Especializada em Direito Empresarial pelo Instituto Internacional de Ciências Sociais. Cursou extensão universitária em Contratos Empresariais pela Fundação Getúlio Vargas. Graduada pela Faculdade de Direito da Pontifícia Universidade Católica de São Paulo. CIPP/E (Certified Information Privacy Professional).

1. Introdução

Prevista para entrar em vigor em agosto de 2020, a Lei Geral de Proteção de Dados (LGPD)[1] trará inúmeros impactos para o mercado de seguros e resseguros.

Embora já exista, atualmente, no Brasil, arcabouço legislativo que garante a inviolabilidade da liberdade, da privacidade e da intimidade, como previsto na própria Constituição Federal e Código Civil, a LGPD é, certamente, um novo marco, o qual trata o assunto de dados de forma muito mais específica e com maior rigor do que conhecemos até então.

Para elucidar, a norma estabelece que os agentes de tratamento que violarem as disposições da LGPD, ficam sujeitos às seguintes sanções administrativas:

- Advertência, com indicação de prazo para adoção de medidas corretivas;

1 Lei nº 13.709, de 14/08/2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

- Multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 por infração;
- Multa diária, observado o limite total acima;
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- Eliminação dos dados pessoais a que se refere a infração.

Certamente, a LGPD traz uma mudança de paradigma para todas as empresas que operam nos mais diversos ramos de atividades, que irá fomentar o seguro para riscos cibernéticos, sendo uma oportunidade e um desafio para o mercado de (re) seguros.

Mas nem de longe esse é o único efeito para o mercado de (re) seguros. As supervisionadas, isto é, seguradoras, resseguradores e corretoras de (re) seguros deverão se adaptar à LPGD[2], adequando a forma de oferta, subscrição, contratação e cumprimento do contrato de (re) seguro.

O presente artigo busca elucidar, justamente, alguns aspectos práticos das discussões envolvendo a LGPD e a necessária adaptação das supervisionadas ao novo regramento.

2. Sujeição das supervisionadas pela SUSEP à LGPD

Nos termos da LGPD, todas as pessoas estão sujeitas à observância da legislação, desde que os dados sejam tratados ou coletados no Brasil ou, ainda, no caso de oferecimento de produtos e serviços no território nacional.

Há uma abrangência enorme na LGPD ao mencionar as seguintes atividades de tratamento de dados protegidos: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Destarte, considerando que a atividade (re) securitária depende da coleta e do tratamento de dados, não há dúvidas quanto a sua sujeição ao novo regramento. Seguradoras, corretoras de seguros, resseguradores e corretores de resseguros deverão observar a LGPD. A extensão da observância, entretanto, depende da forma como os dados são coletados, dos tipos de dados que são coletados e da realização das atividades de tratamento de dados.

3. Dados Protegidos

A LGPD define (i) dados pessoais como sendo aqueles identificados ou identificáveis (nome, endereço, idade, estado civil, e-mail, situação patrimonial, nº de IP); (ii) dados pessoais sensíveis (raça ou etnia, religião, política, saúde, vida sexual, dados genéticos ou biométricos); e (iii) danos anonimizados como aqueles que não contém nenhum elemento de identificação específico.

Os dois primeiros são dados protegidos nos termos da lei. Logo, tanto o ramo de danos como o ramo de pessoas e saúde estão abrangidos, sempre que envolverem dados de pessoas físicas, muito embora o dado sensível tenha maior tutela

2 A adaptação deverá, também, considerar os aspectos trabalhistas envolvidos, com relação aos dados dos funcionários.

legislativa, que deve ser ponto de alerta nas operações de (re) securitárias de vida e saúde.

Já o dado anonimizado, por ser um dado dissociado do titular, não é um dado protegido, nos termos da LGPD.

Nesse sentido, se a seguradora receber dados anonimizados para o estabelecimento do perfil ou mesmo se o ressegurador, por exemplo, receber dados anonimizados quando negociar produtos na subscrição em contratos automáticos de ramos como vida e saúde, sendo um dado anonimizado, não é dado protegido. Por outro lado, é importante que isso seja visto com cautela, pois esse dado poderá vir a ser protegido se o processo de anonimização ao qual foi submetido for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. Daí a importância da documentação por parte da supervisionada, de que, naquele momento, era, de fato, um dado anônimo, não protegido.

4. Princípios e Hipóteses de Tratamento

Os princípios elencados pela LGPD são os seguintes:

- finalidade (dados tratados para um fim específico);
- adequação (compatibilidade de tratamento dos dados com a finalidade);
- necessidade (uso e tratamento minimalista);
- livre acesso (garantia à consulta dos dados);
- transparência;
- qualidade de dados (clareza, relevância, atualização de acordo com a finalidade de tratamento);
- segurança (uso das medidas técnicas para garantir a segurança no tratamento);
- prevenção (adoção das medidas necessárias para prevenir danos); e
- não discriminação (impossibilidade de tratamento para fins discriminatórios, ilícitos e abusivos).

Portanto, com a entrada em vigor da LGPD, é importante que haja uma avaliação de como os dados são coletados, para quais finalidades e se o cliente tinha conhecimento de que seus dados seriam usados para a oferta de seguros, além de ter clareza quanto àquela finalidade específica quando forneceu os seus dados.

Vale o alerta de que, não se espera que o cliente cote um seguro de automóvel e forneça dados que possam ser usados para os ramos de vida / saúde ou oferta de outros seguros sem que ele tenha sido devidamente informado que seus dados poderiam ser utilizados para outras finalidades e que tenha concordado com isso.

Resguardada a hipótese de venda direta (ainda pouco utilizada), a seguradora, basicamente, depende de parceiros para ter acesso à base de clientes. É muito comum que, além do corretor de seguros, a seguradora busque parceiros com ampla base de clientes, como varejistas, concessionárias e canais bancários.

Por exemplo, o cliente tem relacionamento com o varejista, com o banco, e forneceu os seus dados para aquela finalidade específica de comprar um bem ou para ser correntista de uma instituição financeira. Esse cliente espera ser acessado para a oferta de seguros?

Certamente, não espera. Se a oferta do seguro for feita de forma concomitante à oferta do bem, a informação poderá ser mais facilmente transmitida. Porém, se o dado for coletado como um cliente de um parceiro comercial e, posteriormente, esse

cliente for acessado para a oferta de seguros, poderá haver um problema com relação à finalidade para qual aqueles dados foram coletados.

Assim, será necessário avaliar se o cliente tinha conhecimento e consentiu que o dado coletado seria utilizado, também, para a finalidade de oferta de seguros, por exemplo.

Por isso, o consentimento para que os dados do cliente sejam utilizados para a oferta de seguros parece ser a hipótese mais adequada quando estamos diante de canais de distribuição diferentes do corretor.

Deve-se ter em consideração o dever de informação ao titular do dado (potencial segurado) quando da oferta, sendo fundamental a estruturação da oferta de um modo que atenda às necessidades legislativas, mas que continue atraente do ponto de vista comercial.

Se, por um lado, a LGDP possibilita que o consentimento não seja dado por escrito, isto é, seja oral, interativo, por vídeos, chamadas, etc.; por outro, a LGPD proíbe termos genéricos e muito longos, o que ensejará a necessidade de as empresas serem criativas para estruturar suas políticas de privacidade, materiais de marketing e documentos para obtenção do consentimento.

Órgãos de proteção à defesa do consumidor poderão entender como irregulares termos de uso genéricos que mencionam que os dados poderão ser usados pelos parceiros comerciais para aprimoramento da prestação de serviços (uma vez que isso pode abranger diversas finalidades não especificadas), pois não se sabe exatamente o que vai ocorrer com esses dados e qual nível de compreensão do que irão fazer com o dado.

Outro ponto que merece atenção é a possibilidade de retirada do consentimento, que requer uma grande adaptação no que se refere à integração de sistemas a fim de torná-lo eficaz e viável, quando seu exercício for possível e não obstar o próprio cumprimento do contrato.

Enfim, justamente, pelo fato de que o consentimento pode ser retirado a qualquer momento e, a depender da forma como é feito esse consentimento, que pode ser considerada nula, é que, nem sempre essa será a melhor base para justificar o tratamento.

Além do consentimento, o artigo 7º, da LGPD, estabelece outras nove hipóteses de tratamento de dados pessoais:

(i) para o cumprimento de obrigação legal ou regulatória pelo controlador;

(ii) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições da lei;

(iii) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

(iv) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

(v) para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

(vi) para a proteção da vida ou da incolumidade física do titular ou de terceiro;

(vii) para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

(viii) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

(ix) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Entre as hipóteses acima, o interesse legítimo (interesse certo, verdadeiro, autêntico à luz da lei), o cumprimento de obrigação legal (por exemplo, uma exigência da SUSEP) e de execução do contrato destacam-se como aquelas que vislumbramos ser mais pertinentes quando o (re) seguro já foi contratado, ou seja, após a fase da oferta, na regulação do sinistro e no cumprimento do contrato.

5. Agentes de Tratamento: Seguradora e Ressegurador, Controlador ou Operador?

Quanto aos agentes de tratamento, a LGPD traz a figura do controlador e do operador. O primeiro é aquele a quem compete as decisões sobre tratamento dos dados pessoais. Já, o segundo, é aquele que realiza o tratamento de dados conforme as instruções do controlador.

A simples definição legal de ambas as figuras não torna indubitável a inserção da seguradora, do ressegurador ou dos brokers em uma ou outra figura (controlador ou operador), merecendo uma análise mais acurada no âmbito das relações entre eles no caso concreto.

A linha entre uma e outra figura pode ser bastante tênue. O representante de seguros, por exemplo, é o controlador no âmbito dos dados coletados para o seu cliente (exemplo: compra de um eletrodoméstico), mas para a oferta do seguro, ele poderá ser o operador, já que trata aqueles dados no âmbito do seguro por força da sua qualidade de representante de seguros.

No âmbito do resseguro, o fato de o ressegurador ser responsável pelo pagamento da indenização ou de ter controle na regulação de sinistros[3] não o torna automaticamente um controlador ou um operador. Porém, na medida em que o ressegurador tratar os dados em seu benefício próprio, independentemente de instruções da seguradora e/ou do broker, poderia sim ser enquadrado como um controlador.

Na maioria das vezes, considerando a dinâmica atualmente estabelecida nas operações de seguros e resseguros, a tendência é que os players (seguradora / corretor / ressegurador) irão atuar como co-controladores e, como tal, teriam uma série de obrigações previstas na lei, como a de nomear um encarregado.

O encarregado (mais comumente conhecido também como –) é indicado pelo controlador (não pelo operador) para estabelecer um canal de comunicação entre agentes, titulares (no caso, clientes / segurados) e órgãos competentes relacionados à proteção de dados. O DPO teria como principais funções: (i) a orientação de funcionários sobre as regras de proteção de dados; (ii) o recebimento de reclamações; (iii) o mapeamento estratégico do tratamento de dados da empresa; (iv) a realização de auditorias para controle do cumprimento da legislação.

Por maior desconforto que possa trazer para o ressegurador o recebimento de instruções da seguradora acerca de como tratar os dados no âmbito do resseguro e o que fazer com eles, talvez a adaptação das operações e contratos atuais possa fazer mais sentido e criar um desconforto menor a fim de evitar que o ressegurador seja visto como quem tem contato com

3 Por força de claims cooperation / claims control.

o segurado (pessoa física e titular dos dados), o que iria ao desencontro de toda a sistemática conceitual do resseguro.

O ressegurador, na maioria das vezes, não tem contato direto (ou ao menos não deveria ter contato direto com o segurado, embora saibamos que, em grandes riscos, muitas vezes o próprio segurado determina, busca e vai atrás da colocação do risco diretamente no ressegurador). Porém, como a lei protege dados de pessoas físicas e não jurídicas, poderão ser poucas as situações em que o ressegurador é o controlador. O fato de ter ou não um broker, a princípio, nada mudaria a obrigação do ressegurador. É preciso, igualmente, avaliar qual o papel do broker com relação aos dados (se é controlador de algum modo ou operador e operador de quem – da seguradora ou do ressegurador).

Independentemente do enquadramento, é digno de nota que tanto o controlador como o operador têm responsabilidades legais. Logo, não é a inserção de uma cláusula contratual que tornará a seguradora, o broker ou o ressegurador responsável pelo tratamento do dano, mas sim a própria atividade desempenhada pelo e a responsabilização legal advinda do desempenho da referida atividade. Obviamente, a inserção de cláusulas contratuais é relevante para dirimir a relação entre as partes e para definir, no âmbito do contrato, o direito de regresso entre as partes (seguradora / representante de seguros; seguradora / corretora de seguros; seguradora / estipulante de seguros; seguradora / ressegurador; ressegurador / broker, etc.), mas não será o contrato que irá eximir uma ou outra parte perante o titular do dado, à luz das suas obrigações legais de controlador ou operador[4].

4 Os agentes de tratamento devem adotar medidas de segurança para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

6. Autoridade Nacional de Proteção de Dados

Os artigos da LGPD que tratavam sobre a criação de uma agência de proteção de dados foram vetados no momento de sua sanção. Nesse contexto, e para suprir tal lacuna, foi publicada, em 28/12/2018, a Medida Provisória nº 869 que criou a Autoridade Nacional de Proteção de Dados (ANPD), cujas principais competências são:

(i) zelar pela proteção de dados pessoais;

(ii) editar normas e procedimentos sobre a proteção de dados pessoais;

(iii) interpretar, na esfera administrativa, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), sendo o órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para sua interpretação;

(iv) requisitar informações aos controladores e operadores de dados pessoais;

(v) implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a LGPD;

(vi) fiscalizar e aplicar sanções, mediante processo administrativo, nos casos de descumprimento da LGPD, tendo competência exclusiva para a aplicação de tais sanções; e

(vii) promover ações de cooperação com autoridades de proteção de dados internacionais.

A ANPD será vinculada diretamente à Presidência da República, tendo em sua composição um Conselho Diretor (órgão máximo de direção, com cinco membros a serem nomeados pelo presidente da República); um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;

uma Corregedoria; uma Ouvidoria; um órgão de assessoramento jurídico próprio; além de unidades administrativas e unidades especializadas necessárias à aplicação do disposto na LGPD.

Vale notar que a ANPD gozará de autonomia técnica, razão pela qual, será ela a autoridade para tratar de dados, não cabendo à SUSEP fazê-lo, ainda que para o mercado supervisionado.

Apesar disso, considerando que o mercado (re) securitário é fortemente regulamentado, é importante que não haja incompatibilidade com as regras editadas por ambas. Assim, percebemos um certo consenso de que o mercado deve se unir e levar à ANPD as especificidades de sua atividade regulada, envolvendo seguros e resseguros, a fim de evitar que as regras editadas pela nova autoridade sejam contraditórias à dinâmica (re) securitária.

De qualquer modo, aguarda-se a conversão da Medida Provisória nº 869 em lei, o que ainda não ocorreu até a data do envio do presente artigo.

7. Considerações Finais

É de fundamental importância que as supervisionadas avaliem quais dados são coletados, para quais finalidades, como é feita a coleta, se é realizada mais alguma atividade de tratamento (armazenamento, distribuição, etc.), se, na referida atividade, o papel desempenhado encaixa-se no conceito de controlador ou de operador e, ainda, quais são os papéis de seus parceiros comerciais.

Feito o referido mapeamento, a revisão dos acordos operacionais celebrados entre as seguradoras e seus parceiros comerciais, bem como dos contratos de resseguro, é bastante recomendável a fim de que seja estabelecido, claramente (i) a quem compete a decisão quanto aos dados tratados; (ii) as obrigações e deveres de cada parte, evitando-se a inclusão de cláusulas genéricas, para resguardar o direito de regresso de uma parte com relação à outra.

Igualmente relevante a revisão dos materiais de marketing relacionados à distribuição de seguros e políticas de privacidade, especialmente, na hipótese de contratação por meios remotos.

Além disso, a adoção de medidas para a documentação das operações de tratamento e a estruturação de plano de ação para o caso de eventuais incidentes de vazamento de dados são recomendáveis à luz da LGPD. A adaptação ao novo regramento demandará, portanto, um trabalho conjunto, que deve ser feito por diversas áreas, como tecnologia da informação, jurídico, , comunicação, entre outras.

Por fim, embora a ANPD goze de autonomia técnica, espera-se que a SUSEP possa dialogar com a nova autoridade, para que a regulamentação da LGPD não prejudique a atividade (re) securitária, a fim de evitar incompatibilidade entre o conjunto normativo regulatório de (re) seguros e a legislação de proteção de dados. Para tanto, é o momento do mercado estar unido, na busca pela melhor interpretação e cumprimento da LGPD.

A Diversidade e o Ambiente Ético da Empresa

VALERIA CAMACHO MARTINS SCHMITKE
LatAm regional General Counsel Zurich Minas Brasil Seguros e Presidente do Instituto pela Diversidade no Setor de Seguros

Muito se tem falado sobre Diversidade. E isso é muito bom. Devemos reforçar a cultura de Diversidade nas empresas porque isso é o certo a fazer, porque o respeito pela Diversidade humana nos torna mais humanos, porque isso traz inovação e agilidade para a empresa nos negócios.

Mas há outro aspecto importante da cultura de respeito à Diversidade que é pouco comentado: implementar uma cultura de Diversidade torna o ambiente interno da empresa mais ético, mais "em compliance".

Primeiramente, qualquer cultura de Diversidade depende de um ambiente de real meritocracia. A própria essência dos programas de D&I indica que cada profissional será contratado, avaliado e promovido por seus próprios méritos, sem consideração de gênero, raça, opção sexual, idade, religião etc. Se todos serão avaliados pelo que entregam, pelo próprio desenvolvimento como profissionais, não haverá favoritismos e a Justiça se instalará. Onde há Justiça, não há espaço para atos desonestos, corrupção e práticas erradas de qualquer tipo. Não haverá preferidos, nem duas classes de profissionais – os que têm chance de promoção e os que não têm.

Ainda, o respeito à Diversidade eleva os patamares éticos de uma companhia. Não se toleram mais piadas racistas, sexistas e homofóbicas, portanto não se toleram assédios sexuais, assédios morais, bullying, desrespeito em geral. Todo o ambiente ético da empresa se eleva, deixando as práticas desonestas e facilitadoras cada vez mais abaixo do que se espera dos empregados.

Os programas de Diversidade atraem pessoas melhores, pessoas preocupadas com o outro, que têm padrões éticos mais rígidos. Tais pessoas se sentem confortáveis em ambientes onde as mulheres, os negros, os gays, os idosos são vistos como pessoas e profissionais tão importantes quanto qualquer outro. Tais pessoas não têm nenhuma necessidade de utilizar seus privilégios para crescer profissionalmente, porque já são bons profissionais. E bons profissionais não precisam de subterfúgios para conseguir bons negócios, não precisam de ações fraudulentas para obter mais dinheiro, porque para eles o dinheiro é consequência do bom trabalho e da boa postura profissional. Ainda, a empresa atrairá os melhores talentos entre as mulheres, os negros, os gays, porque estes se sentirão respeitados, valorizados, com chance de crescer. Cria-se um círculo virtuoso que somente trará benefícios.

Os programas de D&I trazem diversos benefícios às empresas: melhor ambiente de trabalho, construção de uma marca respeitada, atração de melhores talentos, mais inovação, mais meritocracia entre outros. Mas um bônus inesperado é um melhor ambiente de compliance: mais honestidade, mais cumprimento das regras, menos problemas trabalhistas.

As empresas em geral ainda têm um longo caminho a seguir, há muito que fazer. Mas entender que D&I traz muitas vantagens e é bom para a empresa em muitos aspectos vai incentivar os administradores a trabalhar ativamente para que isso seja uma realidade.

LegisCompliance, o Portal que auxilia na Gestão das Demandas Regulatórias ligadas ao compliance no Brasil

Cadastre-se gratuitamente em:
www.legiscompliance.com.br

- Base de Dados inteligente
- Textos atualizados e consolidados
- Filtros de busca que facilitam a pesquisa
- Legislação e normatização reunidas em um único ambiente
- Ferramenta de suporte para as áreas de compliance, jurídica, controles internos e governança
- Envio de informativos

RONCARATI EDITORA

Legis Compliance

LEGISCOR: INFORMAÇÕES E NOVIDADES PARA O CORRETOR DE SEGUROS

LegisCor®
Legislação do Corretor de Seguros