CNseg

GUIA

DE BOAS PRÁTICAS DO MERCADO SEGURADOR BRASILEIRO SOBRE A PROTEÇÃO DE DADOS PESSOAIS

2ª EDIÇÃO

ÍNDICE

ÍNDICE

1

APRESENTAÇÃO

Em dezembro de 2019, a Confederação Nacional das Seguradoras (CNseg) lançou o "Guia de Boas Práticas do Mercado Segurador Brasileiro sobre Proteção de Dados Pessoais".

A referida publicação foi pioneira ao apresentar a visão de um setor produtivo sobre a LGPD, tendo sido elaborada por Grupo de Trabalho constituído por representantes das associadas, coordenado pela Superintendência Jurídica da CNseg, contando com a consultoria jurídica dos Drs. Mario Viola e Leonardo Heringer Mattos.

A LGPD foi um marco legal ao introduzir no arcabouço normativo brasileiro uma estruturação do conteúdo jurídico da proteção de dados, e, para o setor segurador, cuja atividade tem como insumo o uso de dados, os seus efeitos foram imediatos. Nesse contexto, o Guia de Boas Práticas foi concebido como instrumento de apoio às empresas do setor de seguros na fase de implementação dos dispositivos da LGPD em sua rotina diária e na relação com seus prestadores e parceiros, além de construir e consolidar no setor de seguros a cultura de respeito à proteção de dados pessoais.

Agora, em 2024, com cerca de seis anos de publicação da LGPD e diante de importantes transformações regulatórias, econômicas,

tecnológicas e sociais, apresentamos a primeira atualização deste Guia. Este trabalho reafirma o compromisso contínuo do setor com a conformidade legal e com a promoção de práticas éticas no tratamento de dados pessoais.

É importante contextualizar, que desde a publicação inicial do Guia, ocorreram importantes marcos que justificaram a sua atualização.No campo regulatório, a constituição da Autoridade Nacional de Proteção de Dados – ANPD, que publicou normas e orientações, que são norteadoras para a aplicação da lei. Até o momento, foram publicadas 06 (seis) Resoluções, 07 (sete) Guias Orientativos, 18 (dezoito) Notas Técnicas e 06 (seis) Estudos Técnicos, além de 08 (oito) Consultas Públicas e 16 (dezesseis) Tomadas de Subsídios, tendo a CNseg apresentado contribuições como entidade representativa do setor de seguros.

A proteção de dados pessoais foi ainda alçada ao direito fundamental previsto na Constituição Federal, por meio da Emenda Constitucional nº 115/2022, e o Superior Tribunal de Justiça já publicou um compêndio com os seus precedentes nesses primeiros quatro anos de vigência da LGPD.

O setor de seguros passou por uma ampla revisão das normas regulatórias promovida pela Superintendência de Seguros Privados – SUSEP, com destaque para **i)** a criação do Sistema de Registro de Operações de seguros, previdência complementar aberta, capitalização e resseguros – SRO, instituído pela Resolução CNSP nº 383/2020, que criou a obrigação de as supervisionadas efetuarem o registro de suas operações em sistemas de registro previamente homologados pela SUSEP e administrados por entidades registradoras credenciadas pela SUSEP e **ii)** o *Open Insurance* (OPIN), ambiente de 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, sempre, a partir do consentimento do cliente e entre participantes desse ecossistema.

Além disso, a pandemia acelerou a digitalização de processos e ampliou o uso de tecnologias, como a telemedicina. Ocorreu também

a popularização do uso da inteligência artificial generativa (chatgpt) bem como uma intensificação na interação em ambiente virtual nas relações sociais e econômicas, inclusive no setor de seguros.

Reconhecendo a importância do assunto e a necessidade de ter um grupo especializado e dedicado exclusivamente ao tema, a CNseg criou a Comissão da Lei Geral de Proteção de Dados Pessoais – CLGPD, que tem como missão primordial debater e avaliar os temas afetos à LGPD, bem como subsidiar as manifestações da Confederação frente à regulamentação da LGPD pela ANPD. Foi, inclusive, essa Comissão responsável por atualizar este Guia.

A atualização do referido Guia não apenas revisa e aprimora o conteúdo original, mas também incorpora novos capítulos que refletem temas atuais, como Telemetria; Decisões Automatizadas; Término do Tratamento de Dados Pessoais; *Privacy by Design; Open Insurance e Open Finance*. Assim, o Guia continua sendo uma referência para o setor.

Com este trabalho, reafirmamos o compromisso do setor segurador com a proteção de dados pessoais, a sua conformidade legal e a disseminação da cultura de proteção de dados no Brasil. O Guia de Boas Práticas permanece, assim, como uma ferramenta essencial, não apenas para auxiliar as empresas, mas para colaborar com a transparência e a confiança junto aos consumidores de seguro.

A proteção de dados é um desafio contínuo e coletivo, e este Guia atualizado reflete o esforço constante do setor segurador em contribuir para uma cultura de proteção de dados no Brasil, reafirmando o papel do setor como protagonista nesse importante desafio.

Glauce Carvalhal

Diretora Jurídica e DPO da CNseg

2

PRINCÍPIOS E NORMAS GERAIS APLICÁVEIS AO SETOR

A exemplo de outras leis brasileiras de grande alcance, como o Código de Defesa do Consumidor (Lei nº 8.078/1990), a Lei Geral de Proteção de Dados Pessoais não dispõe, via de regra, de determinações específicas para os diferentes setores econômicos. Seus dispositivos e princípios serão calibrados para a aplicação em cada setor econômico, levando-se em conta as especificidades de cada setor.

Em razão disso, este tópico apresentará fundamentos, princípios e normas gerais que deverão ser objeto de maior atenção pelas sociedades integrantes do setor de seguros.

Fundamentos da LGPD

A LGPD estabelece, no art. 2º os fundamentos da disciplina de proteção de dados pessoais, e deixa expresso o objetivo de proteger a privacidade do titular, a liberdade de expressão, de informação, de comunicação e de opinião (art. 2º, III). A LGPD também explicita seu compromisso com o desenvolvimento econômico e tecnológico e a inovação (art. 2º, V), a livre iniciativa e a livre concorrência (art. 2º, VI). Ou seja, conquanto a LGPD tenha a finalidade de assegurar o respeito à privacidade (art. 2º, I), a inviolabilidade da intimidade, da

honra e da imagem (art. 2º, IV) do titular dos dados pessoais, também assume expresso compromisso com outras relevantes garantias e direitos.

Isso demonstra que a temática alusiva à proteção de dados não é, evidentemente, uma via de mão única. O titular dos dados merece e deve ter os seus direitos respeitados, mas isso deve levar em conta outros direitos que, para permitir uma sociedade desenvolvida e próspera, também merecem a devida tutela.

É com essa perspectiva que a LGPD deve ser lida, não apenas como um diploma protecionista dos direitos dos titulares dos dados, e, sim, igualmente como uma lei indutora do desenvolvimento científico e econômico.

Princípios da LGPD

A LGPD é uma legislação principiológica, como se tornou corriqueiro no Brasil após a Constituição Federal de 1988. O Código de Defesa do Consumidor e outras leis de grande repercussão são, também, leis principiológicas que adotam a metodologia de princípios exatamente porque seus temas são complexos, sujeitos a sucessivas modificações com o passar do tempo, e os princípios direcionam a conduta a ser dada, atendendo melhor a necessidade de constante atualização.

A LGPD tem semelhança, também, com as disposições contidas no Marco Civil da Internet – Lei nº 12.695/2014 (art. 7º, VIII), e nesse sentido, positivou o **princípio da finalidade** (art. 6º, I), indicando que a *"[...] realização do tratamento [deve servir] para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades"*.

Isto é, os dados pessoais só poderão ser tratados para atender finalidades que **(i)** sejam lícitas e compatíveis com o ordenamento

jurídico; **(ii)** sejam específicas e permitam uma delimitação do objetivo do tratamento; e **(iii)** tenham sido explicitamente informadas ao titular, de modo a facilitar a sua fácil compreensão.

É necessário que haja real coerência entre o tratamento realizado e a finalidade informada ao titular, pois essa adequada pertinência constitui o **princípio da adequação** (art. 6º, II), que é um segundo princípio indissociavelmente vinculado ao primeiro e que estabelece a necessidade de *"[...] compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento"*.

O princípio da **necessidade** (art. 6º, III) é outro importante elemento positivado pela LGPD e tem especial relevância para o setor de seguros. Determina esse princípio que o tratamento de dados deverá se limitar ao mínimo necessário para o alcance da finalidade almejada, vedando que haja tratamento de dados excessivos, que sejam desnecessários e que extrapolem as finalidades do tratamento.

Assim, de acordo com a LGPD, só poderão ser tratados os dados pessoais que forem efetivamente necessários à finalidade perseguida. Estará em desacordo com a lei a prática de coletar dados pessoais excessivos, desvinculados da declarada finalidade do tratamento que será realizado.

A aplicação do princípio da necessidade requer cautela. De fato, algumas contratações do setor de seguros requerem a análise de base ampliada de dados, porém, o objetivo a ser perseguido para a conformidade com a lei é *evitar coletar e tratar dados pessoais que não estejam relacionados com a finalidade objetivada*.

O seguro auto e o seguro residencial são dois bons exemplos da aplicação do princípio da necessidade. Alguns dados são imprescindíveis para o cálculo de risco e de probabilidades de ocorrência de um sinistro; outros dados poderiam até contribuir para esses cálculos, porém, não se encontram diretamente relacionados e podem gerar controvérsias.

Por isso, é recomendável que as seguradoras façam um mapeamento dos dados que são efetivamente necessários para as suas análises, pois elas terão a obrigação de manter os registros e justificar as operações de tratamento de dados pessoais que forem realizadas (art. 37). Em outras palavras, poderá ser necessário para as seguradoras justificar a razão de terem coletado e arquivado os dados pessoais, e, se essa justificativa não for robusta e diretamente relacionada à finalidade do tratamento, por exemplo cálculos de risco e de valor de prêmio, poderá ficar caracterizada a não-conformidade com o texto da LGPD.

No que diz respeito aos direitos dos titulares dos dados pessoais, dois princípios são muito relevantes: o do livre acesso (art. 6º, IV), que garante a *"[...] consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade dos dados"*, e o princípio da qualidade dos dados (art. 6º, V), que é a *"[...] 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"*.

Isso significa dizer que a relação dos agentes de tratamento de dados com o titular deverá ser a mais transparente possível. Ao titular dos dados pessoais deverá ser assegurado, com a transparência devida (art. 6º, VI) o conhecimento acerca dos principais aspectos relacionados ao tratamento de seus dados pessoais, ressalvados a proteção dos segredos comercial e industrial e o sigilo legal. O titular de dados pessoais pode consultar seus dados a qualquer momento, mediante simples solicitação. É uma mudança de cultura na prática empresarial brasileira, porém, é uma tendência global, já praticada em países da União Europeia, por exemplo.

A LGPD contém outros princípios relacionados à **segurança dos dados** (art. 6º, VII), à **prevenção de danos** (art. 6º VIII) e à **responsabilização** (art. 6º, X). Todos são princípios que devem ser atentamente respeitados pelos agentes de tratamento, incluindo-se o setor de seguros, mercado objeto deste Guia.

Há, no entanto, um princípio que vai requerer maior cuidado do setor de seguros que é o **princípio da não discriminação (art. 6º, IX).** Compreender corretamente o alcance desse princípio poderá evi-

tar o cometimento de equívocos que podem, no limite, inviabilizar a atuação das seguradoras.

O princípio da não discriminação determina a *"impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos"*.

Merece destaque o fato de que a discriminação que a LGPD veda é aquela para fins **ilícitos ou abusivos.** Nessa medida, a seleção de riscos realizada com finalidade ética e legalmente válida fica protegida de ser considerada ilegal à vista da LGPD.

Um exemplo relevante é a precificação de seguros de automóvel ou residencial a partir de dados do CEP de residência do segurado. Não é discriminação social, mas seleção de risco com objetivo legalmente válido, porque é realidade que alguns locais são estatisticamente mais sujeitos a práticas de violência que outros. Trata-se, aliás, de consequência da inércia do Estado em garantir igualdade de índices de segurança para a população urbana e rural. Essa inércia do Estado faz com que as populações se organizem, e disso decorre que em alguns lugares há maior segurança e em outros menos. Essa realidade não pode ser ignorada no momento em que as seguradoras realizam cálculos de risco e de prêmio para organizarem fundos mutuais sustentáveis e solventes.

Especificamente no que toca ao setor de saúde suplementar, deve-se dar destaque ao disposto no §5º do art. 11 da LGPD. Uma leitura isolada e não sistemática desse dispositivo poderia levar à interpretação de que estaria vedada a utilização de dados de saúde para a subscrição de seguros saúde. Esse dispositivo, porém, deve ser lido em consonância com o que dispõe a Lei nº 9.656/98 (que versa sobre os planos e seguros privados de assistência à saúde), e aqui merece ser feita uma distinção entre seleção de riscos e análise de risco para fins de subscrição e precificação. A Lei nº 9.656/98 veda a seleção de riscos, ou seja, a possibilidade de recusa de oferecimento de cobertura a determinado proponente, porém, a mesma lei reconhece a possibilidade de precificação e de análise de riscos para fins de subscrição ao admitir que, na presença de doença preexistente, deverá ser ofertado ao proponente a

cobertura parcial temporária ou o agravo do prêmio durante o período no qual seria aplicável a cobertura parcial temporária. Portanto, é nessa linha que deve ser interpretado esse dispositivo da LGPD.

Logo, é fundamental que se ponha em perspectiva que nem toda discriminação é prejudicial e ilícita, como não é, por exemplo, aquela diretamente relacionada a subsidiar a contratação de um seguro.

Conceitos

A LGPD inaugurou no Brasil um marco legal abrangente a respeito da disciplina de proteção de dados pessoais. Por mais que já tivessem sido aprovadas algumas normas legais esparsas tratando pontualmente da matéria, não existia uma legislação que sobre ela versasse de maneira sistematizada. Por isso, preocupou-se o legislador em estabelecer a definição de alguns conceitos, de modo a facilitar a compreensão da lei.

Os principais conceitos adotados pela Lei Geral de Proteção de Dados Pessoais poderão ser encontrados no seu artigo 5º:

(I) DADO PESSOAL:
informação relacionada à pessoa natural identificada ou identificável.

Não é qualquer dado, ainda que diga respeito à pessoa natural, que será considerado como pessoal. O dado só será considerado pessoal se puder estar associado à pessoa natural identificada ou identificável.

Por outro lado, há de se registrar que o conceito legal de dado pessoal não se limita às informações descritivas sobre o indivíduo. Dado pessoal pode abranger, por exemplo, fotografias, que podem ser até mesmo do bem segurado, desde que, obviamente, contenham ele-

mentos capazes de identificar a pessoa do titular, como o número da placa de um automóvel.

É necessário que as empresas do setor de seguros estejam atentas à amplitude do conceito de dado pessoal, realizando análise detalhada em casos cujos dados possam ser enquadrados nessa categoria para evitar o descumprimento da Lei e suas consequências.

(II) DADO PESSOAL SENSÍVEL:
dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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.

Essa qualificação especial de dado pessoal sensível decorre do fato de esse tipo de dado estar associado à privacidade do titular, o que justifica inclusive maiores restrições para o seu tratamento (art. 11). São dados que quase sempre uma pessoa só revela para aqueles com quem tem vínculos de confiança e intimidade.

O dado pessoal sensível é aquele relacionado ao âmago do indivíduo, associado a elementos mais aprofundados da sua intimidade e vida privada e que, por isso, deve ser merecedor de maior proteção legal.

(III) DADO ANONIMIZADO:
dado relativo a titular que não possa ser identificado, considerando-se a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dado anonimizado é a informação que não é capaz de ser associada ao titular.

É importante destacar, porém, que essa impossibilidade de associação dos dados ao seu titular deve ser considerada mediante a utilização de fatores objetivos, tais como os custos, o tempo necessário para reverter o processo de anonimização e os meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, pois o processo de anonimização, segundo o seu conceito legal (art. 5º, XI), não exige o emprego de técnicas que tornem a reversão impossível, apenas faz alusão à *"utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo"*. Isso significa dizer que a eventual possibilidade de identificação do titular dos dados, para a qual, todavia, é necessário um grande aparato tecnológico, demandando um custo operacional elevado e um tempo considerável, não seria suficiente, por si só, para descaracterizar a natureza anônima do dado. Deve-se assegurar, contudo, que se trata de um processo de anonimização e não de pseudonimização, já que apresenta regramentos distintos na LGPD.

A compreensão do conceito de dado anonimizado é relevantíssimo para o setor de seguros, visto se tratar de dados que podem ter utilidade para fins estatísticos, podendo servir, por exemplo, para áreas atuariais, estudos de precificação etc. e pelo fato de tais dados não se enquadrarem na definição de dado pessoal e, como consequência, não estarem, a partir da anonimização, sujeitos ao regime da LGPD, conforme preceitua o art. 12 da Lei.

(IV) BANCO DE DADOS:
conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Banco de dados inclui não apenas os dados tratados por meios eletrônicos, mas também aqueles que empregam suporte físico, como fichários, livros de registro, documentos impressos (apólices, propostas de seguro, relatórios de sinistro), entre outros.

(V) TITULAR:
pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

O titular dos dados pessoais, de forma coerente com o que dispõe o art. 1º da Lei, será sempre uma pessoa natural. A pessoa jurídica, segundo os preceitos contidos na LGPD, não é titular de dados pessoais e, portanto, o tratamento de dados relativos a pessoas jurídicas não está submetido ao regime previsto na LGPD.

(VI) CONTROLADOR:
pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

(VII) OPERADOR:
pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Dada a utilidade de compreender a diferenciação entre a figura do controlador e a do operador, especialmente por conta dos limites da responsabilização de cada um (art. 42 e seguintes), optou-se por tratar de ambos os conceitos de forma conjunta.

Primeiramente, convém salientar que as tarefas do controlador e do operador poderão ser executadas tanto por pessoa física como por pessoa jurídica; a Lei admite textualmente essas possibilidades. Entretanto, é preciso ressaltar que a pessoa física só será considerada agente de tratamento de dados pessoais quando estiver executando a operação em nome próprio e para fins econômicos, seja para atender às suas próprias necessidades (hipótese em que será controladora) ou as de um controlador (hipótese em que será operadora). Se o tratamento for realizado pela pessoa física no contexto de uma relação de trabalho, o empregado não deve ser considerado agente de tratamento, pois, nessa hipótese, a operação será realizada em nome e por determinação de seu empregador, que deverá, para todos os fins, ser considerado o agente do tratamento.

Por outro lado, é preciso considerar que, à míngua de vedação expressa, as operações de tratamento de dados pessoais também podem ser executadas conjuntamente e com o compartilhamento de responsabilidade por mais de um agente de tratamento. No setor de seguros, por exemplo, a atuação de mais de um agente como controlador poderá ocorrer na hipótese de resseguro ou de cosseguro.

Portanto, é possível que o tratamento de dados pessoais envolva mais de um controlador e/ou mais de um operador (suboperador).

A **diferença** entre a figura do controlador e a do operador reside no poder de decisão acerca dos elementos essenciais do tratamento de dados. Enquanto **ao controlador cabe o papel de tomar as decisões a respeito dos limites e dos parâmetros para que seja realizado o tratamento de dados pessoais**, ao operador **cabe o papel de realizar o tratamento de dados em nome do controlador.**

Em resumo, cabe ao controlador tomar as principais decisões sobre o tratamento a ser realizado e cabe ao operador cumprir essas determinações. Há responsabilidade solidária do controlador e do operador em algumas situações no cumprimento da legislação de proteção de dados pessoais, nos termos do artigo 42, § 1º, I da Lei.

Logo, o que diferenciará o controlador do operador será o poder de decisão a respeito dos elementos essenciais do tratamento de dados pessoais.

(VIII) 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, embora seja uma figura muito relevante para assegurar o adequado cumprimento da LGPD, não é agente de tratamento de dados (art. 5º, IX).

O papel do encarregado é servir como o elo de comunicação entre o titular dos dados, o controlador e a Autoridade Nacional de Proteção de Dados, competindo-lhe, também, *"[...] aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências" (art. 41, §2º, I), "[...] receber comunicações da autoridade nacional e adotar providências" (art. 41, §2º, II), "[...] orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais" (art. 41, § 2º, III) e "[...] executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares" (art. 41, §2º, IV).*

Para desempenhar adequadamente essas relevantes atribuições, o encarregado deve possuir qualificação profissional compatível e ter liberdade e recursos (materiais e humanos) para a realização de suas atividades. Além disso, é necessário que a indicação do encarregado seja formal (ato de designação, contrato de prestação de serviço etc.), e que as informações para contato e identidade sejam mantidas atualizadas e divulgadas publicamente em local de destaque e de fácil acesso, no sítio eletrônico do agente de tratamento, e que lhe seja designado também formalmente um substituto para que

possa exercer suas funções nas ausências, impedimentos e vacâncias do encarregado.[1]

O encarregado pode ser tanto uma pessoa natural como jurídica. Sendo o encarregado uma pessoa natural, ele também pode ser tanto um empregado do controlador como um agente externo. Com isso, as empresas do setor de seguros poderão optar pela indicação de um empregado ou representante da empresa como seu encarregado ou contratar um prestador de serviço terceirizado para assumir essa responsabilidade (escritório de advocacia, consultoria especializada etc.).

O papel do encarregado é extremamente relevante, cabendo a ele zelar para que o controlador cumpra e faça cumprir na empresa todas as determinações da LGPD. Dada a sua importância, esse tema foi objeto de tratamento pela ANPD, através da Resolução CD/ANPD nº 18, de 16 de julho de 2024.

(IX) CONSENTIMENTO:
manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Elemento de suma importância para a aplicação da LGPD é a compreensão do conceito de consentimento. A Lei consigna que consentimento é a manifestação *"livre, informada e inequívoca"* da concordância do titular quanto ao tratamento de seus dados pessoais.

1 Resolução CD/ANPD Nº 18, DE 16 DE JULHO DE 2024. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074

Como se observa, a Lei não exige que o consentimento seja expresso, o que permite que seja concedido pela simples aceitação dos termos e condições de uso de um site, por exemplo. É possível também que o consentimento seja dado através da marcação de "x" em um formulário. Em ambas as situações, devem existir finalidades determinadas, não sendo admitidas autorizações genéricas para o tratamento de dados pessoais. Isso não impede, ainda, que sejam considerados formatos específicos para o consentimento previstos em outros instrumentos, como, por exemplo, o Código de Ética Médica. Aliás, a própria LGPD (art. 8º) dispõe que o consentimento deve ser fornecido por escrito ou *"por outro meio que demonstre a manifestação de vontade do titular"*.

Independentemente do meio que vier a ser utilizado para a obtenção do consentimento do titular dos dados, ele deve ser livre, informado e inequívoco, o que significa dizer que: **(i)** precisa ser obtido sem ameaças de consequências negativas e sem que haja intervenção do controlador capaz de macular a livre manifestação de vontade do titular; **(ii)** deverão ser prestadas informações a respeito do tratamento que será realizado; e **(iii)** a concordância do titular com o tratamento de seus dados pessoais deve exprimir a manifestação clara e inequívoca de sua vontade, não sendo admitido o consentimento tácito.

Outro ponto a ser considerado sobre esse conceito diz respeito à existência de um aparente conflito entre os requisitos de validade do consentimento presentes na LGPD e no Marco Civil da Internet quando o acesso ocorre por meio da internet, o qual, em seu art. 7º, IX, faz menção à necessidade de *"consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais"*.

Apesar de a LGPD ser norma geral, há razoáveis argumentos para justificar a sua aplicação preferencialmente em relação ao Marco Ci-

vil da Internet nesse particular. Os argumentos relevantes são: **(a)** a LGPD, apesar de ser lei geral, regula de forma específica o consentimento, procurando discipliná-lo com detalhamento e minúcias, de forma que não pode ser comparada ao tratamento que lhe dispensa o Marco Civil da Internet, podendo, portanto, ser identificada como a norma específica sobre consentimento no ordenamento pátrio; **(b)** no seu artigo 1º, a LGPD deixa clara a sua aplicação, *"inclusive nos meios digitais"*, fazendo esvanecer a pretensão de uma primazia absoluta e apriorística do Marco Civil da Internet em ambiente digital e na Internet; e, por fim, **(c)** a LGPD procura concretizar valores constitucionais e direitos fundamentais, alguns dos quais (direito à privacidade e liberdade) se corporificam e se concretizam na noção de autodeterminação informativa, um dos fundamentos da LGPD, pela qual o titular tem uma série de instrumentos e meios de tutela à sua disposição para efetivar suas opções, seja por escolha literal ou pelo cumprimento de legítimas expectativas a respeito do uso de seus dados pessoais por terceiros.

A LGPD decorre integralmente de dispositivos constitucionais de proteção à pessoa e, consequentemente, a seus dados. O Marco Civil da Internet não está fundamentado em direitos de natureza constitucional. Assim, é possível afirmar que as medidas de caráter preventivo e de direitos subjetivos da LGPD devem prevalecer em casos de conflito com o Marco Civil da Internet. Além disso, **a LGPD proporciona igualmente a utilização de outras bases legais autorizativas** que não o consentimento do titular, já que essa base legal não se sobrepõe às demais, e que podem ser legitimamente **aplicáveis ao tratamento de dados pessoais por meio da internet.**

Cabe registrar, finalmente, que o consentimento além de poder ser revogado a qualquer tempo pelo titular de dados pessoais (art. 8º, §5º) é concedido para uma finalidade determinada (específica). Destaque-se, contudo, que a LGPD trata o consentimento como uma das hipóteses autorizativas para o tratamento de dados pessoais, sem qualquer precedência em relação às demais hipóteses auto-

rizativas previstas na LGPD, **não havendo hierarquia entre as bases legais previstas na LGPD,** conforme será tratado neste Guia de Boas Práticas no item dedicado às bases legais para o tratamento de dados pessoais.

(X) TRANSFERÊNCIA INTERNACIONAL DE DADOS:
transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

(XI) USO COMPARTILHADO DE DADOS:
comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos ou entre entes privados.

Esses conceitos são relevantes na medida em que um simples armazenamento de dados na nuvem poderá caracterizar, a depender da localização do servidor, uma transferência internacional de dados, o que demandará o cumprimento de regras específicas (art. 33 e seguintes).

É importante que o setor de seguros dedique a devida atenção para esses conceitos, de forma a capacitar todos os colaboradores e prestadores de serviços para evitar que sejam realizadas operações que

caracterizem o compartilhamento de dados pessoais em desacordo com a LGPD.

(XII) AUTORIDADE NACIONAL:
órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

A Autoridade Nacional de Proteção de Dados (ANPD) é uma autarquia de natureza especial, dotada de autonomia técnica e decisória, incumbida da competência de zelar, implementar e fiscalizar o cumprimento da LGPD, observada a composição e as atribuições descritas nos artigos 55-A e seguintes da Lei.

Bases legais de tratamento de dados pessoais

Para o setor de seguros, além do consentimento, poderão ser utilizadas outras bases legais adequadas para conferir legalidade ao tratamento de dados pessoais. Grande parte dos tratamentos de dados será licitamente realizada pelas empresas desse setor, independentemente do consentimento do titular, observadas as obrigações previstas na LGPD e demais normas aplicáveis ao setor.

As empresas do setor de seguros se submetem a variadas regras legais e regulatórias e devem cumprir obrigações que eventualmente poderão exigir o tratamento de dados pessoais de seus segurados. Logo, quando o **tratamento de dados tiver por finalidade o cumprimento de obrigação legal ou regulatória pelo controlador**, a base legal adequada não será **o consentimento do titular** (art. 7º, II), como nas hipóteses previstas pelas normas sobre guarda de dados e documentos, prevenção à lavagem de dinheiro e controles internos para a prevenção à fraude, apenas para citar alguns exemplos.

Todavia, dada a natureza protetiva da norma, é recomendável que no momento inicial da contratação seja feita a comunicação ao titular para informá-lo de que seus dados pessoais poderão ser compartilhados com órgãos controladores da atividade de seguros, para fins de cumprimento de obrigações legais ou regulatórias. Essa informação prévia ao titular dos dados vai conferir maior transparência às operações de tratamento de dados pessoais realizadas pelo setor de seguros.

Também é dispensado o consentimento prévio do titular de dados quando a finalidade for *"[...] a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais"* (art. 7º, IV). Os estudos por órgãos de pesquisa são essenciais para o desenvolvimento tecnológico e de inovação, razões pelas quais é pertinente que tratamentos de dados com o objetivo de realização de pesquisa sejam legitimados pela lei. É importante lembrar que a LGPD conceitua como órgão de pesquisa o *"órgão ou entidade da administração púbica direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico"*. Considerando as características de (a) ausência de fins lucrativos e (b) necessidade de ter em seu objeto social a pesquisa básica e/ou aplicada de caráter histórico, científico ou estatístico, as empresas do setor de seguros não se enquadram nessa definição.

Também é autorizado o tratamento de dados pessoais na hipótese de a operação ter por finalidade *"[...] a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados"* (art. 7º, V). Essa base legal tem especial importância para o setor de seguros, que necessita realizar análises preliminares para subsidiar a contratação (conhecimento do risco), como também para cumprir o contrato, como na hipótese da regulação de um sinistro, do fornecimento de assistência 24 horas, da inspeção de risco etc.

Além disso, essas hipóteses não eliminam a necessidade de o controlador observar no tratamento de dados pessoais os princípios estabelecidos no art. 6º da Lei, em especial o da necessidade e o da adequação, a fim de evitar que ocorra o tratamento de dados excessivos, sob o pretexto de estar objetivando o cumprimento de um contrato.

O tratamento de dados também é possível quando tiver por finalidade **subsidiar o exercício regular de direitos em processo judicial, administrativo ou arbitral** (art. 7º, VI).

Trata-se de relevante previsão legal, pois não seria razoável que uma parte ficasse privada de legitimamente se defender, tendo que depender do consentimento (que provavelmente jamais seria dado) da parte adversa para apresentar determinadas provas ou informações, em defesa de seus interesses. O dispositivo está em consonância com as determinações constitucionais de direito à ampla defesa e *ao contraditório e* terá especial relevo para os departamentos jurídicos, dada a possibilidade de tratamento de dados pessoais para fins de utilização em processos, sejam eles judiciais, administrativos ou arbitrais.

Igualmente podem ser tratados os dados pessoais que tenham por finalidade *"[...] a proteção da vida ou da incolumidade física do titular ou de terceiro"* (art. 7º, VII) e *"[...] para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária"* (art. 7º, VIII), sendo essas as bases legais que autorizam o tratamento. Essas hipóteses guardam certa similitude, pois versam sobre o tratamento de dados pessoais visando salvaguardar os interesses do próprio titular dos dados. Essas duas hipóteses estão relacionadas ao setor de saúde suplementar, já que muitas vezes se mostra necessário o tratamento de dados pessoais dos segurados ou dos beneficiários de seguros saúde, sem o consentimento desses, a fim de que determinado tratamento ou procedimento médico seja autorizado pela seguradora ou operadora de saúde e, consequentemente, realizado. O mesmo pode valer para o resgate de um segurado envolvido em um sinistro de seguro automóvel ou mesmo do seguro DPVAT.

A ANS, por meio da Nota Técnica N° 3/2019/GEPIN/DIRAD-DIDES/DIDES, reconhece que:

> *"A expressão 'serviços de saúde' foi incluída por alteração feita pela Lei n° 13.853, de 2019, claramente contemplando gestores públicos e privados de saúde, como as operadoras de planos privados de assistência à saúde, não apenas no atendimento assistencial, mas também na gestão do cuidado. É possível, portanto, vislumbrar que são admitidos os seguintes tratamentos de dados sem o consentimento do titular:*
>
> - *compartilhamento de registros de saúde com os médicos assistentes e outros prestadores de serviços de saúde para melhorar o cuidado e o resultado em saúde para o paciente; utilização de informações de saúde por gestores de sistemas de saúde públicos ou privados para a condução de programas de promoção de saúde e de prevenção de doenças, bem como para o direcionamento dos pacientes para prestadores mais adequados para seus quadros; (...)"*[2] Outra hipótese possível na lei para o tratamento de dados pessoais ocorrerá *"quando [for] 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"* (art. 7°, IX), desde que o tratamento seja destinado a atender a *"finalidades legítimas, consideradas a partir de situações concretas"* (art. 10).

---

2 Nota Técnica N° 3/2019/GEPIN/DIRAD-DIDES/DIDES. 2019. Disponível em: https://www.sbac.org.br/wp-content/uploads/2019/12/Nota-Te%CC%81cnica-sobre-LGPD.pdf . Acesso em: 07.07.2021.

A LGPD não precisou quais seriam esses "interesses legítimos" do controlador ou de terceiro que justificariam o tratamento de dados. Não obstante, respaldados nas disposições da própria LGPD, pode-se afirmar que é lícito o tratamento de dados pessoais fundado no legítimo interesse do controlador quando tiver por finalidade o *"[...] apoio e promoção de atividades do controlador"* (art. 10, I), como seria o caso, por exemplo, de oferta de produtos e serviços. O mesmo pode se dizer com relação ao tratamento destinado à *"[...] proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais"* (art. 10, II). Igualmente se mostra evidente o legítimo interesse na hipótese de tratamentos de dados com vistas à prevenção e combate à fraude securitária, tema esse de vital importância para o setor de seguros, o que, aliás, já restou pacificado na experiência da União Europeia, que muito inspirou a lei[3] brasileira. **Destaque-se que, na hipótese de existirem normas regulatórias que contemplem um tratamento de dados que normalmente decorreria de um interesse legítimo das empresas do setor de seguros, como a norma sobre controles internos específicos para a prevenção contra fraudes, a base legal passaria a ser aquela do inciso II do art. 7º e não mais a do inciso IX do mesmo artigo da LGPD. De todo modo, ainda nesses casos, eventuais tratamentos de dados que não estivessem autorizados por uma norma regulatória, mas que fossem necessários ao combate e prevenção à fraude em seguros, poderiam ter lugar com base no interesse legítimo.**

3 Grupo de Trabalho do Artigo 29 para a proteção de dados pessoais. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na acepção do artigo 7.º da Diretiva 95/46/CE (adotada em 09.04.2014). Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf. Acesso em: 14.10.2019. P. 39.

Outro relevante aspecto a ser considerado no uso do interesse legítimo como base legal é a necessidade de o controlador avaliar a proporcionalidade do tratamento de dados antes de realizá-lo. Para ser legítimo, é preciso que o interesse do controlador ou do terceiro seja proporcional aos direitos e às legítimas expectativas do titular dos dados.

O tratamento de dados pode destinar-se, ainda, *"[...] para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente"* (art. 7°, X). Também nessa hipótese dispensa-se o consentimento do titular dos dados, como, aliás, já ocorre atualmente, com fundamento nas disposições do Código de Defesa do Consumidor.

Derradeiramente, poderá ocorrer o tratamento sem o consentimento quando se tratar de dados pessoais cujo acesso é público (art. 7°, § 3°) ou, que foram tornados manifestamente públicos pelo próprio titular (art. 7°, § 4°).

É indispensável que se leve em consideração que, além da identificação de uma base legal que autorize o tratamento de dados pessoais, os agentes de tratamento deverão ainda dar cumprimento às demais obrigações previstas na LGPD, *"[...] especialmente da observância dos princípios gerais e da garantia dos direitos do titular"* (art. 7°, §6°).

Bases legais de tratamento de dados pessoais sensíveis

Os dados pessoais sensíveis também poderão ser tratados com base no consentimento do titular. Contudo, diferentemente do que é previsto para o tratamento de dados em geral, o consentimento que legitima o tratamento de dados sensíveis, sempre que necessário, **tem que ser específico, inequívoco, destacado e, ainda, para finalidades determinadas** (art. 11, I).

É necessário, assim, que haja clareza nas informações que serão passadas ao titular a respeito do tratamento que será feito com os seus

dados pessoais sensíveis – assim como no caso de dados pessoais não sensíveis –, sendo recomendável que o setor de seguros faça constar esses esclarecimentos em suas políticas de privacidade.

Os dados pessoais sensíveis também poderão ser tratados com fundamento em uma das outras bases legais previstas na legislação, como na hipótese de cumprimento de obrigação legal ou regulatória pelo controlador (art. 11, II, "a"); realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis (art. 11, II, "c"); exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (art. 11, II, "d"); proteção da vida ou da incolumidade física do titular ou de terceiro (art. 11, II, "e"); tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 11, II, "f"); e garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (art. 11, II, "g"), hipóteses essas muito semelhantes – mas não idênticas – àquelas previstas para o tratamento de dados pessoais em geral. O tratamento de dados pessoais sensíveis com base em normas regulatórias expedidas tanto pela SUSEP (Superintendência de Seguros Privados) quanto pela ANS (Agência Nacional de Saúde Suplementar) é decorrente do cumprimento de uma obrigação regulatória do controlador, sendo essa a base legal a ser utilizada, portanto, dispensa o consentimento do titular do dado.

Ao contrário do que acontece com os dados pessoais em geral, não há previsão específica na LGPD para que seja realizado o tratamento de dados pessoais sensíveis com a finalidade de viabilizar a execução de contrato ou de procedimentos preliminares relacionados ao contrato do qual seja parte o titular.

A LGPD, no entanto, permite o tratamento de dados pessoais sensíveis com fundamento no exercício regular de direitos, **inclusive em contrato** e em processo judicial, administrativo e arbitral (art. 11, II, "d"). Ou seja, haverá hipótese em que o tratamento de dados pessoais sensíveis será legítimo, independentemente de ter ha-

vido o consentimento do titular, quando se destinar ao exercício regular de um direito relacionado a um contrato, por exemplo. Trata-se de situação ligeiramente diversa daquela prevista no art. 7°, V, da LGPD, aplicável ao tratamento de dados pessoais em geral, pois no caso dos dados pessoais sensíveis não será a mera execução do contrato que legitimará o tratamento, mas o exercício de um direito a ele vinculado.

Por exemplo, no caso do seguro saúde ou seguro de vida, a necessidade de coleta de informações sensíveis poderá se justificar para concretizar o exercício regular de direitos da seguradora (controladora), já que sem o tratamento de tais dados poderá não ser possível entregar a prestação que lhe compete decorrente da relação contratual, como o ressarcimento de despesas médicas no seguro saúde ou o pagamento de indenização por algum tipo de invalidez decorrente de acidente ou doença nos seguros de pessoas. Nesses casos, a seguradora não tem só o dever de cumprir a obrigação contratual, mas também o direito de a adimplir (art. 304 do Código Civil).

Vale destacar, contudo, que o requisito para o tratamento de dados com base no exercício regular de direitos em sede contratual não se confunde com os interesses legítimos do controlador ou de terceiros. Como se trata de dados sensíveis, aqui a legislação **impõe um controle maior sobre o que efetivamente poderia contar como requisito que chancele o tratamento, incluindo a análise sobre**: **(i)** a existência de um direito envolvido no caso; **(ii)** se o exercício desse direito é regular (e não abusivo); e **(iii)** se esse direito decorre de uma relação contratual.

Por outro lado, verifica-se que também não há previsão legal para que seja realizado o tratamento de dados pessoais sensíveis com a justificativa de atender ao legítimo interesse do controlador, como é permitido para os dados pessoais em geral (art. 7°, IX).

Não obstante, será possível se valer do exercício regular de um direito em sede contratual como base legal para o tratamento de dados em algumas hipóteses, por exemplo, na prevenção e combate

à fraude, porque prevenir e combater a fraude em seguros, mais do que um direito da sociedade seguradora, é um dever, como entidade encarregada de proteger a mutualidade representada por toda a massa de segurados e em decorrência de determinações legais e regulatórias específicas para essa finalidade.

Essa regra poderá ser muito útil especialmente para os segmentos de seguro de vida, de saúde e de previdência complementar que, com regular frequência, precisarão realizar o tratamento de dados pessoais sensíveis para prevenir a tentativa de fraudes.

A LGPD permite, ainda, o tratamento de dados sensíveis sem fornecimento do consentimento do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos para fins de garantir a prevenção à fraude e segurança (art. 11, II, "g"). De se destacar, contudo, que essa possibilidade de tratamento de dados sensíveis para garantia de prevenção à fraude se aplica apenas a processos de identificação e autenticação de cadastro. Isso incluiria, por exemplo, os tratamentos de dados necessários à gravação de voz para confirmação de identidade do titular do dado em solicitação de modificação da cobertura securitária contratada ou a exigência para atendimento médico-hospitalar com a utilização de plano de assistência à saúde em que o segurado/beneficiário colocasse o seu polegar em um leitor biométrico para confirmar sua identidade, a fim de evitar que outra pessoa utilize a cobertura securitária em seu lugar.

Quanto aos dados pessoais sensíveis referentes à saúde, ainda deve ser considerada a vedação para que haja a sua comunicação ou uso compartilhado entre controladores com o objetivo de obtenção de vantagem econômica (art. 11, § 4º). Essa vedação, entretanto, é excetuada nas hipóteses em que o tratamento é destinado à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia em benefício dos interesses dos titulares de dados (art. 11, § 4º), também para permitir a portabilidade de dados quando solicitada pelo titular (art. 11, §4º, I) ou para possibilitar

as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de saúde (art. 11, §4º, II).

Por fim, cumpre chamar a atenção para outra regra restritiva ao tratamento de dados de saúde, cujo conhecimento é de extrema relevância para o setor de seguros, pois veda *"[...] às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários" (art. 11. §5º).*

Essa determinação legal está em consonância com a Súmula Normativa nº 27/2015 da ANS, que estabelece vedação à *"prática de seleção de riscos pelas operadoras de plano de saúde na contratação de qualquer modalidade de plano privado de assistência à saúde"*.

A súmula normativa se refere à restrição à prática de seleção de riscos ao ingresso de beneficiários em razão da idade ou de serem portadores de deficiência, sendo que qualquer intepretação que expandisse tal vedação seria ilegal. Aqui, conforme já destacado neste Guia ao final do tópico que trata dos princípios da LGPD, há de se interpretar esse dispositivo em consonância com a Lei nº 9.656/98, que em seu art. 11 reconhece a possibilidade de se estabelecer cobertura parcial temporária ou o agravamento de prêmios em razão da pré-existência de doenças, o que seria inviável caso ocorresse uma vedação ampla e irrestrita para o tratamento de dados na contratação. Portanto, seleção de riscos para fins de não oferecimento de cobertura em seguro saúde é vedada pelo dispositivo em questão, mas não a análise de risco para fins de precificação (agravo do prêmio) ou para o estabelecimento de cobertura parcial temporária, no caso de identificação de preexistência de alguma doença, o que, como consequência, autoriza o tratamento de dados sensíveis referentes à saúde do beneficiário ou do segurado para essas finalidades.

É importante destacar, ainda, que nem toda comunicação ou uso compartilhado de dados sensíveis referentes à saúde terá escopo de obter vantagem econômica. Um exemplo de uso compar-

tilhado com finalidade não econômica é justamente o combate e a prevenção à fraude contra o seguro. Impedir que seguradoras compartilhem dados de sinistros envolvendo informações de saúde de segurados inviabilizaria o combate à fraude contra o seguro, em detrimento não apenas da massa de segurados, mas de toda a sociedade. Na atualidade, é sabido que existem grupos que atuam em sistemas de fraude contra seguros, seja no fornecimento de materiais ou dispositivos médico implantáveis, seja no fornecimento de tratamento estético ou de emagrecimento fantasiados de tratamentos médicos para viabilizar o reembolso ou o custeio pela operadora de saúde suplementar. Nesses casos, não há dúvida de que o combate à fraude e a preservação dos fundos mutuais impõem a comunicação e uso compartilhado de dados sensíveis, inclusive para denúncia junto ao órgão regulador e às autoridades estatais incumbidas de coibir e punir fraudes. Ademais, a experiência europeia reconhece que *"Um prestador de serviços pode ter um interesse comercial legítimo em assegurar que os seus clientes não utilizem o serviço de forma abusiva (ou não consigam obter serviços sem pagar) e, ao mesmo tempo, os clientes da empresa,* ***os contribuintes e o público em geral têm igualmente um interesse legítimo em assegurar que as atividades fraudulentas, quando ocorram, sejam desencorajadas e detectadas".*** [4]

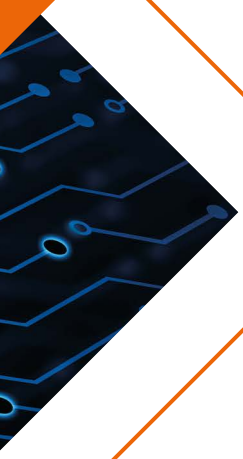
Assim, ressalvadas essas mencionadas particularidades, pode-se dizer que as bases legais de tratamento dos dados pessoais em geral são semelhantes àquelas aplicáveis aos dados pessoais sensíveis.

Outro ponto a ser observado sobre o tratamento de dados é o destaque diferenciado que a LGPD dá aos dados de crianças e adolescentes. O art.14 da Lei estabelece critério para o tratamento de

4 Grupo de Trabalho do Artigo 29 para a Proteção de Dados Pessoais. Op. cit. P. 54-55.

dados desse público, que deverá ser visto com cautela pelo setor de seguros. Referido dispositivo prevê que o tratamento de dados de crianças e adolescentes deverá ser realizado em seu melhor interesse. O seu parágrafo primeiro acrescenta, ainda, que o tratamento de dados pessoais de crianças deverá ser realizado mediante consentimento específico e em destaque, dado por pelo menos um de seus pais ou responsável legal. No entanto, considerando que esse público é recorrente nos contratos de seguro, seja como dependentes, beneficiários ou como participantes de planos de previdência complementar aberta, mostra-se evidente que o consentimento não é a única base legal para o tratamento de seus dados, sob pena de inviabilizar as operações do setor de seguros que envolverem crianças ou adolescentes. Nesse sentido, a ANPD publicou o Enunciado nº 01/2023, que estabelece que "O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei."

Diante disso, é necessário entender que, considerando o interesse do titular do contrato de seguros, saúde suplementar, previdência complementar ou titular de título de capitalização em promover a prestação de serviços ao seu dependente ou beneficiário (ou até ser o próprio, no caso de participante de plano de previdência complementar), a mesma base autorizativa deverá ser utilizada, ou seja, execução do contrato e/ou exercício regular de direitos, por exemplo, cabendo às empresas de seguros dar ciência às crianças e adolescentes sobre o tratamento de seus dados pessoais *"[...] de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança"* (art. 14, § 6º da LGPD).



3

ETAPAS DA OPERAÇÃO

Como forma de tornar mais facilmente compreensível a correlação entre os princípios e normas gerais da LGPD e as atividades das empresas do setor de seguros, serão analisadas a seguir as regras que poderão ser utilizadas para respaldar algumas das principais etapas das operações cotidianamente realizadas pelo setor de seguros.

Antes, porém, deve ser compreendido que, nos tratamentos de dados pessoais realizados pelo setor de seguros nas etapas das operações que serão a seguir descritas, atuam como **controladoras**, uma vez que realizam esses tratamentos em nome próprio para atender as suas necessidades e/ou obrigações (legais, regulatórias ou contratuais).

- **PROSPECÇÃO** – abrange o conjunto de atividades desempenhadas por uma seguradora (aqui entendida também como a entidade de previdência complementar aberta, a seguradora de saúde suplementar e a empresa de capitalização) para identificar seus clientes e potenciais clientes, definir e desenvolver os produtos que eles desejam adquirir e para vender e distribuir esses produtos aos clientes. Consulta de bases de dados com informações sobre potenciais clientes.

Na etapa de prospecção, o tratamento de dados terá como finalidade a realização de estudos que permitirão o desenvolvimento de produtos e a identificação de possíveis clientes.

Uma primeira fase dessa etapa que consistirá na realização de estudos estatísticos, mercadológicos etc., destinados ao desenvolvimento de produtos, envolverá a análise de dados que podem estar anonimizados, o que dispensaria o cumprimento das obrigações estabelecidas pela LGPD (art. 12). De todo modo, caso a empresa realize o tratamento de dados pessoais nessa fase, deverá observar as regras previstas na LGPD e identificar uma base autorizativa para o tratamento de dados aplicável ao caso.

Após desenvolvido o produto, igualmente é possível que surja a necessidade de realizar o tratamento de dados pessoais e não apenas de dados anonimizados, com o objetivo de identificar perfis de potenciais clientes. Nesse caso, seria igualmente necessário associar o tratamento dos dados a alguma base legal que o legitime.

Nessa hipótese, o tratamento de dados poderá ser justificado no legítimo interesse do controlador, especialmente em razão da regra prevista no art. 10, I, da LGPD, que prevê que o legítimo interesse poderá estar associado ao apoio e promoção das atividades do controlador.

Todavia, é importante realizar teste de proporcionalidade para avaliar se o legítimo interesse é cabível na situação específica, especialmente considerando os dados a serem tratados para essa finalidade. Nessa linha, uma opção seria facultar ao titular a possibilidade de não ter seus dados tratados para a oferta de novos produtos ou serviços, por seu expresso requerimento, em um regime de *opt out* do tratamento de dados com base no interesse legítimo.

ANGARIAÇÃO DE PROPOSTAS – é o processo de selecionar pessoas que querem adquirir cobertura de seguro e reunir informações sobre elas. Estabelecida a necessidade do seguro, o corretor ou o proponente preenche uma proposta e a submete à segurado-

ra. Nesse tema, especial atenção deve ser dada aos questionários relativos às condições de saúde do proponente, inclusive sobre exames médicos, se houver, pertinentes aos seguros de pessoa e seguros de saúde.

Na angariação da proposta, a coleta de dados terá o propósito de permitir a contratação do seguro, ou seja, será aplicável a regra autorizativa contida no artigo 7º, V, da LGPD.

Assim, é indiscutível que nessa etapa da operação o tratamento de dados pessoais será lícito, sem a necessidade do consentimento do titular. Todavia, é preciso ressaltar que o objetivo de subsidiar uma contratação legitimará a operação de tratamento que disser respeito a dados pessoais em geral, não se aplicando aos dados sensíveis.

Para os dados pessoais sensíveis, coletados para tornar possível a contratação, deverá ser buscada outra base legal, que poderá ser o consentimento ou mesmo o exercício regular de um direito em contrato (art. 11, I e art. 11, II, alínea "d"). Sem prejuízo dessas observações, é importante mencionar que nessa ou em qualquer outra etapa da operação não haverá necessidade de obtenção do consentimento do titular para a coleta de dados (mesmo os de natureza sensível) quando forem destinados ao cumprimento de obrigação legal ou regulatória do controlador (art. 7º, II e art. 11, II, "a").

CORRETOR DE SEGURO – o corretor tem mandato legal para assinar proposta em nome do proponente, mas com ele não se confunde. Que tipo de informações pode ser entregue ao corretor de seguros e como se relacionar com ele na troca de dados pessoais é questão relevante.

O corretor de seguros, enquanto intermediário do pretendente à contratação do seguro, tem poderes de representação para a apresentação da proposta, para negociar reajustes, para a renovação de vigência etc.

Quanto à troca de dados entre a seguradora e o pretenso segurado, especialmente quando se tratar de dados pessoais sensíveis, é recomendável que seja feito diretamente na pessoa do titular para evitar a possibilidade de caracterização de compartilhamento em desconformidade com o § 4º do art. 11 da LGPD.

ESTIPULANTE – nos seguros coletivos, o grupo segurado é representado pelo estipulante. Essa entidade tem acesso aos dados pessoais dos proponentes e faz a intermediação entre o grupo segurado e a seguradora.

Nesse caso, deve-se observar as limitações da representação do estipulante, que conquanto possa fazer as vezes do pretenso segurado para firmar a contratação em si, negociar ajustes, para a renovação de vigência, para solicitar a movimentação de segurados etc, não o representa para outros fins.[5] Destaque-se, contudo, que *"[n]os casos de seguros legalmente obrigatórios, o estipulante equipara-se ao segurado para os efeitos de contratação e manutenção do seguro"*.[6] Além disso, a Resolução CNSP nº 434, de 17 de dezembro de 2021, prevê, entre as obrigações do estipulante, as de *"[...] fornecer à sociedade seguradora todas as informações necessárias para a análise e aceitação do risco, previamente estabelecidas por aquela, incluindo dados cadastrais"* e de *"[...] manter a sociedade seguradora informada a respeito dos dados cadastrais dos segurados e alterações na natureza do risco coberto, de acordo com o definido contratualmente"* (art. 8º, I e II).

5 §2º do art. 21 do Decreto-Lei nº 73/66.

6 Art. 21 do Decreto-Lei nº 73/66.

É certo que o titular dos dados é a pessoa natural e, nas hipóteses de seguro coletivo contratado pelo empregador na qualidade de estipulante, este não poderá consentir em substituição ao seu empregado para fins de tratamento de dados sensíveis. Ademais, é certo que, para o tratamento de dados sensíveis, outras bases legais serão utilizadas, não só o consentimento como exercício regular de direitos ou o cumprimento de obrigações legais ou regulatórias.

EXAME DA PROPOSTA DE SEGURO – inclui a busca de informações sobre o proponente. O subscritor do risco pode precisar de informações adicionais, inclusive de base de dados internas e externas. Analisa informações para análise do risco, oriundas de inspeção prévia, declaração de saúde, exames médicos etc.

O exame da proposta de seguro poderá envolver o tratamento de dados pessoais em geral, o que será lícito, independentemente do consentimento do titular, com base no que preceitua o art. 7º, V, da LGPD, visto que inegavelmente se estará diante de hipótese de *"procedimentos preliminares relacionados a contrato do qual seja parte o titular"*.

Diversa é a hipótese de tratamento de dados pessoais sensíveis. Para esse tipo específico de dados, o tratamento realizado para a etapa de exame de proposta deverá ocorrer, preferencialmente, mediante a obtenção do consentimento do titular, e o titular deverá ser informado que o tratamento de tais dados é condição para a contratação (art. 9º, §3º LGPD). Há, contudo, hipóteses nas quais o tratamento de dados sensíveis nessa etapa decorre de uma obrigação legal ou regulatória – como no caso da exigência de preenchimento de Declaração de Saúde prevista na Resolução Normativa da ANS nº 558/2022 ou das normas da SUSEP e CNSP que tratam da possibilidade de preenchimento de questionário de avaliação de risco e de

informações sobre doenças preexistentes[7] ou mesmo que sirva ao exercício regular de um direito em sede contratual – hipótese, por exemplo, de acessar bases de dados de sinistros do mercado de seguros para fins de identificar eventuais tentativas de fraude –, o que afastaria a necessidade de consentimento. Entretanto, outras hipóteses autorizativas poderão igualmente ser utilizadas, dependendo do caso concreto, já que não há hierarquia entre elas.

SUBSCRIÇÃO DE RISCOS – após considerar todos os dados, o subscritor toma uma decisão sobre o caso, podendo recusar o risco / a proposta, aceitá-lo com modificações ou na cobertura concedê-lo nos termos propostos. Deve considerar a vigência de leis que versem sobre não discriminação.

Na etapa de subscrição de riscos, que é a aceitação, ainda que com modificações ou recusa da proposta, deve ser considerada a possibilidade de restar caracterizada a hipótese de término do tratamento (art. 15), situação que poderá impor a obrigação de eliminação dos dados ou de sua anonimização (art. 16).

Caso tenha ocorrido a aceitação da proposta, restará justificada a manutenção (armazenamento) dos dados do segurado, e, eventualmente se justificará até mesmo a coleta de dados adicionais para a execução do contrato, pois nesse caso o contrato estará apenas em sua fase inicial e, evidentemente, não poderá dar ensejo ao término do tratamento.

Outro ponto a ser considerado nessa etapa diz respeito à aplicação do princípio da não discriminação. Como já mencionado anteriormente, ressalvada a exceção alusiva aos dados de saúde em sede de saúde suplementar, não há vedação para que seja feita a sele-

7 São exemplos a Circular SUSEP nº 667, de 04 de julho de 2022 e Resolução CNSP nº 439, de 04 de julho de 2022.

ção de riscos, mas deverão ser adotados cuidados para não incorrer em processo que resulte na adoção de critérios discriminatórios que sejam **ilícitos e abusivos**.

CONTRATAÇÃO/EMISSÃO – celebração do contrato (apólice); inclusão das informações em um processo de emissão em cada seguradora, transformando os dados em registros legais; compartilhamento das informações com prestadores de serviço; e compartilhamento das informações com órgãos reguladores (SUSEP, ANS).

Celebrado o contrato, tem início a etapa denominada contratação/emissão, que envolve a emissão da apólice, com o eventual compartilhamento de dados com prestadores de serviço e com órgãos reguladores, dando ensejo à necessidade de novas operações de tratamento de dados.

Nessa etapa, o tratamento de dados pessoais será justificado, principalmente, na necessidade de execução do contrato (art. 7º, V), no cumprimento de obrigação legal ou regulatória (art. 7º, II e art.11, II, "a") ou, eventualmente, no exercício regular de um direito em sede contratual (art. 11, II, "d"), além, é claro, de ser possível que o tratamento esteja respaldado no consentimento obtido do titular, quando não se puder enquadrar o tratamento de dados realizado em uma das outras hipóteses aqui citadas.

RESSEGURO - é mecanismo de pulverização de riscos, por meio do qual a seguradora se protege de perdas superiores às tecnicamente suportáveis, valendo-se de um ressegurador no Brasil ou no exterior. Nesse caso, poderá haver necessidade de compartilhamento de dados entre segurador e ressegurador.

Para os fins específicos de resseguro, poderá haver necessidade de compartilhamento de dados com terceiro, o que poderia ser justificado no art. 7º, §5º da LGPD[8], que, dispondo de dados pessoais em geral, estabelece que *"[...] o controlador que obteve o consentimento"* e *"que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento"*.

É importante salientar, contudo, que, se o compartilhamento de dados com o ressegurador ocorrer para fins de execução de um contrato ou para procedimentos preliminares relacionados ao contrato, essa será a base autorizativa adequada e não o consentimento. Há de salientar, também, que o CNSP, por meio da Resolução CNSP nº432, de 12 de novembro de 2021, estabelece os limites máximos de retenção para as sociedades integrantes do mercado segurador, o que em alguns casos poderia atrair a necessidade de compartilhamento de dados com o ressegurador, com vistas ao cumprimento de uma obrigação regulatória, o que deverá ser avaliado caso a caso.

No que diz respeito especificamente ao compartilhamento dos dados pessoais sensíveis, ressalvadas as particularidades daqueles referentes à saúde, que, como já salientado, estão submetidos a um regramento mais restritivo, não há impedimento de comunicação de dados entre seguradoras para viabilizar a contratação de resseguro, especialmente se o compartilhamento de dados tiver como finalidade o cumprimento de obrigação legal ou regulatória ou mesmo se decorrer do exercício regular de direito decorrente de um contrato. Portanto, dependendo do caso, diferentes bases legais poderão ser utilizadas para legitimar o compartilhamento de dados

8 Esse dispositivo pode ser especialmente relevante para o tratamento de dados sensíveis, já que o art. 11 da LGPD não prevê o tratamento de dados sensíveis para a execução de um contrato ou para procedimentos preliminares relacionados a contrato, conforme destacado neste tópico, mas reconhece a possibilidade de compartilhamento com base no consentimento, desde que ele seja dado "de forma específica e destacada, para finalidades específicas" (art. 11, I da LGPD).

entre segurador e ressegurador: execução de contrato; dever legal ou regulatório; exercício regular de direitos; e consentimento.

Por fim, como nos contratos de resseguro pode ocorrer a necessidade de uma transferência internacional de dados pessoais, no caso de um ressegurador estrangeiro, deve-se observar o disposto no Capítulo V da LGPD, em especial no que toca às salvaguardas aplicáveis, observando-se a possibilidade de transferência internacional de dados pessoais (não sensíveis) quando necessária para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular (art. 33, IX da LGPD), desde que demonstrada a real necessidade de tal transferência de dados pessoais para a execução do contrato, por exemplo, para fins de pagamento de ressarcimento de danos em razão de sinistro.

COSSEGURO – assim como o resseguro, o cosseguro funciona como mecanismo de pulverização de risco, mas nesse caso entre seguradoras. Aqui pode haver igualmente o compartilhamento de dados pessoais entre a seguradora e as cosseguradoras.

As mesmas bases legais aplicáveis ao resseguro podem ser utilizadas, segundo o caso concreto, para o cosseguro, desde que presentes os requisitos necessários: execução de contrato; dever legal ou regulatório; exercício regular de direitos; e consentimento.

Diferente do resseguro, no cosseguro não é evidente a necessidade de transferência internacional de dados, já que ocorre entre seguradoras que operam no país.

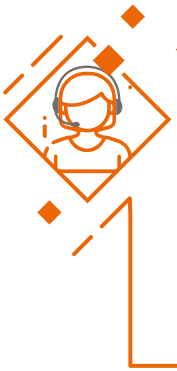
Deve, contudo, ser prestada informação ao titular do dado no que toca às cosseguradoras participantes do seguro contratado, não apenas por força da exigência contida no art. 9°, V da LGPD no que toca a *"[...] informações acerca do uso compartilhado de dados pelo controlador e a finalidade"*, mas, também, por força do que estabelece a Resolução CNSP n° 451, de 2022.

COBRANÇA – realização de cobrança de prêmio por sistemas de cada companhia, podendo ser interno ou externo. Abordagem para realização de cobrança em atraso, podendo gerar nova inspeção de risco para avaliação da continuidade do seguro.

Na etapa de cobrança de prêmio, os dados que serão objeto de tratamento não serão, em regra, sensíveis, exceção aplicável apenas aos seguros saúde, nos quais os procedimentos realizados durante a vigência dos seguros coletivos ou por adesão têm repercussão no reajuste do prêmio do seguro. Logo, versando sobre dados pessoais em geral, nessa etapa o tratamento poderá ser justificado tanto na necessidade de cumprimento do contrato (art. 7º, V) quanto no interesse legítimo do controlador em receber o valor do prêmio (art. 7º, IX) ou, na hipótese de seguros saúde coletivos empresariais ou por adesão como decorrência do exercício regular de um direito em sede contratual (art. 11, II, "d").

ENDOSSO – disponibilização de informações para geração de endosso (aditivo ao contrato), podendo ter várias finalidades: cancelamento, substituição do bem, alteração no risco etc.

Para viabilizar o endosso, o tratamento de dados pessoais será justificado, principalmente, na necessidade de execução do contrato ou na adoção de procedimentos preliminares relacionados a contrato do qual seja parte o titular (art. 7º, V) e no cumprimento de obrigação legal ou regulatória (art. 7º, II e art. 11, II, "a"), além de eventualmente ser possível que o tratamento esteja respaldado no exercício regular de um direito ou no consentimento obtido do titular quando se tratar de dados pessoais sensíveis.



ATENDIMENTO AOS CLIENTES – os funcionários do atendimento ao cliente (SAC, Ouvidoria) são responsáveis por responderem às várias solicitações e reclamações acerca dos diversos aspectos da cobertura e dos serviços. Muitas vezes, o atendimento é realizado por empresas terceirizadas que terão acesso a informações dos segurados e beneficiários.

Na etapa de atendimento ao cliente, o tratamento de dados pessoais se justifica pela necessidade de cumprimento do contrato ou no exercício regular de direito decorrente de um contrato (art. 7º, V ou art. 11, II, "d").

Caso o atendimento seja prestado por empresa terceirizada, é recomendável que haja no instrumento contratual de terceirização o detalhamento das obrigações que deverão ser assumidas pela empresa que for prestar o serviço, pois ela atuará, nessa hipótese, na qualidade de operadora, subordinando-se às instruções que lhe forem passadas pelo controlador (art. 39).

Quando existir processo de identificação e autenticação em sistemas eletrônicos, por exemplo, por meio de gravação de voz para identificação do segurado que contatou o SAC de determinada seguradora, esse dado poderá ser tratado, ainda que sensível (já que a voz pode ser considerada um dado biométrico), para o fim de garantir a prevenção à fraude e a segurança do titular do dado.

PRESTAÇÃO DE SERVIÇO – as apólices atualmente estabelecem coberturas relacionadas à prestação de serviços, assistência 24 horas. Esses serviços são, via de regra, realizados por empresas terceirizadas que têm acesso a informações dos segurados.

Quando o tratamento de dados estiver associado à etapa de prestação de serviços, ou seja, ao cumprimento do contrato em si, faz sentido valer-se da base legal referente à necessidade de cumprimento do contrato ou de exercício regular de direito em contrato (art. 7º, V ou art. 11, II, "d"), o que conferirá licitude à operação, independentemente do consentimento do titular.

Vislumbramos que eventualmente o legítimo interesse do controlador (art. 7º, IX) pode ser utilizado como base autorizativa, caso o tratamento de dados realizado no âmbito da prestação de serviços não se enquadre na hipótese de execução de um contrato ou em nenhuma outra base legal.

Tratando-se de operação associada ao cumprimento de contrato de seguro saúde, a sua legitimação também poderá fundamentar-se, a depender do caso concreto, nos permissivos do art. 11, II, "e" e "f", visto que o tratamento, nessas hipóteses, destina-se a atender ao interesse do próprio titular dos dados, como, por exemplo, a liberação de procedimentos, reembolsos, prestação de contas etc.

Caso o serviço seja prestado por terceiro, é prudente que se adote a cautela de especificar no instrumento contratual de terceirização o detalhamento das obrigações que deverão ser assumidas pela empresa que for prestar o serviço, pois ela atuará, nessa hipótese, na qualidade de operadora, subordinando-se às instruções que lhe forem passadas pelo controlador (art. 39).

É importante que as seguradoras estabeleçam em seus instrumentos contratuais com os prestadores que realizarem esses serviços para estabelecer regras claras quanto ao cumprimento do disposto na LGPD. Aliás, é recomendável que qualquer relação contratual com prestadores de serviço que realizam tratamento de dados pessoais seja formalizada por escrito, com o estabelecimento dos limites de atuação do operador e das responsabilidades das partes.

REGULAÇÃO E LIQUIDAÇÃO DE SINISTRO – na regulação de sinistro, a área técnica precisa determinar se o sinistro ocorreu, se o sinistro está coberto e, frequentemente, reunir informações adicionais. Tais informações podem consistir em registros médicos, relatórios sobre o perfil do motorista, levantamento de registros criminais e pode necessitar solicitar uma investigação de informações sobre clientes. Se houver beneficiários, é necessário determinar quem tem legitimidade para receber o pagamento.

A regulação e a liquidação de sinistro constituem importante etapa da operação do seguro e envolvem a necessidade de tratamento de dados para finalidades diversas, que não se limitam, mas englobam a necessidade de cumprimento do contrato, o exercício de direito vinculado a um contrato e o legítimo interesse para a prevenção de fraudes e outros ilícitos, assim como o cumprimento de uma obrigação legal ou regulatória.

Não apenas as finalidades são diversas, como diversos são também os dados que deverão ser objeto de tratamento nessa etapa de regulação e liquidação de sinistro, que incluem dados pessoais em geral e dados pessoais sensíveis.

A multiplicidade de finalidades do tratamento permitirá que sejam igualmente variadas as bases legais que poderão ser utilizadas para o respaldar.

Sob a perspectiva de cumprir o contrato ou de exercer um direito a ele vinculado, pode-se considerar como autorização para o tratamento as disposições contidas nos artigos 7º, V e 11, II, "d" da LGPD. Com a finalidade de prevenção à fraude, por sua vez, o tratamento poderá ser justificado no legítimo interesse do controlador (art. 7º,

IX) e no cumprimento de uma obrigação legal (art. 7°, II e art. 11, II, a)[9] ou, versando sobre dados sensíveis, na regra do art. 11, II, "g", quando referir-se a processos de identificação ou autenticação de cadastros em sistemas eletrônicos, ou na regra do art. 11, II "d" sempre que se configurar um exercício regular do controlador, como na hipótese de regulação de um seguro de acidentes pessoais ou mesmo de autorização para procedimentos médicos no seguro saúde. Essa linha de interpretação, aliás, foi a adotada no âmbito do Regulamento Geral de Proteção de Dados da União Europeia (GDPR).[10]

Uma última consideração a ser feita sobre essa etapa do tratamento é que ela também poderá ser respaldada no cumprimento de obrigação legal ou regulatória (art. 7°, II ou art. 11, II, "a"), nas hipóteses em que houver necessidade, por exemplo, de enviar comunicações ao Conselho de Controle de Atividades Financeiras – COAF, à SUSEP e à ANS.

9 Como exemplo de norma regulatória que impõe a realização de tratamentos de dados para fins de à prevenção e combate aos crimes de "lavagem" ou ocultação de bens, direitos e valores, ou aos crimes que com eles possam relacionar-se, bem como à prevenção e coibição do financiamento do terrorismopodemos citar a Circular SUSEP nº 612, de 18 de agosto de 2020..

10 USTARAN, Eduardo. European Data Protection Law and Practice. Portsmouth: IAPP, 2018, p. 88.

4

ASPECTOS ESPECÍFICOS

Uma vez analisadas as normas aplicáveis às principais etapas das operações do cotidiano das empresas que atuam no setor de seguros, cabe agora apresentar derradeiras observações sobre alguns aspectos específicos.

CUMPRIMENTO DE EXIGÊNCIAS LEGAIS E REGULATÓRIAS – captura de informações dos clientes para fins de verificação da lavagem de dinheiro, guarda de documentos sobre clientes, contratos etc.

A finalidade de cumprir obrigações legais e regulatórias servirá como base legal para autorizar tanto o tratamento de dados pessoais em geral (art. 7°, II) como o de dados pessoais sensíveis (art. 11, II, "a"), assim como para justificar a guarda de dados após o término do período de tratamento que ensejou a sua coleta, conforme se depreende do art. 16, I da LGPD.

São situações em que a realização do tratamento de dados está prevista em normas legais ou regulatórias, sendo, portanto, uma obri-

gação que é imposta aos controladores, como é o caso, por exemplo, do Sistema de Registro de Operações (SRO) de seguro, de previdência complementar aberta, de capitalização e de resseguro, instituído pela Resolução CNSP nº 383/2020, que criou a obrigação de as supervisionadas efetuarem o registro de suas operações em sistemas de registro previamente homologados pela Superintendência de Seguros Privados (SUSEP) e administrados por entidades registradoras credenciadas pela SUSEP para fins de supervisão e fiscalização da autarquia. O registro deve permitir: **(i)** a apuração dos riscos inerentes à operação, segmentados de acordo com as principais características dos objetos segurados e das coberturas contratadas; **(ii)** a apuração dos fluxos financeiros da operação; **(iii)** a identificação das partes envolvidas; e **(iv)** a identificação das características dos eventos e transações registrados.

Ressalta-se que as operações de seguro, de previdência complementar aberta, de capitalização e de resseguro correspondem ao registro do conjunto de eventos e transações referentes a uma mesma apólice, bilhete, contrato, certificado, título ou série de uma mesma supervisionada.

São exemplos ainda de compartilhamento de dados, em razão de cumprimento de norma regulatória, a Resolução Normativa da ANS nº 529, de 2 de maio de 2022, as Circulares SUSEP nº 605, de 28/05/2020 e nº 612, de 18 de agosto de 2020.

FISCALIZAÇÃO DOS ÓRGÃOS COMPETENTES – entrega de todo tipo de informações ao órgão regulador e exigência de entrega de informações à empresa credenciada para viabilizar a supervisão eletrônica.

Como já afirmado, a finalidade de cumprir obrigações legais e regulatórias servirá como base legal para autorizar tanto o tratamento de dados pessoais em geral (art. 7º, II) como o de dados pessoais

sensíveis (art. 11, II, "a") para fins de atendimento a exigências formuladas pelo órgão regulador. Isso não quer dizer, contudo, que o tratamento de dados pessoais, por parte dos órgãos competentes, não deva observar as regras e princípios previstos na LGPD. Ao contrário, caso alguma exigência regulatória vier a estabelecer o dever de tratamento de dados pessoais em desconformidade com a LGPD, o referido órgão ou entidade pública estará sujeito às penas previstas no art. 52, combinado com o § 3º do mesmo artigo da LGPD.

GESTÃO DE BASE DE DADOS – guarda e utilização de informações pessoais sobre clientes e outros participantes das operações e outras atividades das empresas.

A manutenção de banco de dados é possível em alguns casos e será necessária em outros. Enquanto não tiver sido alcançada a finalidade do tratamento a operação não estará finalizada, tornando necessário o armazenamento seguro (art. 6º, VII e 46) dos dados.

Um bom exemplo são os dados coletados na etapa de subscrição. Esses dados serão úteis e necessários para viabilizar a execução do contrato, de modo que a sua manutenção é impositiva pelo menos enquanto estiver vigente a contratação que justificou a sua coleta, ou se existir outra base legal que autorize o seu tratamento para outras finalidades.

Por outro lado, haverá situações em que será possível ou até mesmo obrigatória a manutenção dos dados após o término do tratamento. A LGPD expressamente assegura o direito de conservação dos dados para além do término do tratamento, desde que seja para quaisquer das seguintes finalidades: **(i)** cumprimento de obrigação legal ou regulatória pelo controlador (art. 16, I); **(ii)** estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (art. 16, II); **(iii)** transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD

(art. 16, III); e **(iv)** uso exclusivo do controlador, vedado seu acesso por terceiro (art. 16, IV), lembrando que, em caso de anonimização dos dados, a vedação de compartilhamento com terceiros não se aplicaria, conforme art.12 da LGPD.

Novamente, é preciso ressaltar que outras hipóteses legais poderão justificar o tratamento de um dado pessoal para além de sua finalidade inicial. Essas hipóteses incluem a existência de um dever legal ou regulatório, o exercício regular de direitos em processo judicial, administrativo ou arbitral e até decorrente de contrato para o caso de dados sensíveis, assim como o legítimo interesse do controlador ou de terceiro.

Dois pontos essenciais devem ser observados na gestão dos bancos de dados. O primeiro é concernente à necessidade de garantir a segurança dos dados armazenados, inclusive com observância dos padrões que venham a ser definidos pela Autoridade Nacional de Proteção de Dados - ANPD (art. 46, §1º), e o segundo é referente à necessidade de verificação da manutenção de situação que respalde a conservação dos dados. É importante destacar, aqui, que o art. 63 da LGPD prevê que *"A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados"*, o que importa dizer que, até que a ANPD estabeleça esse regime de transição, os bancos de dados já em operação quando da entrada em vigor da LGPD poderão não ensejar a incidência das sanções previstas no Art. 52 da LGPD, caso ainda não se encontrem em total conformidade com os termos dessa lei. Porém, como destacado, o tema dependerá de regulamentação por parte da ANPD.

ACESSO A BASES DE DADOS EXTERNAS – diretamente, ou através de terceiros, as empresas têm acesso a dados pessoais oriundos de bases públicas.

A informação é insumo do mercado de seguros. Não raro, as informações obtidas diretamente do segurado são necessárias para fins de combate e prevenção à fraude, além de embasar uma adequada avaliação do risco.

Ressalta-se que a fraude representa a vantagem injusta de um indivíduo sobre o outro, prejudicando a coletividade. Além de moralmente condenável, a ocorrência da fraude em seguros atinge de forma perversa um conceito fundamental do seguro, que é o mutualismo, tornando o sistema desequilibrado e prejudicando justamente os participantes que atuam de maneira correta, já que o custo da fraude acaba sendo repassado ao valor do seguro (prêmio) para todo o grupo de segurados.

As ocorrências fraudulentas repercutem diretamente nas operações realizadas pelo setor de seguros, pois cada fraude não detectada leva ao pagamento de um sinistro que não teria cobertura, elevando os índices de sinistralidade da seguradora.

Vale citar que a prevenção à fraude é um interesse legítimo, reconhecido pelo Regulamento Geral de Proteção de Dados da União Europeia (GDPR em inglês), no qual a LGPD foi inspirada, que em seu considerando 47 ressalta: “O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controle da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento”.

Por sua vez, para garantir a justa precificação do prêmio do seguro, visando atender aos interesses dos segurados e preservar o mutualismo, são realizadas análises complexas, que demandam o uso de informações que não necessariamente podem ser fornecidas pelo próprio segurado. Nesse sentido, é possível e legítimo que as seguradoras utilizem dados obtidos de bases externas, inclusive de órgãos públicos, para, por exemplo, oferecer produtos mais acessíveis. Destaque-se que a consulta a bases de dados geridas por empresas ou mesmo por órgãos públicos muitas vezes decorre de disposição regulatória, como ocorre no caso da Circular SUSEP nº 612, de 18 de

agosto de 2020, que dispõe sobre controles internos específicos para a prevenção e combate aos crimes de "lavagem" ou ocultação de bens, direitos e valores.[11]

É necessário, pois, assentar a existência de regramento na LGPD, permitindo que o poder público compartilhe informações de seus bancos de dados quando **(i)** os dados forem acessíveis publicamente; **(ii)** houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; e **(iii)** na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades (art. 26, § 1º da LGPD).

Também é possível que o poder público compartilhe os dados visando à execução descentralizada de atividade pública que exija a transferência exclusivamente para esse fim específico e determinado, mas essa hipótese, em regra, não será aplicável ao setor de seguros. Essas hipóteses deverão ser lidas em consonância com o que prevê o art. 27 da LGPD, o que acrescenta, em tese, a possibilidade da transferência também ocorrer *"[...] nas hipóteses de dispensa de consentimento previstas nesta Lei"* (inciso I do art. 27 da LGPD).

O que é importante considerar, porém, é que a LGPD não veda ao poder público o compartilhamento de informações constantes de seus bancos de dados com agentes privados, o que é uma garantia de grande utilidade para o setor de seguros, que depende dessa fonte de informações para executar regularmente as suas atividades.

É necessário, contudo, que a utilização de tais bases de dados esteja em conformidade com as regras e princípios previstos na LGPD, em

11 Ver inciso II, do §3º do art. 23 da referida circular.

especial com o princípio da necessidade. Ou seja, é possível que na exploração de suas atividades as seguradoras utilizem dados obtidos de bases externas, desde que haja uma base legal para justificar o tratamento e desde que seja possível demonstrar a necessidade do uso desses dados.

Por fim, é recomendável que a relação com as fontes dos dados seja formalizada por escrito, especialmente para que haja delimitação dos dados que serão tratados, da finalidade e duração do tratamento bem como das medidas de segurança que serão adotadas para manter os dados protegidos.

BASES DE DADOS COMPARTILHADAS DO MERCADO SEGURADOR – bases de dados oriundas de informações fornecidas pelas empresas integrantes do setor de seguros, relativas a seus segurados ou proponentes e acessíveis apenas pelas empresas integrantes do setor.

O compartilhamento de informações entre as empresas integrantes do setor de seguros é medida salutar que tem como principal finalidade a prevenção e combate à fraude contra o seguro. Isso porque, por meio do compartilhamento de dados, é possível identificar a atuação de organizações criminosas em distintos ramos do seguro, assim como tentativas de utilização indevida da cobertura securitária.

Conforme já destacamos, o tratamento de dados para fins de prevenção e combate à fraude se enquadra no legítimo interesse do controlador e de terceiro, nesse caso dos dois – a seguradora que compartilha os dados e as demais que têm acesso a eles –, e, na hipótese de o compartilhamento envolver dados sensíveis, como pode ser o caso dos ramos de pessoas e saúde, a base autorizativa será aquela da alínea “d” do inciso II do art. 11 da LGPD (exercício regular de direitos oriundos de contrato).

Nessa linha, resta igualmente justificado o compartilhamento de dados de apólices recusadas – e, também, das aceitas – para fins, por exemplo, de verificação de seguro sobre um mesmo interesse, o que é vedado por lei, na forma do art. 782 do Código Civil, entre entidades integrantes do mercado segurador, nos casos de seguros de danos.

TRATAMENTO DE DADOS DE RECURSOS HUMANOS – tratamento de dados pessoais de seus empregados, estagiários e daqueles que se candidatam a vagas de estágio e emprego. O mesmo poderá ocorrer com prestadores de serviços contratados pelas empresas integrantes do setor.

Os tratamentos de dados no âmbito das relações de emprego ou de prestação de serviços não estão diretamente relacionados à operação de seguros, portanto, não são o foco deste Guia. Entretanto, assim como os consumidores, os empregados do setor de seguros são peça fundamental da operação de seguros e são igualmente titulares de dados pessoais nessa relação. Usualmente, os dados nessa relação são tratados para fins de cumprimento de obrigações legais ou regulatórias (p. ex., eSocial, DIRF, CAGED/RAIS) para viabilizar o cumprimento dos deveres decorrentes do próprio contrato (ex.: pagamento, concessão de férias, licença-paternidade ou maternidade), ou, então, para o exercício regular de um direito (ex.: o caso de uma reclamação trabalhista). Há, contudo, situações não necessariamente ligadas a tais finalidades, como programas de melhoria da saúde do trabalhador, que, apesar de terem impacto na relação de emprego, não são diretamente necessários à execução do contrato nem decorrem de um dever legal ou regulatório, o que dependeria de outra base autorizativa, como o consentimento, desde que assegurados os requisitos previstos na LGPD: manifestação livre, informada e inequívoca para uma finalidade determinada e, quando se tratar de dados sensíveis, de forma específica e destacada.

Situações relacionadas à gestão de recursos humanos incluem, também, a utilização de servidores na nuvem (*cloud*), o que pode atrair questões relacionadas à transferência internacional de dados e à necessidade de se identificar a existência de salvaguardas específicas. É comum em grupos multinacionais a centralização da gestão de recursos humanos do grupo em determinado país que, se não for o Brasil, exigiria igualmente a observação das regras previstas no Capítulo V da LGPD.

É importante também ressaltar que o segurador pode se ver na situação de estipulante ao contratar seguros coletivos para seus funcionários, aplicando-se também a ele as observações efetuadas neste Guia no que toca à figura do estipulante.

TELEMETRIA – tecnologia utilizada para fins de monitoramento e rastreamento.

A telemetria, que em poucas palavras pode ser descrita como a tecnologia usada para monitorar comportamentos e rastrear objetos, é uma importante ferramenta para o setor de seguros, especialmente para o segmento de automóveis. Como o uso da telemetria muitas vezes contempla o tratamento de dados pessoais dos segurados, é preciso adotar algumas medidas para assegurar o cumprimento da LGPD.

Primeiramente, é preciso identificar a base legal que justificará o tratamento de dados. Em geral, a base legal utilizada para legitimar o tratamento de dados pessoais obtidos através da telemetria é o consentimento, que, como já referido neste guia, deve ser livre, informado e inequívoco. Além disso, caso o tratamento de dados pessoais seja uma condição para a contratação do seguro (por exemplo: concessão de bônus, seguro *pay as you drive* etc.), essa informação deverá ser prestada ao segurado de forma destacada (art. 9º, §3º), juntamente com a informação sobre os meios pelos quais poderão ser exercidos os direitos previstos na LGPD.

O tratamento de dados obtidos por meio de telemetria costuma envolver a tomada de decisões automatizadas – tema que será abordado mais adiante – e frequentemente está associado a processos de enriquecimento de dados e aos segredos comerciais e industriais das empresas. Ou seja, os dados brutos que são coletados são meros insumos para análises mais complexas, que, realizadas com o emprego de conhecimento tecnológico e estratégico de cada seguradora (ou de seus prestadores de serviço), geram novos dados, que podem ser classificados como dados inferidos ou derivados e que muitas vezes são utilizados para aperfeiçoar o processo de precificação do seguro em benefício do próprio segurado.

Diante dessa realidade, é recomendável que o controlador mapeie e tenha conhecimento detalhado das atividades de tratamento de dados que realiza, o que poderá ser vital para a preservação de seus segredos comerciais e industriais no contexto de tratamento de dados obtidos por meio de telemetria.

DECISÕES AUTOMATIZADAS – tomada de decisão a partir do tratamento automatizado de dados pessoais.

De acordo com o art. 20 da LGPD, o titular tem o direito de solicitar a revisão das decisões que afetem seus interesses e que tenham sido tomadas exclusivamente a partir do tratamento automatizado de seus dados pessoais (por exemplo, atribuição de *score*). Nesses casos, o direito do titular não se restringe à possibilidade de solicitar a revisão da decisão automatizada, mas também de conhecer os critérios e os procedimentos que foram utilizados para a tomada da decisão, desde que isso, evidentemente, não coloque em risco os segredos comercial e industrial do controlador.

Se o controlador reputar que o fornecimento dessas informações sobre os critérios e os procedimentos utilizados na decisão automa-

tizada viola os seus segredos, ele poderá se recusar a prestá-las, ficando sujeito, porém, à possibilidade de a Autoridade Nacional de Proteção de Dados realizar auditoria para verificar a presença de aspectos discriminatórios no tratamento de dados (art. 20, §2º).

Nesse sentido, é recomendável que o controlador, no mapeamento dos tratamentos de dados pessoais que realiza, identifique aqueles que envolvam a tomada de decisões exclusivamente automatizadas (o que pode ocorrer, por exemplo, na etapa da subscrição de riscos), a fim de estabelecer meios para viabilizar a revisão dessas decisões, quando for necessário, e para assegurar ao titular dos dados o exercício de seus demais direitos previstos em lei.

TÉRMINO DO TRATAMENTO DE DADOS PESSOAIS – momento em que deve ser encerrada a atividade de tratamento, não restando caracterizada nenhuma das hipóteses que a LGPD autoriza à conservação. Os dados deverão ser eliminados e/ou anonimizados.

A LGPD não especifica o período exato que deve durar o tratamento de dados pessoais, mas estabelece que o término do tratamento ocorrerá nas seguintes hipóteses: **(i)** verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; **(ii)** fim do período de tratamento; **(iii)** comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou **(iv)** determinação da autoridade nacional, quando houver violação à LGPD.

Ou seja, apesar de a LGPD não precisar o prazo de duração do tratamento de dados pessoais, indica a necessidade de que seja estabelecido um limite temporal.

O estabelecimento desse limite temporal, por sua vez, cabe ao controlador e deve estar relacionado ao contexto específico do tratamen-

to. Por exemplo, para se defender de uma possível ação judicial, pode ser necessário que o controlador realize o tratamento de dados pelo tempo correspondente ao prazo prescricional do direito aplicável à hipótese ou para atender a uma obrigação regulatória do controlador, como ocorre com as operadoras de saúde, que devem se ater ao tempo de guarda de documentos e informações a pedido do órgão regulador, como descrito na RN 529/2022 da ANS (artigo 4º), que determina a guarda de documentos pelo prazo de cinco anos.

Portanto, uma vez que os dados pessoais devem ser conservados apenas durante o período necessário para o tratamento (salvo nas situações previstas no art. 16 da LGPD), é recomendável que as empresas do setor de seguros, avaliando internamente suas operações, fixem prazos para a duração dos tratamentos, o que deve ser feito levando-se em consideração as finalidades para as quais eles são realizados.

PRIVACY BY DESIGN – a proteção dos dados pessoais desde a fase da concepção de produtos e serviços.

Para além de adequar suas rotinas às regras da LGPD, os agentes que realizam tratamento de dados pessoais precisam apreender a privacidade como um valor. No mercado de seguros em particular, em que o tratamento de dados pessoais é atividade indissociável do próprio modelo de negócio, é necessário criar uma cultura de proteção de dados pessoais que seja incorporada a toda estrutura da companhia, inclusive nas áreas responsáveis pelo desenvolvimento de novos produtos e serviços.

A LGPD positivou o conceito de *privacy by design,* que, grosso modo, pode ser explicado como a prática de incorporar antecipadamente, ou seja, desde a fase de concepção, mecanismos capazes de proteger a integridade dos dados pessoais e a privacidade de seus titulares.

Portanto, para que haja observância dessa regra, é recomendável a adoção de práticas de difusão da cultura de proteção de dados (conscientização de colaboradores, revisão periódica de rotinas internas, estabelecimento de políticas de privacidade e segurança da informação etc.). Uma boa prática para incorporar o conceito de *privacy by design* é estimular a interação do encarregado de proteção de dados com os demais setores da companhia para que ele possa orientar a respeito das medidas que deverão ser adotadas em cada etapa da operação.

OPEN INSURANCE – modelo de 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.

Através do *Open Insurance,* o segurado poderá, por meio eletrônico, consentir com o compartilhamento de seus dados com outras seguradoras ou terceiros, que poderão utilizar esses dados para atender finalidades específicas, em prazo determinado, previamente informadas no momento da obtenção do consentimento.

Vale destacar que, findo o prazo determinado pelo cliente para o compartilhamento de seus dados, estes não mais devem ser compartilhados para essa finalidade. Contudo, não se pode confundir o encerramento desse prazo com o fim do período de retenção das informações pelo término do tratamento de dados, que ocorrerá conforme indicado pela LGPD e normativos da SUSEP/CNSP.

O rol de dados disponíveis para compartilhamento, no âmbito do *Open Insurance*, é padronizado e “pré-definido”, não podendo ser ampliado pelo segurado.

Sobre o consentimento que é exigido do segurado para fins de compartilhamento de seus dados no âmbito do *Open Insurance*, há de se chamar atenção para uma particularidade. Esse consentimento vai servir para autorizar o compartilhamento dos dados, mas não será, necessariamente, a base legal que justificará os demais tratamentos que serão realizados com esses dados. Por exemplo: a seguradora "A" é autorizada a receber da seguradora "B" os dados de determinado segurado. Isso não significa que esse consentimento será a base legal que respaldará os demais tratamentos que serão realizados pela seguradora "A" com esses dados, que poderá se valer de outras bases legais previstas nos artigos 7º e 11 da LGPD para legitimar esses tratamentos.

Outro relevante aspecto a ser considerado a respeito do *Open Insurance* é a necessidade de adoção de medidas efetivas de segurança das informações que irão trafegar por meio dos sistemas interoperáveis das sociedades participantes.

OPEN FINANCE – modelo de compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas de instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Antes do *Open Insurance*, voltado para o mercado de seguros, implementou-se no Brasil o Sistema Financeiro Aberto (*Open Banking*). Criado a partir da lógica de que os dados pertencem aos clientes e não às instituições financeiras, o *Open Banking* estabeleceu um modelo de *"[...] compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas"* (art. 2º, I, da Resolução Conjunta nº 1/2020).

Mais recentemente, foram promovidas alterações normativas para alterar a sua nomenclatura para *Open Finance*. Precisamente em

razão do significativo volume de dados que poderão ser compartilhados no âmbito do *Open Finance*, que fará interoperabilidade com o *Open Insurance*, é necessário que os agentes de mercado estabeleçam diretrizes sólidas de governança para evitar o tratamento de dados excessivos, que pode levar a questionamentos quanto à legalidade da operação.

Portanto, em razão do aumento da disponibilidade de dados em decorrência dessa interoperabilidade de sistemas, é recomendável a adoção de medidas robustas de segurança da informação, como também de controles internos, para evitar que sejam tratados dados excessivos e desnecessários.

5

CONSIDERAÇÕES FINAIS

Este Guia, assim como já informado anteriormente, não tem a pretensão de trazer todas as respostas para que as empresas integrantes do setor de seguros estejam totalmente em conformidade com o que dispõe a LGPD.

Ele apresenta, por sua vez, a interpretação dos dispositivos da LGPD em relação às distintas etapas da operação de seguros, saúde suplementar, previdência complementar aberta e capitalização sob a ótica do setor, levando em consideração as suas especificidades.