ISSN 0123-1154 (IMPRESO)
ISSN 2500-7556 (EN LÍNEA)

NOVAS TECNOLOGIAS, PROTEÇÃO DE DADOS PESSOAIS E SEGUROS[*]

NEW TECHNOLOGIES, DATA PROTECTION AND INSURANCE

NUEVAS TECNOLOGÍAS, PROTECCIÓN DE DATOS Y SEGUROS

ANGELICA L. CARLINI[**]

Fecha de recepción: 10 de octubre de 2022
Fecha de aceptación: 30 de octubre de 2022
Disponible en línea: 30 de diciembre de 2022

Para citar este artículo/To cite this article

Carlini, Angelica L., *Novas tecnologias, proteção de dados pessoais e seguros,* 57 Rev.Ibero-Latinoam.Seguros, 271-288 (2022). https://doi.org/10.11144/Javeriana.ris57.ntpd

doi:10.11144/Javeriana.ris57.ntpd

[*] Ponencia presentada en XVII Congreso del Comitê Iberolatinoamericano da Associação Internacional de Derecho de Seguros – CILA-AIDA em agosto de 2022, em San José na Costa Rica.

[**] Pós-Doutorado em Direito Constitucional. Doutora em Direito Político e Econômico. Mestre em Direito Civil. Pós-Graduada em Direito Digital e em Análise Econômica do Direito. Graduada em Direito. Advogada, parecerista, consultora e palestrante nas áreas de Direito de Seguro, Novas Tecnologias, Proteção de Dados, Responsabilidade Civil e Relações de Consumo. Contacto: angelicacarlini@carliniadvogados.com.br.

RESUMO

O artigo analisa os principais aspectos da Lei Geral de Proteção de Dados – LGPD implantada no Brasil em agosto de 2020. Também cuida do impacto da nova legislação no setor de seguros, em especial em ambiente de implantação do sistema aberto de seguros –open insurance–, criado para ampliar o acesso a seguros para a população brasileira.

Palavras Chave: Novas Tecnologias. Proteção de Dados Pessoais. Seguros. Open Insurance.

ABSTRACT

The article analyzes the main aspects of the General Data Protection Law – LGPD implemented in Brazil in August 2020. It also deals with the impact of the new legislation on the insurance sector, especially in the environment of implementation of the open insurance system – open insurance -, created to expand access to insurance for the Brazilian population.

Keywords: New Technologies. Protection of Personal Data. insurance. Open Insurance.

RESUMEN

El artículo analiza los principales aspectos de la Ley General de Protección de Datos - LGPD implementada en Brasil en agosto de 2020. También aborda el impacto de la nueva legislación en el sector de seguros, especialmente en el ámbito de implementación del sistema de seguros abierto - open seguros -, creado para ampliar el acceso a los seguros para la población brasileña.

Palabras clave: Nuevas Tecnologías. Protección de Datos Personales. seguro. Seguro Abierto.

SUMARIO

INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais, Lei 13.709, de 14 de agosto de 2018, entrou em vigor no Brasil no dia 20 de agosto de 2020 e, trouxe substancial modificação na forma como as empresas que atuam com dados pessoais executam seu trabalho no cotidiano.

Essa lei que tem sido chamada pelas iniciais LGPD teve relevante impacto para o setor de seguros que, por excelência, utiliza dados pessoais para realizar a avaliação e subscrição de riscos, tanto quanto precisa deles para os trabalhos específicos de regulação de sinistros e pagamento de indenizações.

A LGPD modificou a forma como as empresas administram a coleta, arquivamento, tratamento e utilização de dados em seu dia a dia. A lei define tratamento de dados como toda operação realizada com dados pessoais tais como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Essa definição é fundamental para a compreensão da aplicabilidade da lei.

O objetivo da lei foi definido para proteger o titular dos dados pessoais para que não haja utilização sem consentimento, excessiva, desnecessária ou, prejudicial.

Na atividade de seguros todos os ramos utilizam em maior ou menor escala dados pessoais do próprio segurado, do beneficiário indicado ou, de representantes legais de empresas que contratam seguros. Nas diferentes etapas, da proposta ao pós-contrato os dados pessoais são importantes na relação entre segurados e seguradores e, exatamente por isso, a LGPD terá influência significativa nesse setor.

A lei foi aprovada pelo poder legislativo brasileiro apenas quatro meses após a entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia - RGPD, que ocorreu em maio de 2018. O regulamento europeu criou a necessidade de adaptação para muitas empresas que trabalham globalmente, inclusive seguradoras, resseguradoras e corretoras de seguro.

O RGPD europeu é aplicável a situações em que o tratamento de dados acontece nas atividades de uma empresa que está estabelecida em um dos países que compõem a União Europeia e, em consequência, se aplica às empresas que não estão instaladas na União Europeia, mas se relacionem comercialmente com empresas situadas naquela região.

A necessidade de algumas empresas adequarem suas atividades ao Regulamento de Proteção de Dados Pessoais da União Europeia contribuiu para que o legislativo brasileiro agilizasse o debate sobre a lei geral de proteção de dados brasileira, até porque já existiam projetos de lei em andamento há alguns anos no parlamento brasileiro.

A proteção de dados pessoais é uma necessidade indiscutível em nossos tempos. Todas as pessoas são portadoras de dados e os fornecem diariamente em inúmeras situações diferentes.

Nossos dados pessoais são indispensáveis para a formalização de transações de alto valor como a obtenção de empréstimo para compra da casa própria, como também em transações de pequeno valor e, por vezes, até para acesso a serviços gratuitos.

Regular o tratamento de dados pessoais é uma exigência contemporânea em especial no contexto da implementação das novas tecnologias e, refletir sobre essa exigência à luz da atividade de seguros privados é o objetivo deste trabalho.

1. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) – A QUEM SE APLICA, ONDE SE APLICA, QUAIS OS OBJETIVOS E PRINCÍPIOS.

1.1. A Quem Se Aplica

A Lei Geral de Proteção de Dados se aplica às pessoas naturais ou jurídicas, da área pública ou privada, que atuam com dados pessoais em qualquer meio inclusive digital.

Assim, se alguma pessoa natural ou jurídica de direito público ou privado ainda tratar dados pessoais em papel também terá que, obrigatoriamente, cumprir a lei; e, quem atua por meio digital, mais comum em nossos dias, igualmente estará obrigado a cumpri-la.

1.2. Onde Deve Ser Aplicada a Lei

A LGPD será aplicada a todas as operações de tratamento de dados realizadas em território brasileiro; ou, quando os dados tenham sido coletados para a oferta ou o fornecimento de bens ou serviços ou, o tratamento de dados de indivíduos localizados no território brasileiro; e, ainda, nas situações em que os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Não importa que a pessoa natural ou jurídica, de direito público ou privado, tenha sua sede em outro país. Basta que a operação de tratamento de dados se realize no Brasil para que a legislação nacional seja aplicada. Também não importa que os dados sejam coletados de pessoas naturais estrangeiras; se elas estiverem no Brasil no momento da coleta dos dados, a lei brasileira será aplicada para sua proteção.

1.3. Objetivos da Lei

Os objetivos da lei da LGPD são:

a) Respeito À Privacidade – todo titular de dados pessoais tem direito de ser respeitado em sua privacidade, ou seja, partilhar dados apenas para pessoas autorizadas por ele e com objetivos específicos.

b) Autodeterminação Informativa – autodeterminação é o direito que cada pessoa tem de decidir por si só, ou seja, decidir de forma livre e autônoma o que considera

melhor para ela. A partir da LGPD não se admite o compartilhamento de informações sem consentimento do titular dos dados. O consentimento do titular de dados pessoais é essencial em qualquer atividade pública ou privada de tratamento de dados.

c) Liberdade de Expressão, Informação, de Comunicação e de Opinião – esses fundamentos estão previstos na Constituição brasileira como direitos fundamentais.

d) Inviolabilidade da Intimidade, da Honra e da Imagem – todas as pessoas nascidas no Brasil ou estrangeiros residentes n o país, têm direito constitucional a proteção de sua intimidade, honra e imagem, por isso a lei de proteção de dados pessoais igualmente garante esses direitos.

e) Desenvolvimento Econômico e Tecnológico e a Inovação – a necessidade de proteção de dados pessoais não pode colidir com a necessidade que o país tem de desenvolvimento econômico, tecnológico e de inovação.

f) Livre Iniciativa, Livre Concorrência e Defesa do Consumidor – são princípios constitucionais que serão respeitados por meio da aplicação da lei de proteção de dados pessoais. Cumprem o papel de equilibrar a necessidade de desenvolvimento econômico pela livre iniciativa com o respeito às pessoas naturais que não podem ter seus dados pessoais utilizados indevidamente e sem seu consentimento.

g) Direitos Humanos, Livre Desenvolvimento da Personalidade, Dignidade e Exercício da Cidadania pelas Pessoas Naturais – todos esses são fundamentos constitucionais da República Federativa do Brasil para a proteção das pessoas naturais nos múltiplos aspectos que compõem seu direito a uma vida digna. Em 10 de fevereiro de 2022 entrou em vigor a Emenda Constitucional 115, que acrescentou o inciso LXXIX ao artigo 5º da Constituição Federal brasileira, para tornar o direito à proteção de dados pessoais, inclusive nos meios digitais, um direito e garantia fundamental constitucional.

1.4. Princípios da LGPD

A LGPD brasileira também adotou princípios que terão que ser rigorosamente seguidos por todas as pessoas físicas ou jurídicas, públicas ou privadas, que atuarem com coleta e tratamento de dados pessoais.

Os princípios estão listados no artigo 6° da LGPD e são: boa-fé, finalidade, adequação, necessidade, qualidade de dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Entre esses princípios merecem destaque:

- Finalidade – a utilização dos dados pessoais terá que ser feita sempre com propósitos legítimos, específicos, explícitos e informados ao titular dos dados. Coletados os dados para uma finalidade específica, não poderão ser utilizados para outra.

- Adequação – os dados coletados deverão ser tratados em conformidade com a finalidade para a qual foram obtidos. Novamente aqui, fica vedada a obtenção para uma finalidade e o uso inadequado.

- Necessidade – os dados pessoais coletados deverão ser tratados de forma limitada ao mínimo necessário para que as finalidades sejam adequadamente atingidas. Isso significa que os dados pessoais solicitados deverão ser sempre o mínimo necessário.

- Livre Acesso **–** os titulares dos dados pessoais terão direito a consulta facilitada e gratuita de seus dados, durante todo o período de duração da utilização deles; a consulta poderá ser à integralidade dos dados ou, a alguns especificamente do interesse do titular.

- Qualidade dos Dados **–** a lei obriga aqueles que coletam e tratam dados pessoais que garantam a exatidão, clareza, relevância e atualização em conformidade com as necessidades e finalidades do tratamento. As pessoas físicas e jurídicas, públicas ou privadas, que utilizam dados pessoais devem coletá-los de forma objetiva, exata, clara e mantê-los atualizados para que nenhum resultado adverso atinja o titular dos dados apenas por falta de atualização ou clareza.

- Transparência – significa que os titulares dos dados pessoais deverão ter a garantia de que as informações disponíveis a seu respeito são claras, precisas, facilmente acessíveis para qualquer verificação necessária, respeitados os segredos industriais e comerciais utilizados pelos organizadores da coleta e do tratamento de dados.

- Prevenção **–** consiste na obrigatoriedade na adoção de medidas para prevenir qualquer fato ou ato que propicie danos aos titulares de dados pessoais.

- Não Discriminação **–** a coleta de dados pessoais não pode ser realizada com finalidade discriminatória.

Os princípios são objetivos e ao mesmo tempo organizam a atividade de coleta e tratamento de dados pessoais, com a finalidade de proteger os titulares, mas não impedem a atividade econômica e empresarial, apenas impõe que elas sejam adaptadas aos termos da lei.

2. LEI GERAL DE PROTEÇÃO DE DADOS –LGPD– TERMINOLOGIA ADOTADA

O uso de dados pessoais para realização de negócios ou para a viabilização de atendimento pelo setor público é antigo na história da humanidade. Desde há muito tempo as pessoas fornecem seu endereço, número de telefone, número de documentos pessoais, dados bancários, dados pessoais como gênero, estado civil, entre tantos outros para que os setores público e privado possam atuar.

Nas últimas décadas, no entanto, o fornecimento de dados se avolumou exponencialmente porque passamos a utilizar a rede mundial de computadores – internet– para muitas atividades que antes só fazíamos presencialmente. Depois do período de isolamento social que foi adotado em muitos países como medida profilática para a prevenção da contaminação da COVID-19, praticamente não há limite para o que pode ser feito pela internet.

Para uniformizar as expressões utilizadas nesse novo universo do mundo digital a Lei Geral de Proteção de Dados dedicou o artigo 5°, exclusivamente, para definições que deverão ser adotadas por todos que utilizam dados pessoais em suas atividades.

Algumas dessas definições merecem destaque:

- Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável.

- Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. São dados que uma pessoa nem sempre deseja compartilhar ou, mesmo que se torne conhecido para outras pessoas.

- Dado Anonimizado: dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

- Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. É importante reparar que a lei adjetivou o consentimento de forma a tornar claro que não é qualquer forma de consentimento que pode ser interpretada como adequada à lei. Somente o consentimento prestado de forma livre, informada e inequívoca, que não deixe dúvida de que se trata de consentimento para tratamento de dados pessoais.

- Agentes de Tratamento: pela lei brasileira são o controlador e o operador.

- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

- Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O encarregado poderá ser pessoa natural ou jurídica e, não é preciso que seja uma pessoa com poderes específicos apenas para isso, pode ser alguém que exerça outras atividades na empresa e passe a exercer também essa. Pode ser, ainda, uma empresa pessoa jurídica contratada para exercer essa atividade.

- Relatório De Impacto À Proteção De Dados Pessoais: documento de responsabilidade do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Sendo o controlador o agente de tratamento de dados responsável pelas decisões, também será dele a responsabilidade pela construção do relatório de impacto à proteção de dados, com objetivo de descrever os processos utilizados para tratamento de dados pessoais, bem como todos as medidas adotadas para prevenir a ocorrência dos riscos a que os bancos de dados estão sujeitos.

3. BASE LEGAL PARA TRATAMENTO DE DADOS NA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

O artigo 7º da Lei Geral de Proteção de Dados – LGPD determina em que situações específicas poderá ser realizado o tratamento de dados, ou seja, fornece a base legal que autoriza o tratamento de dados por pessoas físicas, jurídicas, de direito público ou privado.

A primeira alternativa legal é consentimento do titular de dados. Essa tem sido considerada a base de dados mais frágil porque o consentimento poderá ser revogado a qualquer tempo. Esse consentimento deverá estar expresso desde o primeiro contato que, no caso específico do seguro, quase sempre ocorre no preenchimento físico ou digital da proposta de seguros, momento em que já são solicitados dados como nome, endereço, estado civil, número de documentos de identidade, gênero, existência de filhos, profissão, entre outros.

Além do consentimento expresso, os dados pessoais poderão ser utilizados para cumprimento de obrigação legal ou regulatória pelo controlador. Essa possibilidade é muito importante para o setor de seguros que é um setor regulado pelo Estado e tem inúmeras obrigações a atender em razão da regulação.

A administração pública poderá tratar e compartilhar dados necessários à execução de políticas públicas previstas em lei e regulamentos ou, respaldadas em contrato, convênios ou instrumentos congêneres. Também o poder público e a iniciativa privada poderão utilizar dados pessoais para estudos por órgãos de pesquisa, garantida, sempre que possível a anonimização dos dados pessoais.

Os dados pessoais poderão ser utilizados, ainda, quando necessários para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular dos dados pessoais seja parte e, sempre a pedido deste. Esta também é uma base legal importante para o setor de seguros privados porque propostas e contratos são fundamentais para a relação securitária entre segurados e seguradores. Também é relevante para todos os setores econômicos e de seguros em especial, a previsão legal de utilização de dados pessoais para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

A LGPD autoriza a utilização de dados para proteção da vida ou da incolumidade física do titular ou de terceiros; e, para a tutela da saúde exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou de autoridade sanitária.

Há, ainda, previsão legal para utilização de dados pessoais 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 de dados pessoais.

Prevê o artigo 7º por fim, que os dados pessoais poderão ser utilizados na proteção do crédito, em consonância com a legislação existente sobre o assunto.

A utilização de dados pessoais fora dessas hipóteses estará em confronto com a legislação e, ensejará a aplicação de sanções e condenação em indenizações por responsabilidade decorrente da utilização indevida.

A LGPD não proíbe o compartilhamento de dados, mas determina que o titular dos dados tem direito de saber sobre o compartilhamento e sua finalidade e, não autorizar que sejam utilizados em algumas circunstâncias.

No setor de seguros privados o compartilhamento de dados pessoais é feito de forma usual em muitas situações diferentes. Dados pessoais são compartilhados entre o corretor de seguros e o segurador; entre o segurador e os prestadores de serviços (oficinas referenciadas, rede credenciada de prestadores de serviços de saúde, reguladores de sinistro terceirizados, advogados, entre outros); entre os prestadores de serviços (reguladores de sinistro e oficinas referenciadas; médicos e hospitais); e, também entre empresas do mesmo grupo econômico para fins negociais. Em todas essas hipóteses o compartilhamento deverá ser: autorizado expressamente e informado ao titular de dados pessoais; e, nas hipóteses em que não houver autorização expressa mas existir base legal nos termos do artigo 7º, como por exemplo para atender as exigências regulatórias, o segurador poderá utilizar sem receio de aplicação de punições ou de condenação no dever de reparar danos, ainda que morais.

4. AGENTES DE TRATAMENTO DE DADOS PESSOAIS E RESPONSABILIDADES

A LGPD determina que o controlador e o operador deverão manter registro das operações de tratamento de dados pessoais que realizarem, principalmente quando esse tratamento for fundamentado em legítimo interesse, como ocorre com o setor de seguros quando precisa manter dados pessoais arquivados para cumprimento de disposições do órgão regulador.

As atividades de controlador e operador poderão ser objeto de relatório solicitado pela Autoridade Nacional de Proteção de Dados, inclusive em relação a dados sensíveis, e o relatório deverá conter entre outras informações, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O operador de tratamento de dados pessoais é a pessoa encarregada de realizar o tratamento em conformidade com as instruções do controlador, cabendo ao próprio controlador verificar se suas instruções estão sendo cumpridas e se elas estão adequadas à legislação.

Cabe ao controlador, ainda, indicar quem será o encarregado pelo tratamento de dados pessoais, disponibilizar sua identidade e informações de contato de forma pública preferencialmente no portal da empresa na qual o controlado exerce sua atividade.

As principais atividades previstas na LGPD para o encarregado são:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

- Receber comunicações da autoridade nacional e adotar providências;

- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e,

- Executar outras atribuições determinadas pelo controlador ou, estabelecidas em normas complementares que venham a ser criadas principalmente pela Autoridade Nacional de Proteção de Dados – ANPD.

Da atividade de controlador e encarregado decorrerão responsabilidades e obrigação de reparar danos materiais e imateriais quando esses atingirem o titular de dados pessoais.

As duas principais causas de danos são: deixar de observar as determinações da Lei Geral de Proteção de Dados e, tratar dados sem segurança técnica adequada para a finalidade a que se destina.

Os agentes de tratamento de dados pessoais ou, qualquer outra pessoa que trate dados pessoais autorizada por eles, terá obrigação de garantir a segurança da informação em todas as fases, o que inclui responsabilidade mesmo após o término da finalidade que deu sustentação ao tratamento. No caso dos contratos de seguro após o encerramento do período de vigência, persiste a responsabilidade pela segurança técnica dos dados pessoais dos segurados enquanto o segurador for obrigado pelo regulador a manter esses dados arquivados.

O operador de dados pessoais responderá solidariamente pelos danos que causar aos titulares nos casos em que comprovadamente não cumprir as determinações da lei ou, as instruções do controlador. Este por sua vez quando estiver diretamente envolvido no tratamento de dados do qual resultaram danos para o titular, responderá solidariamente com o operador.

O titular de dados terá em seu benefício o instituto da inversão do ônus da prova nos termos do que já acontece na atualidade em decorrência da aplicação do Código de Defesa do Consumidor, Lei 8.078, de 1990. A inversão do ônus da prova não ocorrerá de forma automática, mas, por determinação judicial quando o magistrado concluir que as alegações do titular de dados são verossímeis, quando houver comprovada hipossuficiência do titular ou, quando a produção da prova se mostrar excessivamente onerosa para o titular.

Não haverá responsabilidade em todas as situações comprovadas em que os agentes: (I) não realizaram o tratamento de dados pessoais que lhes foi atribuído; (ii) embora tenham realizado o tratamento de dados pessoais, não ficou demonstrada a violação da LGPD; e, (iii) o dano alegado pelo titular de dados pessoais decorreu de sua ação exclusiva ou, de terceiro que não tem nenhum relacionamento com os agentes de tratamento de dados pessoais.

A segurança no tratamento de dados pessoais é ponto fundamental para que não ocorram hipóteses de responsabilidade a ser reparada por danos causados ao titular dos dados. Todos os dispositivos de segurança técnica deverão ser utilizados com a finalidade de proteger o tratamento de dados contra vazamento e outras possibilidades que possam vir a causar prejuízos aos titulares.

O controlador de tratamento de dados pessoais está obrigado por lei a comunicar a Autoridade Nacional de Proteção de Dados e, ao titular dos dados pessoais todos o incidente de insegurança que potencialmente possa causar riscos ou danos relevantes aos titulares. Essa hipótese será aplicada apenas e tão somente às situações em que os riscos ou danos sejam relevantes, ou seja, de importância comprovada como acontece com os vazamentos de dados ou, o acesso indevido.

A LGPD estabelece que a comunicação deverá ser feita em um prazo razoável e, embora não haja estipulação do prazo em dias ou horas, é possível interpretar que ele deva ser definido para cada situação concreta e aplicado sempre com critério de maior brevidade possível para transmissão da informação. Não tão rápido que a informação não seja segura e, nem tão lento que não seja mais possível tomar providências próprias do gerenciamento de crise.

Ao ter conhecimento da informação sobre riscos a Autoridade Nacional de Proteção de Dados – ANPD avaliará a gravidade do fato ocorrido. Essa avaliação levará em conta as medidas técnicas que tenham sido adotadas para tornar os dados ininteligíveis para terceiros não autorizados ao tratamento. Após a avaliação, a ANPD poderá determinar a ampla divulgação do fato em meios de comunicação e, medidas para reverter ou mitigar os efeitos do incidente.

5. BOAS PRÁTICAS E GOVERNANÇA

A divulgação em meios de comunicação de grande circulação de riscos de vazamento de dados pessoais ou de acesso indevido ou, as notícias publicadas a esse respeito constituem significativo abalo à reputação da empresa obrigada a adotar essas medidas. Na área de seguros esse abalo reputacional fere o vínculo de confiança que é imprescindível para que o contratante escolha uma seguradora para proteger seu interesse legítimo. Evitar os riscos aos dados pessoais é uma estratégia que todas as empresas que operam na área de seguros – seguradores, corretores de seguro, prestadores de serviços e outros -, deverão adotar com especial atenção e cuidado.

Para isso, a LGPD inseriu as boas práticas e a governança como imprescindíveis para os controladores e operadores de dados pessoais no âmbito de suas competências. As boas práticas e a governança terão regras construídas a partir da consideração sobre a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

Determina a lei que as regras de boas práticas e de governança deverão estabelecer 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.

O controlador de dados pessoais avaliará a estrutura, escala e volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos riscos que poderão ser causados aos titulares de dados pessoais, para implementar programa de governança em privacidade; e, demonstrar a efetividade de seu programa de governança em privacidade a pedido da ANPD ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta.

As regras adotadas pela empresa para boas práticas e governança na área de proteção de dados pessoais deverão ser publicadas e atualizadas periodicamente e, a Autoridade Nacional de Proteção de Dados poderá reconhece-las e divulga-las quando necessário.

6. SANÇÕES APLICÁVEIS AOS AGENTES DE TRATAMENTO DE PROTEÇÃO DE DADOS

Determina a LGPD que em razão das infrações cometidas por falta de cumprimento da lei, os agentes de tratamento de dados pessoais ficarão sujeitos a sanções que poderão ser: de advertência, multa simples, multa diária, publicização da infração ou, eliminação de dados pessoais. A multa simples poderá ser fixada em até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os valores referentes a tributos, limitada, no entanto, ao total de 50 milhões de reais por infração.

A ANPD promoverá processo administrativo que viabilize a ampla defesa dos agentes de tratamento de dados pessoais e, só após o resultado é que serão aplicadas as sanções, de forma gradativa, isolada ou cumulativa e de acordo com as particularidades de cada caso concreto.

Para fixação da sanção serão levados em conta, obrigatoriamente, a gravidade e a natureza das infrações e dos direitos pessoais afetados; a boa-fé do infrator; a vantagem auferida ou pretendida pelo infrator; condição econômica do infrator; reincidência; o grau do dano; a cooperação do infrator; adoção de mecanismos de prevenção e minimização dos danos; a política de boas práticas e governança; a pronta adoção de medidas corretivas; e, a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

É importante ressaltar que a LGPD não exclui a aplicação de sanções administrativas, civis ou penais definidas no Código de Defesa do Consumidor e, também em outras leis específicas sobre o tema da proteção de dados pessoais. Essas sanções poderão ser cumuladas com aquelas aplicadas pela LGPD.

O valor arrecadado com as multas não se destina às vítimas de danos, mas ao Fundo de Defesa dos Direitos Difusos, que utilizará os valores arrecadados para efetivação de

projetos de educação e proteção nas áreas de meio ambiente, direitos do consumidor, proteção do patrimônio cultural, artístico e histórico, entre outros.

7. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A Autoridade Nacional de Proteção de Dados – ANPD é órgão da administração pública federal vinculado à Presidência da República, e tem como competências: zelar pela proteção dos dados pessoais, nos termos da legislação; zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos da LGPD; elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; promover o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na lei; deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD, as suas competências e os casos omissos; comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; e, implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a lei, entre outras funções relevantes.

A ANPD não está definida em lei como autarquia, mas poderá vir a ter essa natureza jurídica se a avaliação de sua operação ao final de dois anos de atividade, recomendar que seja adotada novo formato. Mas, independentemente disso, vai atuar como órgão regulador e fiscalizador de todos os setores econômicos que atuem com tratamento de dados e, será mais uma entidade administrativa à qual o setor de seguros terá que se reportar.

8. OPEN FINANCE, OPEN BANKING, OPEN INSURANCE E OPEN HEALTH

O setor de seguros privados no Brasil vive importantes mudanças regulatórias que poderão representar avanço para o setor, mas que precisam ser analisadas cuidadosamente à luz da Lei Geral de Proteção de Danos – LGPD.

O setor de seguros privados como todos os setores que administram recursos de terceiros, sempre foi cauteloso em relação a mudanças ou inovações, mas, nos últimos anos, a força das novas tecnologias em todas as áreas e, mais recentemente, a intensa digitalização da vida que a pandemia provocou, estimularam os órgãos reguladores e fiscalizadores do setor de seguros a ampliar as possibilidades de atuação, com o objetivo de tornar a atividade de seguros mais diversificada e, em consequência, capaz de incluir maior número de contratantes.

Seguro é um instrumento de equilíbrio social. A inclusão de maior número de pessoas que possam contratar seguros é recomendável para todas as sociedades e, é o que acontece nos países de economia central. Se as mudanças regulatórias que ocorrem no Brasil nos últimos anos forem efetivas para a inclusão de maior número de pessoas entre os contratantes de seguro e, principalmente, se essas mudanças propiciarem produtos de seguro mais flexíveis, com maior concorrência, menor preço final ao contratante e, maior facilidade para a compreensão dos instrumentos de contratação, a regulação terá atingido um estado bastante avançado, em condições de colocar o país entre aqueles em que os seguros respondem por um percentual expressivo no Produto Interno Bruto – PIB.

De 2019 para cá várias mudanças regulatórias importantes ocorreram no setor de seguros privados no Brasil e, entre elas, uma delas merece especial destaque: as regras para implantação do sistema de *open insurance.*

Open finance é a denominação que vem sendo aplicada ao sistema que reúne *open banking* e *open insurance.* As bases legais desse sistema estão na Lei n.º 13.874 de 2019, mais conhecida como Declaração de Direitos de Liberdade Econômica e, nas regras do Conselho Nacional de Seguros Privados e da Superintendência de Seguros Privados.

Há integração entre os objetivos dos reguladores de bancos e seguros para estimular a concorrência entre os agentes econômicos, ampliar as possibilidades de acesso ao mercado às pessoas conhecidas como *desbancarizadas* e, tornar os contratantes mais livres para contratar com quem lhes ofereça as melhores perspectivas. Em outras palavras, o objetivo do governo central do Brasil é atribuir maior poder aos contratantes para que façam escolhas e, com isso estimular a concorrência na criação de produtos customizados às necessidades específicas dos contratantes.

O que tornou possível o sistema *open finance* foi a popularização de *smartphones,* telefones celulares com cada vez maior capacidade computacional. O aumento de velocidade da rede mundial de computadores e a viabilidade de transmissão de maior quantidade de dados em tempo real, também contribuíram significativamente para que os telefones celulares pudessem incluir inúmeras outras funções além da original, em especial por meio de aplicativos que podem realizar infindáveis tarefas.

O Brasil ainda possui quantidade expressiva da população totalmente *desbancarizada,* sem acesso formal a instituições bancárias ou financeiras, porém, tem uma quantidade significativa da população que possui telefones celulares.

Outro aspecto importante da realidade brasileira é que os dados bancários de uma pessoa pertencem ao banco e não a ela própria, o que dificulta muito a migração de uma instituição para outra. O *open banking* se torna, então, uma medida para colocar o usuário no centro do poder de decisão, permitindo que ele partilhe seus dados como quiser e com quem quiser, de forma a obter em troca melhores condições de negociação nos diferentes produtos bancários e de seguro.

O Banco Central afirma que o objetivo do *open finance* é incentivar inovações no setor financeiro, promover aumento da concorrência e também da eficiência do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro. Entre os resultados esperados está alocada a educação financeira ou, cidadania financeira, que consiste na ampliação da compreensão dos usuários sobre os diferentes produtos bancários e de seguro, de forma a facilitar escolhas mais adequadas às diferentes necessidades.

8.1. Open Insurance

O Conselho Nacional de Seguros Privados – CNSP aprovou a Resolução n.º 415, de 2021, que define *open insurance* como *compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas no âmbito dos mercados de seguros, previdência complementar aberta e capitalização.*

Também aprovou a Circular 635, de 2021, que dispõe sobre a regulamentação das diretrizes estabelecidas pelo Conselho Nacional de Seguros Privados - CNSP para implementação do Sistema de Seguros Aberto (Open Insurance).

Alguns conceitos importantes são definidos pela regulação:

- Sociedade supervisionada: a sociedade seguradora, incluindo aquela participante exclusivamente de ambiente regulatório experimental (sandbox regulatório), a entidade aberta de previdência complementar ou a sociedade de capitalização;

- Sociedade transmissora de dados: sociedade supervisionada, participante do Open Insurance, ou sociedade iniciadora de serviço de seguro que compartilha com a sociedade receptora os dados de que trata esta Resolução;

- Sociedade receptora de dados: sociedade supervisionada, participante do Open Insurance, ou sociedade iniciadora de serviço de seguro que apresenta solicitação de compartilhamento à sociedade transmissora para recepção dos dados de que trata esta Resolução;

- Sociedade iniciadora de serviço de seguro: sociedade anônima credenciada pela Susep como participante do Open Insurance, que provê serviço de agregação de dados, painéis de informação e controle ou, como representante do cliente com consentimento dado por ele, presta serviços de iniciação de movimentação, sem deter em momento algum os recursos pagos pelo cliente, à exceção de eventual remuneração pelo serviço, ou por ele recebidos.

A sociedade iniciadora de serviço de seguro é a novidade mais marcante do novo sistema, porque não existe na atual estrutura de serviços de seguro em que a intermediação é realizada por corretores, agentes ou representantes de seguro.

As sociedades iniciadoras de serviços de seguro parecem se constituir em novo intermediário autorizado pela regulação para atuar especificamente na área de *open insurance,* com a função de orientar os clientes na organização e apresentação de dados para serem disponibilizados em ambiente seguro, na busca das melhores oportunidades de contratação para necessidades específicas.

Os objetivos do *open insurance* são definidos na regulação como: ter o cliente como principal beneficiado; tornar seguro, ágil, preciso e conveniente para os clientes o compartilhamento padronizado de dados, previsto na Lei Geral de Proteção de Dados e demais legislações que tratam do sigilo de operações financeiras, e serviços; incentivar a inovação; promover a cidadania financeira; aumentar a eficiência dos mercados de seguros privados, de previdência complementar aberta e de capitalização; promover a concorrência; e, ser interoperável com o Open Banking.

A regulação do Conselho Nacional de Seguros Privados – CNSP e da Superintendência de Seguros Privados – SUSEP, definiu, ainda, os princípios do *open insurance,* que são:

transparência; segurança e privacidade de dados e de informações compartilhados no âmbito do Open Insurance; livres iniciativa e concorrência; qualidade dos dados; tratamento não discriminatório; reciprocidade; interoperabilidade; e integração com o *open banking*.

O open insurance tem gerado muitas dúvidas entre os operadores de seguros privados em todo o país, tanto na área jurídica como nas áreas de distribuição de produtos, técnica-atuarial, financeira e de sistemas computacionais.

A primeira dúvida, é saber quais outros países do mundo já operam com *open insurance* no setor de seguros. A União Europeia está discutindo o assunto, mas ainda não implantou o sistema. E países como México, Austrália, Índia e Nova Zelândia já iniciaram operações semelhantes a esta aprovada no Brasil.

Outra questão relevante é saber quais os benefícios esperados para o cliente. O órgão regulador brasileiro explica que a expectativa é a melhoria de qualidade dos serviços prestados aos clientes, principalmente para que seja possível precificar de forma mais adequada às necessidades de cada um, além de oferecer produtos diferenciados, mais compatíveis com a diversidade da sociedade brasileira. Em poucas palavras, o compartilhamento autorizado de dados poderá oferecer maior acessibilidade a produtos de seguro, em especial para a parcela da população que ainda não contrata essa modalidade de serviços.

Em princípio, o *open insurance* parece estar destinado a seguros massificados, em especial os nichos que começaram a ser explorados pelas *insurtechs* aprovadas para operar no modelo *sandbox* e, que já são duas dezenas aprovadas em funcionamento. Não há impedimento para a atuação de seguradoras em área de não massificados, mas o *open insurance* parece estar mais focado na distribuição de seguros massificados e específicos, que serão a porta de entrada de novos contratantes.

No momento, o sistema de *open banking* já está operando e o *open insurance* ainda está em fase de implementação.

8.2. Open Health

Em fevereiro de 2022, o Ministério da Saúde no Brasil trouxe a público a intenção de implementar o sistema *open health* no país, a partir de dois pilares: financeiro e assistencial.

Para o pilar assistencial o objetivo é a implementação de prontuário médico eletrônico que permitirá aos setores público e privado da saúde organizarem dados em uma mesma plataforma, para que o usuário não necessite mais carregar seu histórico médico de um lugar para outro. As equipes de saúde autorizadas a consultar o prontuário médico eletrônico terão acesso aos dados necessários para o atendimento dos pacientes, tanto na rede pública como para aqueles que são contratantes de saúde suplementar.

A Rede Nacional de Dados em Saúde já foi aprovada e está em fase de implementação, adotando todos os cuidados para a proteção de dados conforme determinação da Lei Geral de Proteção de Dados – LGPD.

Para o pilar financeiro o objetivo do Ministério da Saúde é que os dados cadastrais e também os de utilização sejam de propriedade do usuário de planos de saúde suplementar, e que eles possam compartilhar em plataforma digital para poderem receber as melhores ofertas das diferentes seguradoras e operadoras do setor.

A ideia é que o *open health* seja organizado e funcione da mesma forma que o *open banking* e o *open insurance,* com a diferença de que as operadoras e seguradoras de saúde terão acesso a dados anonimizados dos usuários e, oferecerão seus produtos e serviços em conformidade com aquele perfil específico, sem identificação do usuário até que ele se decida ela contratação. Assim, dados como assiduidade financeira, tipos de cobertura, características de contrato e até de utilização, poderão ser disponibilizados na plataforma digital para que as partes negociem livremente as melhores coberturas e condições de pagamento, sem que haja identificação prévia do usuário.

O Ministério da Saúde acredita que com essa medida poderá evitar os ônus da intermediação desnecessária e ineficiente, aumentar a concorrência e diminuir a concentração no setor de saúde suplementar.

As operadoras e seguradoras de saúde não foram chamadas para estudar e debater o tema com o Ministério da Saúde, embora tenha sido constituída uma comissão para estudo dos aspectos técnicos e jurídicos da medida a ser aprovada. O setor privado de saúde suplementar observa os movimentos do governo federal e reage com ceticismo, seja porque não participa ativamente do debate, seja porque entende que a saúde suplementar no Brasil tem outros aspectos mais urgentes para serem solucionados e que a implementação de uma plataforma digital de negociação, depende principalmente da maturidade do consumidor para realizar escolhas e, no aspecto de educação financeira a população brasileira ainda possui deficiências que precisam ser sanadas.

O tema precisará ser reestudado e analisado quando as medidas do governo brasileiro se tornarem conhecidas, o que não aconteceu até este momento.

CONCLUSÃO

As inovações tecnológicas atingiram todas as áreas econômicas e sociais. No setor de seguros privados não poderia ser diferente e as mudanças são muito bem-vindas, em especial se atingirem os objetivos desejados: maior flexibilidade na oferta de produtos pelos seguradores, com melhores preços e, principalmente, com a inclusão de novos contratantes.

Tudo isso deverá ser concretizado com absoluto respeito à proteção de dados pessoais que só poderão ser partilhados com prévio e expresso consentimento, para a finalidade estritamente necessária e, em conformidade com as bases legais previstas na Lei Geral de Proteção de Dados.

Os sistemas abertos de negociação consubstanciados em *open finance* e que serão utilizados também pelo setor de seguros privados, poderão representar avanços positivos como menor concentração de mercado, ampliação de oferta de produtos de seguro com maior adequação às necessidades dos contratantes e, em especial, com valores que viabilizem a contratação pelas camadas de baixa renda da população brasileira que, infelizmente, ainda é a grande maioria.

Diversificação de produtos de seguro e precificação para todas as camadas de renda são desafios perseguidos há muito tempo pelo mercado brasileiro, o que poderá ser incentivado por meio do sistema de *open insurance* e *open health.* As premissas fundamentais para que isso ocorra com segurança já estão dadas pela Lei Geral de Proteção de Dados – LGPD e, se concretizarão na fiscalização e cuidados a serem adotados pela Autoridade Nacional de Proteção de Dados – ANPD.

REFERÊNCIAS BIBLIOGRÁFICAS

Blum, Renato Opice (organizador) *Proteção de Dados. Desafios e Soluções na Adequação à Lei.* Rio de Janeiro: Forense, 2020.

Guardia, Andrés F.T. Selingardi. *Teoria Geral da Proteção de Dados. O Tratamento de Dados como Relação Jurídica.* S.Paulo: Max Limonad, 2014.

Mendes, Laura Schertel; Doneda, Danilo; Sarlet, Ingo Wolfgang; Rodrigues JR. Otávio Luiz (coordenadores). Biondi, Bruno (coordenador executivo). *Tratado de Dados Pessoais.* Rio de Janeiro: Forense, 2021.

Mulholand, Caitlin (organizadora). *A LGPD e o Novo Marco Normativo no Brasil.* Porto Alegre: Arquipélago, 2020.

Puccinelli, Oscar R. *Protección de Datos de Carácter Personal.* Buenos Aires: Editoral Astrea, 2004.

Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. *Lei Geral de Proteção de Dados Pessoais e Sua Repercussão no Direito Brasileiro.* S.Paulo: Thomson Reuters Revista dos Tribunais, 2019.