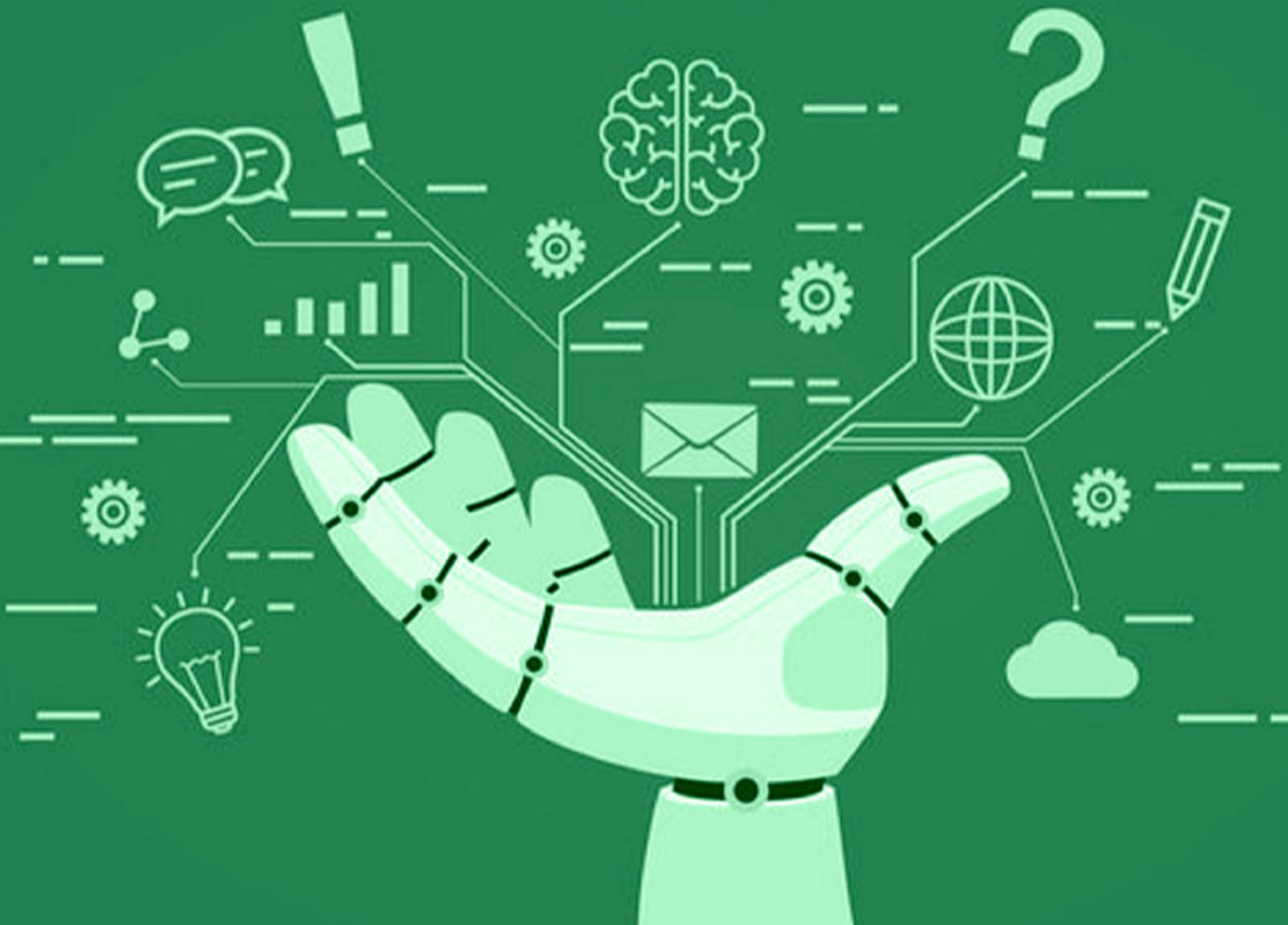
LGPD:
APLICAÇÃO PRÁTICA DAS BASES LEGAIS

COORD. FERNANDA MAIA

AS HIPÓTESES PARA TRATAMENTO DE DADOS PESOAIS DA LGPD



LGPD ACADÊMICO

Esse e-book foi desenvolvido a partir da iniciativa – sem fins lucrativos – do grupo **LGPD Acadêmico**, o qual teve início em agosto de 2018 e é composto por voluntários de todo o Brasil, apaixonados pelo mundo da privacidade e proteção de dados, com o objetivo comum de aprender e compartilhar informação.

Diante da publicação da Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709 de 2018, foi identificada a necessidade direta da sociedade civil, entidades privadas e públicas – independente do seu porte –, profissionais, dentre outros, por conhecimento e acesso a informações relevantes sobre a temática de privacidade e proteção de dados pessoais.

O **LGPD Acadêmico** decidiu reunir neste material acessível e gratuito, o conhecimento e experiência prática de cada autora, utilizando uma linguagem simples e evitando o famoso "juridiquês", recorrendo a termos técnicos somente quando necessário.

Boa leitura!

ÍNDICE

I. Introdução 4

II. Tratamento de dados pessoais 6

1. Consentimento 6

Exemplos práticos 7

2. Cumprimento de obrigação legal ou regulatória 8

Exemplos práticos 9

3. Execução de Políticas Públicas 9

Exemplos práticos 15

4. Estudos por órgão de pesquisa 16

Exemplos Práticos 17

5. Execução de contrato ou procedimentos preliminares 18

Exemplos Práticos 18

6. Exercício regular de direitos 20

Exemplos Práticos 21

7. Proteção da vida ou incolumidade física 21

Exemplos práticos 22

8. Tutela da saúde 23

Exemplos Práticos 24

9. Legítimo Interesse 24

Exemplos Práticos 28

10. Proteção ao crédito 29

Exemplos Práticos 31

III. Tratamento de Dados Pessoais sensíveis 32

1. Consentimento 32

2. Cumprimento de obrigação legal ou regulatória 33

3. Tratamento compartilhado de dados necessários à execução, de políticas públicas 33

4. Estudos por órgão de pesquisa 33

5. Exercício regular de direitos, inclusive em contrato e em processo 33

Exemplos Práticos 35

6. Proteção da vida ou da incolumidade física 35

7. Tutela da saúde 36

8. Prevenção à fraude e à segurança 36

Exemplos Práticos 38

IV. Tratamento de dados de crianças e adolescentes 40

V. Conclusão 41

I. Introdução ◇◇◇

A **Lei Geral de Proteção de Dados Pessoais** – Lei nº 13.709/2018 ("LGPD") estabelece as hipóteses que autorizam o tratamento de dados pessoais que, neste material, denominaremos "bases legais".

As bases legais da LGPD estão divididas em dois artigos: (i) o artigo 7º, dedicado às bases legais para tratamento de dados pessoais em geral (exceto os dados classificados como sensíveis), e (ii) o artigo 11º, dedicado às bases legais especificamente para tratamento de dados pessoais sensíveis (isto é, dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico).

Ao realizar um tratamento de dados pessoais, caberá ao controlador[1] a obrigação de fundamentar cada atividade de tratamento em uma das bases legais estabelecidas pela LGPD.

Este e-book irá abordar as bases legais, mostrando exemplos práticos de suas aplicações. Eventual utilização concreta deverá ser analisada caso a caso pelo leitor, sendo os comentários aqui descritos meramente informativos, não devendo substituir o necessário aconselhamento jurídico para análise da aplicação da lei ao seu contexto específico.

É importante destacarmos que não basta fundamentar o tratamento de dados pessoais em uma das bases legais para que este tratamento seja considerado legítimo. Além desse enquadramento, é imprescindível que sejam observados todos os princípios da lei (vide art. 6º, LGPD), independentemente da base legal adotada para determinado tratamento de dados pessoais.

Adicionalmente, abaixo destacamos os principais aspectos a serem adotados ao realizar um tratamento de dados pessoais:

1. Finalidade: o tratamento deve observar a finalidade que deverá ser lícita, específica e informada ao titular;
2. Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
3. Necessidade: somente poderão ser tratados aqueles dados pessoais efetivamente necessários à finalidade pretendida;
4. Direitos dos titulares: deverão ser observados todos os direitos previstos na LGPD, incluindo a transparência em relação ao tratamento realizado;

[1] Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

5. Qualidade dos dados: todos os dados pessoais tratados deverão ser exatos, atualizados e claros;
6. Segurança e prevenção: deverão ser adotadas medidas técnicas e administrativas para a proteção dos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, bem como a prevenção de danos aos titulares;
7. Não discriminação: o tratamento de dados pessoais não poderá ensejar em atos discriminatórios ou abusivos; e
8. Responsabilização e prestação de contas: conceito conhecido como "*accountability*", que pressupõe a adoção de medidas, , devidamente documentadas, para garantir o cumprimento das normas de proteção de dados e a demonstração de sua eficácia.

Por fim, é importante destacar que ainda não houve definição no Brasil sobre a efetiva interpretação prática da LGPD, bem como não temos orientações, decisões e interpretações provenientes da Autoridade Nacional de Proteção de Dados ("ANPD") que, no momento da elaboração deste e-book, ainda não está em funcionamento, o que significa que as interpretações abordadas neste e-book poderão sofrer atualizações.

II. Tratamento de dados pessoais ◇◇◇

O artigo 7º da LGPD traz um rol de hipóteses que autorizam o tratamento de dados pessoais em geral (exceto de dados pessoais sensíveis, que deverão ser tratados com base no disposto no artigo 11 da lei).

Não há hierarquia entre as bases legais do artigo 7º da LGPD, ou seja, todas as dez opções que autorizam o tratamento desses dados podem ser utilizadas, conforme aplicável ao caso concreto, sem que uma tenha um peso maior do que a outra na decisão pela sua aplicabilidade.

Abaixo listamos os detalhes sobre cada uma das bases legais da LGPD e exemplos de sua aplicação prática.

1. Consentimento

A primeira base legal indicada na LGPD para tratamento de dados pessoais é o consentimento do titular.

Antes da lei, o tratamento de dados pessoais no Brasil era usualmente pensado sob a ótica do consentimento e, sob a nova lei, o cenário se alterou pois, como abordaremos adiante, há novas hipóteses para justificar os tratamentos de dados pessoais.

A LGPD elevou o nível de exigências do consentimento e, em sua redação, a lei define que o consentimento deverá necessariamente representar uma manifestação livre, , informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Neste sentido, vale frisar que um consentimento genérico, sem uma finalidade específica, não seria considerado válido para a LGPD.

Em termos práticos, o usuário deverá concordar afirmativamente, compreendendo de que forma seus dados pessoais serão tratados, para quais finalidades e se, eventualmente, serão compartilhados com terceiros. O consentimento deverá, ainda, ser comprovável, para que o controlador possa demonstrar a aceitação e a livre escolha do titular de dados, quando requisitado.

O GDPR (*General Data Protection Regulation*), norma Europeia, trata o consentimento de maneira bastante semelhante à LGPD. Em seu artigo 4º, o GDPR define o consentimento como: *"uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante*

declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".

O GDPR salienta que o consentimento deve corresponder a uma indicação inequívoca dos desejos expressos por um comportamento ativo. Em outras palavras, o tratamento de dados pessoais deverá ser precedido por um ato positivo e claro do titular de dados. Assim, da mesma forma que a LGPD, o silêncio, as opções pré-marcadas em sites ou aplicativos e a omissão não são suficientes para caracterizar o consentimento válido.

O pedido de consentimento passa a ser destacado, apresentado de forma inteligível, de fácil acesso e com uma linguagem clara e simples, além de ser demonstrável.

Por fim, importante destacar que, justamente pelo caráter de liberdade a ele atrelado, deve ser possível que o consentimento seja revogado a qualquer momento pelo titular, mediante sua manifestação expressa, sempre por procedimento gratuito e facilitado, razão pela qual é importante que o controlador tenha meios aptos (de cunho tecnológico ou não) a realizar a gestão desse consentimento de forma adequada.

Exemplos práticos

Existem circunstâncias em que o controlador pode entender adequado solicitar o consentimento como base legal aplicável.

Alguns exemplos de potencial aplicabilidade da base legal são:

- ***Formulário de envio de newsletter e fins diversos:*** alguns websites contém um formulário para aqueles que desejam receber notícias ou informativos. Nesse caso, o consentimento para envio é coletado. É possível criar outras opções de consentimento (*checkbox*) para finalidades diversas, como envio de promoções e produtos da empresa ou de outros parceiros comerciais. É possível, a depender do conteúdo da *newsletter* e do público-alvo, que exista um interesse legítimo ou até aplicação de execução de contrato, caso seja enviado no contexto do contrato (a ser avaliado com maior detalhes nos itens II, 5 e II, 9, adiante).

- ***Utilização de geolocalização (facultativa) em aplicativos:*** a coleta de dados de geolocalização facultativa em aplicativos, na qual o titular pode optar por esse tipo de comodidade para receber, por exemplo, anúncios específicos para a região em que se encontra.

Uso de dados de empregados para fins diversos e não previsto em contrato (desde que livre): a depender do caso, o empregador poderá solicitar o consentimento (desde que verdadeiramente "livre" – ou seja, comprovadamente opcional e de forma que o empregado não se sinta compelido a aceitar ou eventualmente sinta que poderá sofrer qualquer tipo de represália com a recusa), como no caso de um treinamento opcional (não necessário para o exercício das funções do empregado) ou para utilização de imagem do colaborador (em uma situação que não seja necessária para o exercício das funções deste). É importante destacar que, no contexto de uma relação de trabalho, o consentimento obtido do empregado raramente se mostra livre (e, portanto, válido), devido ao desequilíbrio de poder e subordinação entre as partes, razão pela qual uma análise detalhada deverá ser realizada antes de sua eventual aplicação.

É de se notar que, em algumas instâncias, é possível construir uma argumentação e avaliar a aplicabilidade de outra base legal (como legítimo interesse), a depender do tratamento e do apetite de risco do controlador. Por isso, reiteramos que o presente material não consiste em assessoria jurídica e que seus advogados devem ser consultados para fins de avaliação da melhor estratégia para o seu caso específico e a definição da base legal mais adequada.

2. Cumprimento de obrigação legal ou regulatória

A LGPD autoriza o tratamento de dados pessoais caso este ocorra para cumprimento de obrigações legais ou regulatórias, ou seja, em circunstâncias em que, para cumprir com uma lei ou regulamento específico, o controlador precise realizar o tratamento dos dados pessoais.

Isso porque, por imposição de leis ou regulamentos, para cumpri-los, o tratamento de diversos dados pessoais deve ser realizado por certos setores da economia, especialmente em setores regulados como o financeiro, de saúde suplementar, entre outros.

Assim, ainda que o tratamento de dados pessoais baseado em obrigação legal ou regulatória não exija diretamente a realização de tratamentos de dados pessoais específicos, deve-se sempre respeitar os princípios da LGPD (finalidade, necessidade, entre outros).

Importante destacar que a obrigação do cumprimento da lei ou regulamento deverá ser do controlador para a aplicação dessa base legal.

Exemplos práticos

- ***Cumprimento de obrigações de combate aos crimes de "lavagem" de dinheiro:*** uma instituição financeira – conforme exigido pela Circular 3.461/2009 do Banco Central do Brasil ("Bacen") – deverá tratar alguns dados pessoais.

  Lei 12.414/11 – Lei do Cadastro Positivo: os *bureaus* de créditos autorizados pelo Bacen deverão tratar dados pessoais para a criação da base de dados do cadastro positivo.

- ***Resolução 3954 – Correspondentes Bancários:*** as instituições financeiras possuem uma série de regras para cumprir com suas obrigações perante os seus correspondentes que envolvem tratamento de dados pessoais.

- ***Consolidação das Leis Trabalhistas (artigo 168) e Normas Regulamentadoras nº 4 e nº 7:*** determinam e regulamentam a obrigação das empresas em realizar o exame médico para comprovar o estado de saúde física e psíquica do funcionário.

- ***Código Civil 2002 (artigo 118):*** justifica a obrigatoriedade de os contratos sociais das empresas possuírem os dados pessoais dos representantes legais.

3. Execução de Políticas Públicas

O artigo 1º da LGPD estabelece que o setor público também está abarcado no escopo da lei, determinando em seu parágrafo único que, por ser de interesse nacional, a norma deve ser cumprida pela União, Estados, Distrito Federal e pelos Municípios.

O estabelecido na lei justifica-se porque é o setor público um dos maiores - senão o maior - concentradores de dados pessoais em seus vários campos de atuação. Não poderia ser diferente, afinal o Estado é responsável por promover o bem-estar da sociedade, o que faz por meio da prestação dos mais variados tipos de serviços, bem como pela implementação de políticas públicas de atendimento à população, sendo esse um dos caminhos para concretizar o objetivo maior da persecução do interesse público.

Dessa forma, como em todos os demais casos em que há a utilização de dados pessoais, a LGPD exige também do Estado que ele justifique as

atividades de tratamento. Portanto, deve também o poder público declarar a finalidade para a qual o dado pessoal será utilizado, definir e documentar qual a base legal adequada.

O setor público reveste-se de tamanha especificidade no tocante ao tratamento de dados pessoais que a LGPD possui o capítulo IV, que compreende os artigos 23 até o 32 e trata exclusivamente do Poder Público, além de obrigar que a LGPD seja considerada em conjunto com a Lei de Acesso à Informação (Lei nº 12.527/2011). De se notar que esses dispositivos passaram por várias alterações, sendo que os entes públicos tentaram estabelecer critérios menos rigorosos para a aplicação da LGPD em suas próprias atividades.

Dentro do rol taxativo de bases legais existentes na lei, encontra-se no inciso III a base que será certamente a mais utilizada para respaldar as atividades estatais e atividades da administração pública: a execução de políticas públicas. Como veremos, a referida base legal pode ser utilizada inclusive para tratamento de dados sensíveis sem necessidade de fornecimento de consentimento por seu titular, conforme art. 11, II, alínea b da LGPD.

Políticas públicas

Para compreender o previsto no inciso III do art. 7º da LGPD é preciso buscar o significado de políticas públicas, ou seja, quais atividades estatais que poderiam justificar o tratamento dos dados pessoais pelo Poder Público amparados nessa base legal.

Esse é o primeiro desafio de quem se propõe a entender a abrangência dessa base legal, não havendo sequer consenso acerca da definição exata do que se enquadraria como política pública. Uma definição que pode ser utilizada seria "*política pública é uma diretriz elaborada para enfrentar um problema público*[2]", onde "*a razão para o estabelecimento de uma política pública é o tratamento ou solução de um problema entendido como coletivamente relevante*".

Outra definição possível seria que "*Políticas públicas são a totalidade de ações, metas e planos que os governos (nacionais, estaduais ou municipais) traçam para alcançar o bem-estar da sociedade e o interesse público*[3]".

Adotando esse conceito de política pública, a base legal execução de políticas públicas poderia ser utilizada sempre que a finalidade de utilização dos dados

[2] SECCHI, Leonardo. Políticas públicas: conceitos, esquemas de análise, casos práticos. 2012.

[3] Manual de políticas públicas: http://www.mp.ce.gov.br/nespeciais/promulher/manuais/MANUAL%20DE%20POLITICAS%20P%C3%9ABLICAS.pdf

pessoais fosse o atendimento de necessidades ou a solução de problemas da coletividade.

Alguns exemplos de assuntos que têm essa finalidade e admitiriam a utilização da referida base legal podem ser encontrados na própria Constituição da República, que traz expressamente determinadas situações em que o Estado deve atuar mediante a criação de políticas públicas: promoção da saúde para garantir o acesso universal e igualitário (art. 196, CRFB/88); promoção do acesso democrático e permanente à cultura pactuadas entre os entes governamentais e a própria sociedade (art. 216-A, CRFB/88); programas de assistência integral à saúde da criança, do adolescente e do jovem admitida a participação de entidades não governamentais (art. 227, §1º, CRFB/88); estabelecimento do plano nacional de juventude (art. 227, §8, II).

Diante das demandas sociais, é fato que o Poder Público não consegue atender tudo sozinho e, assim, precisa contar com parcerias de organizações privadas na implementação das políticas públicas, isso autorizaria o uso dessa base legal também por organizações do setor privado? Essa é uma das questões a que a ANPD pode ser chamada a se manifestar sobre uma eventual flexibilização na utilização dessa base legal, a princípio o que se tem é a vedação expressa no art. 7º, IIII da LGPD.

Outro ponto ,que necessita ser discutido, diz respeito aos instrumentos legais aptos a estabelecer as parcerias entre entes públicos e sociedade civil. Estabelece o art. 7º, III da LGPD que a base legal execução de políticas públicas autoriza o tratamento e o compartilhamento de dados pessoais desde que tais políticas estejam previstas em lei, regulamentos, contratos, convênios ou instrumentos congêneres (como termos aditivos, acordos de cooperação técnica, protocolos de cooperação). No mesmo sentido, o art. 26 determina que a regra é a proibição de transferência para entidades privadas de dados pessoais a que o Poder Público tenha acesso, todavia, a execução de políticas públicas de forma descentralizada é exceção. Exige, contudo, que a transferência seja feita para esse fim específico e determinado e que ela esteja amparada por lei, contratos, convênios ou instrumentos congêneres; o que impediria a utilização desses dados para outras finalidades que não aquela estabelecida no instrumento legal. O rol de documentos autorizadores é amplo e genérico, permitindo compreender que qualquer instrumento firmado por um ente do Poder Público com outro, ou em uma parceria entre ente público e setor privado para execução de política pública, é suficiente para legitimar o compartilhamento de dados pessoais utilizando como base legal a execução de políticas públicas.

Quando a execução da política pública estiver respaldada em contratos e convênios (e certamente em instrumentos congêneres, em que pese a ausência

do termo no art. 26, §2º), eventuais compartilhamentos deverão ser comunicados à Autoridade Nacional de Proteção de Dados (ANPD). Além disso, é importante pontuar que embora seja o consentimento do titular do dado a base legal indicada para amparar o compartilhamento das informações pessoais pelo Poder Público, a necessidade de consentimento é afastada quando o compartilhamento for feito para atender à execução de políticas públicas, por disposição expressa do art. 27 da LGPD.

Em suma, para que o compartilhamento de dados pessoais com o fim de execução de políticas públicas seja lícito, basta que a política pública esteja prevista em lei, regulamento, contrato, convênio ou instrumento congênere, sendo que para os três últimos tipos de documentos exige-se a comunicação à ANPD, estando, em qualquer um desses casos, dispensado o consentimento do titular do dado.

Atividades Públicas no GDPR vs execução de políticas públicas na LGPD

Por ter sido o GDPR e a sua efetivação utilizados como guia para a implementação da LGPD no Brasil em vários aspectos, é interessante observar como a consecução do interesse público é tratada por ele. O GPDR apresenta em seu art. 6 (e) a base legal autorizadora do tratamento de dados pessoais quando necessários para executar tarefas que visem atender o interesse público. O art. 6 (3) determina que essa base legal só deve ser utilizada se a execução da tarefa estiver prevista em Lei da União Europeia ou na lei do Estado Membro ao qual o controlador esteja submetido. O *recital* 41 esclarece ainda que a previsão em lei exigida para autorizar a utilização dos dados pessoais para a consecução de atividades públicas não requer um ato legislativo específico propriamente dito, bastando que o documento em que a atividade pública esteja prevista seja claro e preciso e sua aplicação seja esperada ou pelo menos previsível às pessoas atingidas.

Inicialmente é preciso distinguir a base legal existente no GDPR – *public task* ou atividades públicas daquela existente na LGPD – execução de políticas públicas. A primeira é mais ampla, uma vez que abrange as atividades de execução de políticas públicas em busca de atender o interesse público e o exercício de outras atividades relativas à autoridade oficial, que são aquelas atribuições próprias de um ente público. Quanto ao adotado na LGPD, embora não se tenha um conceito fechado do que seria política pública, partindo-se, assim, do pressuposto que toda execução de política pública seria uma atuação estatal com o fim de atender à necessidades sociais, estaria-se diante de uma base legal mais restrita do que àquela adotada no regulamento

europeu. Na comparação entre os dois regulamentos, deve-se ter atenção que no GDPR somente a execução de atividades públicas está vinculada ao atendimento do interesse público.

Tomadas as devidas distinções em que a base legal – *public task* - descrita no GDPR é mais ampla que a base legal execuções de políticas públicas prevista na LGPD. Merecem leitura As orientações da autoridade de proteção de dados do Reino Unido, o ICO[4], sobre a utilização da base legal no contexto do GDPR. Defende a autoridade que não importa a natureza jurídica (seja ela do setor público ou privado) da organização que executa a "*public task*" para que a base legal possa ser utilizada, importando, na verdade, a natureza da função que está sendo executada. Dessa forma, a utilização da referida base legal no seu aspecto execução de atividade pública não estaria restrita ao poder público, mas poderia ser utilizada por todos aqueles que executam alguma função de natureza pública que vise concretizar atividades que tenham como fim concretizar o interesse público.

Além disso, o ICO apresenta um rol exemplificativo de tarefas autorizadoras da utilização da referida base legal: administração da justiça, funções legislativas, funções governamentais e atividades que suportem ou promovam o engajamento democrático, e acrescenta que a utilização dessa base é legítima toda vez que a finalidade da tarefa executada seja o atingimento do interesse público.

- Ainda em relação à base legal prevista no regulamento europeu, o ICO apresenta orientações sobre como é possível comprovar o seu uso legítimo. Faz-se importante notar que enquanto a ANPD não é criada para estabelecer os requisitos de prestação de contas (*accountability*), tais instruções servem apenas como meros referenciais de boas práticas, que podem ser utilizados como parâmetros de análise para verificação da correta aplicação da base legal execução de políticas públicas por aqui.É necessário conseguir provar a relevância da tarefa e identificar qual o documento em que a política pública que exige o compartilhamento de dados está prevista, se é uma lei, um regulamento, um contrato ou outro instrumento, além de demonstrar que não havia outra forma mais razoável ou menos intrusiva de se efetivar tal política pública;
- Esclarecer que direitos individuais de apagamento dos dados e de portabilidade não se aplicam aos dados pessoais quando a base legal

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/

utilizada é a de “public task” com a finalidade de atingir o interesse público;

- Considerar a existência de base legal alternativa caso não haja certeza se determinado processamento é necessário para a execução de uma tarefa que seja relevante e que esteja claramente indicada na lei;
- Documentar porque a decisão de utilizar a base legal consecução de ”public task” foi tomada;
- Identificar exatamente qual a política pública relevante e o seu fundamento legal;
- Incluir informações sobre a finalidade do tratamento e a base legal escolhida nos informativos de privacidade;

A base legal de dados execução de políticas públicas prevista na LGPD poderá servir de grande amparo estatal na hora de tratar os dados dos administrados, inclusive dados sensíveis, conforme apresentado nos exemplos de políticas públicas já existentes.

Importante ressaltar que para que os dados sejam tratados pelo Poder Público, ou por quem lhe fizer às vezes, é preciso que exista um instrumento legal que minimamente institua a política pública e que crie suas diretrizes. Devem estar contemplados no documento, por exemplo, quem serão os entes públicos ou as organizações privadas que serão responsáveis por sua gestão ou execução, e que o fim exclusivo da política prevista seja o atingimento do interesse público.

Uma questão que pode surgir nesse momento é se poderia o poder público ao contar com uma base legal tão específica e tão ampla também se utilizar do legítimo interesse para justificar suas atividades de tratamento de dados pessoais? A autoridade britânica (ICO) orienta que é possível que as autoridades públicas utilizem o legítimo interesse desde que não seja um tratamento de dados relacionado ao exercício da autoridade pública. Lembrando que nesse caso é necessário entender o exercício de atividades públicas da forma apresentada no GDPR[5].

No escopo da LGPD, com a incerteza sobre o que está abarcado pelo conceito execuções de políticas públicas, pode-se questionar a utilização do legítimo interesse a par do conceito de legalidade estrita -

que determina a total submissão do Poder Público ao que estiver previsto em lei – a que se submete a Administração Pública, em que ela somente pode

---

5 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

fazer o que a lei autoriza, a utilização da base legal do legítimo interesse nas atividades, por conter aspectos subjetivos e ter como um de seus requisitos a existência de legítima expectativa para utilização de dados pessoais. Importante que fique claro que a LGPD não faz qualquer restrição ao uso do legítimo interesse pelo poder público.

Quanto as demais bases legais, não há dúvidas de que o Poder Público pode lançar mão de qualquer delas, como a execução de contrato ou ainda cumprimento de obrigação legal, por exemplo, caso não seja possível utilizar a base de execuções de políticas públicas.

Acima de tudo, não se pode esquecer que todo e qualquer dado pessoal, ainda que utilizado pelo Poder Público na busca por alcançar a consecução do interesse público, deve ser tratado de forma transparente e sempre atendendo o dever de informação. Todo sujeito titular dos dados pessoais, tem o direito de ser informado quanto à finalidade do tratamento dispensado às suas informações pessoais, bem como de ter acesso aos seus próprios dados. Nunca é demais lembrar que as obrigações de segurança e de prestação de contas em relação ao uso dos dados pessoais se estendem também ao Poder Público.

Exemplos práticos

De forma a exemplificar o entendimento de algumas situações que ensejariam o uso legítimo da base legal prevista no art. 7º, III da LGPD, seguem algumas políticas públicas já em execução no Brasil:

- ***Bolsa Família:*** Programa de gestão descentralizada: União, Estados, Distrito Federal e Municípios compartilham entre si processos e tomadas de decisão, com tratamento dos dados pessoais presentes no cadastro único para programas sociais do governo federal (acesso aos dados regulamentado pela portaria nº 502 de 2017);

- ***Política de cotas para acesso à universidade:*** Programa de execução descentralizada: Governo Federal, Universidades Federais e Institutos Federais de Educação de Jovens e adultos, da Lei nº 12.711/12 e decreto nº 7.824/12, com tratamento de dados documentais de estudantes especificando a raça e etnia;

- ***Política pública de prevenção ao HIV - Programa Nacional de DST/Aids:*** Programa de execução descentralizada inclusive com participação da sociedade civil, conforme preceitua a Constituição Federal, Lei nº 8080/90 e 8.142/90, entre outras, com tratamento de dados cadastrais e dados de saúde;

Política pública de prevenção ao uso de drogas: Programa de execução descentralizada: ações podem ser executadas diretamente pelo Poder Público, nos níveis federal, estadual, distrital e municipal, e por organizações não-governamentais sem fins lucrativos, conforme Lei nº 11.343/06 e Decreto nº 9761/2019, com tratamento de dados de saúde física e mental entre outros.

Todos os exemplos apresentados têm forte apelo social e tem como objetivo a concretização do interesse público, sendo necessárias para a melhoria da vida dos indivíduos na sociedade. Todas elas utilizam dados sensíveis e podem utilizar dados de crianças e adolescentes, sendo que a maioria exige o envolvimento da sociedade civil, uma vez que é impossível o Estado conseguir realizar a sua implementação sozinho, inclusive pelo fato de que o Brasil é um país de extensões continentais, o que impossibilita o Poder Público de chegar a todos os locais diretamente.

4. Estudos por órgão de pesquisa

Uma das hipóteses autorizativas para tratamento de dados pessoais e dados pessoais sensíveis é para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais e dos dados pessoais sensíveis, conforme previsto no art. 7º, IV e art. 11º, II, C da LGPD.

É salutar que a base legal exista e que esse tratamento seja legitimado pela LGPD, já que os estudos realizados por tais órgãos têm um papel ímpar no desenvolvimento econômico, tecnológico e na inovação, questões que são verdadeiros fundamentos da disciplina da proteção de dados pessoais, conforme art. 2º da lei.

Não obstante a necessidade de pesquisa para que o desenvolvimento ocorra, optou-se por conceituar o termo "órgão de pesquisa" de forma restritiva, resultando na delimitação dos órgãos ou entidades que poderão se valer de tal hipótese autorizativa para tratamento de dados pessoais somente para:

> "órgão ou entidade da administração pública 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"

Essa conceituação, em especial a questão da ausência de finalidade lucrativa, cria parâmetros que impedem que, por exemplo, entidades de pesquisa privadas, possam se valer dessa base legal para tratar dados pessoais de

forma indiscriminada ou realizar tratamento de dados com abusos (por exemplo, mediante *profiling* de eleitores e direcionamento de conteúdo eleitoral, como ocorreu no emblemático caso conhecido como *Cambridge Analytica*).

Muito se debateu sobre a impossibilidade de utilização da base legal por instituições privadas de pesquisa com fins lucrativos (para, por exemplo, viabilizar a aplicação da base legal para centros de pesquisa clínica privados), no entanto, o pleito de exclusão da restrição às entidades privadas sem fins lucrativos não prosperou.

Ainda sobre o tema, a LGPD assegura, expressamente, em seu artigo 16, II, o direito de conservação dos dados para além do término do tratamento para algumas finalidades específicas, dentre elas o estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que deverão ser tratados exclusivamente dentro desse órgão e estritamente para a finalidade de realização de estudos e pesquisas. Além disso, deverão ser mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem padrões éticos aplicáveis a estudos e pesquisas. Nesses casos, a divulgação dos resultados, estudos ou pesquisa, em nenhuma hipótese poderá revelar dados pessoais e o órgão de pesquisa será o responsável pela segurança da informação deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiros.

Exemplos Práticos

Quanto aos exemplos de aplicação prática dessa base legal, cabe primeiramente reiterar que o rol de entidades ou órgãos que poderão se valer dessa base legal de tratamento são restritos à administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos, legalmente constituída sob as leis brasileiras e com sede e foro no País. Adicional, é necessário que contenha a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico em sua missão institucional ou em seu objetivo social ou estatutário. Não poderão, portanto, se valer dessa base legal, empresas de pesquisa privada ou universidades privadas (por, notadamente, terem finalidade lucrativa).

- ***Condução de estudos por institutos de pesquisa públicos:*** condução por institutos como Instituto Brasileiro de Geografia e Estatística - IBGE, Fundação Oswaldo Cruz - Fiocruz, Instituto de Pesquisa Econômica Aplicada – Ipea, dentre outros;

- ***Realização de pesquisas por universidade públicas:*** desde que contenha em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

- ***Atividades de pesquisa desenvolvidas por outros órgãos ou entidades:*** somente caso se enquadrem na conceituação trazida pela LGPD para órgãos de pesquisa.

5. Execução de contrato ou procedimentos preliminares

A base legal para tratamento de dados pessoais relacionada a execução de um contrato ou de procedimentos preliminares relacionados ao contrato, a pedido do titular, está disposta no artigo 7º, V da LGPD.

Esta base legal autoriza o tratamento de dados pessoais quando tais dados forem necessários para a execução de contrato ou para a realização de procedimentos preliminares relacionados ao contrato do qual o titular dos dados seja parte ou a pedido deste. Ou seja, será necessário: (i) compreender o racional do contrato; (ii) qual o resultado que aquele documento visa atingir; e (iii) entender se o tratamento de dados pessoais é realmente necessário para atingir aquele objetivo. Portanto, destacamos a importância de cláusulas claras nos contratos que envolverem tratamento de dados pessoais.

No que se refere ao tratamento de dados pessoais para procedimentos preliminares relacionados ao contrato, o tratamento só poderá ocorrer quando decorrer diretamente de fase anterior à elaboração do contrato (e necessária para este), mesmo que não venha a se concretizar.

Em conclusão, entendemos que não é qualquer atividade de tratamento envolvendo uma relação contratual que poderá ser justificada por esta base legal. O simples fato de uma atividade estar descrita no contrato não implica que a mesma seja necessária para a sua execução, o que significa que a utilização dessa base legal deve ser preponderantemente voltada para atividades de tratamento derivadas da essência da relação jurídica contratual, independentemente de estarem ou não mencionadas no contrato em si.

Ainda, caso o controlador pretenda tratar estes dados pessoais para outras finalidades, será necessário o enquadramento em outra base legal.

Exemplos Práticos

- ***Relação de Trabalho:*** O tratamento de dados pessoais em uma relação de trabalho pode ser justificado em algumas situações pela base legal da execução de contrato, incluindo aqueles tratamentos realizados anteriormente à assinatura do contrato. Por outro lado, a relação de

trabalho não configura uma autorização ou consentimento do empregado para uso dos dados para qualquer finalidade que não seja necessária à execução do contrato de trabalho no âmbito do relacionamento entre as partes. Isso significa que, se fundamentado na base legal da execução de contrato, o tratamento de dados pessoais no âmbito laboral deve ser limitado às finalidades necessárias para permitir a execução das atividades profissionais pelo empregado ou o cumprimento da contraprestação pelo empregador. Por exemplo: o tratamento dos dados bancários do empregado para pagamento da contraprestação pelo empregador pode ser justificado pela presente hipótese legal.

Diante do exposto, a base legal relacionada a execução de contratos é útil para os empregadores, mas deverá ser utilizada a luz dos princípios da limitação de finalidade e minimização de dados pessoais, ou seja, levando em consideração a necessidade da coleta e uso dos dados.

Compra e Venda Online: Como exemplo temos a situação em que um titular compra produtos de um vendedor online utilizando o seu cartão de crédito e quer receber o produto em sua casa. Para que isso seja possível, será necessário que o controlador processe os dados do seu cartão de crédito e endereço de cobrança para efetuar o pagamento e o endereço residencial do titular para a entrega do produto[6]. Tais atividades de tratamento podem ser feitas com base no artigo 7º, V da LGPD.

Outro exemplo, é o tratamento do endereço residencial do titular, sendo parte do processo de entrega de um produto comprado pela internet, isto porque, a partir da compra do produto é necessária sua entrega e, por conseguinte é necessário o tratamento do dado de endereço para que a obrigação contratual do vendedor seja cumprida.

Por outro lado, se o titular dos dados não escolher a entrega em domicílio e sim a retirada do produto na loja, não será mais necessário para cumprir o objetivo principal do contrato que se processe os dados relacionados ao seu endereço residencial.

Contratos de forma geral, quando necessário: Considerando o exposto, a presente base legal não se aplicará a qualquer ação relacionada ou incidente ao cumprimento do contrato. Entretanto, existem algumas ações como o envio de notificações de pagamentos em atrasos ou relacionadas ao cumprimento do contrato que podem ser razoavelmente

[6] European Data Protection Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf> Acesso em:

previstas como necessárias para manter a relação contratual e poderão ser incluídas nesta base legal.

Importante destacar que há cenários em que essa base legal não será aplicada, tais como, mas não se limitando a:

- ***Profiling (marketing):*** No contexto do exemplo acima, se o respectivo vendedor online desejar analisar o perfil de seus clientes e suas preferências por meio da análise de suas visitas ao website e incluir essa atividade no contrato de compra e venda online, o exclusivo fato do tratamento destes dados estar no contexto de uma atividade prevista no contrato, não autoriza o controlador a processar dados pessoais para essa finalidade. Ele terá que utilizar outra base legal. Isto porque, o objetivo principal do contrato não requer o profiling dos clientes.

- ***Marketing:*** Seguindo a linha do exemplo do contrato de Compra e Venda Online, o tratamento de dados para fins de marketing incluído neste mesmo contrato não poderá ser utilizado como uma forma de cumprimento de contrato pois não é necessário para que a compra seja efetivada.

6. Exercício regular de direitos

O inciso VI do artigo 7 da LGPD estabelece como hipótese de tratamento de dados pessoais o exercício regular de direitos, ou seja, ele dá o permissivo legal para que o controlador trate dados pessoais quando tiver por finalidade subsidiar o exercício regular de direitos em processo judicial, administrativo ou arbitral, seja existente ou a ser movido no futuro Os direitos podem ser tanto do controlador quanto de terceiros ou do próprio titular.

Com base neste artigo entende-se, por exemplo, que fica resguardado o direito de o controlador produzir provas, mesmo que estas incluam dados pessoais da outra parte ou de terceiros (não precisando, portanto, de consentimento para tal), sempre levando-se em consideração a finalidade, a adequação e a necessidade do uso dos dados pessoais, bem como os demais princípios previstos no artigo 6 da LGPD.

Como veremos adiante (vide capítulo III, 5), o artigo 11 da LGPD, que lista o rol de hipóteses para tratamento de dados pessoais sensíveis, traz em seu inciso II, "d" a possibilidade de tratar dados pessoais sensíveis, sem o consentimento do titular, nas hipóteses em que for indispensável para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral. O exercício regular de direitos previsto como base legal para tratamento de dados pessoais e dados sensíveis vai acertadamente ao encontro da previsão constitucional de garantia da ampla defesa e do contraditório, pois se pairasse qualquer dúvida com relação à produção de provas em processo judicial, e

fosse permitido a uma parte impedir que a outra utilizasse seus dados pessoais no âmbito de um processo judicial, poderíamos estar diante de cerceamento de defesa, o que traria sérios prejuízos para a solução de litígios no Brasil.

É também com base nessa hipótese legal que pode ser justificada a retenção de dados pessoais por período adicional ao término do tratamento, uma vez que pode haver a necessidade de utilização dos dados em processo judicial e, para isso, pode-se considerar como parâmetro de prazo de retenção o prazo prescricional aplicável.

Exemplos Práticos

- ***Apresentação de documentação em juízo:*** por exemplo, no caso de o empregador necessitar de dados do empregado para comprovar o pagamento de verbas ou concessão de benefícios e apresentar tais documentos em juízo. Em casos mais sensíveis, pode haver a necessidade de apresentação de relatórios de performance ou de documentos que justifiquem eventual demissão por justa causa.

- ***Prova em processo judicial:*** pode ser necessário acostar aos autos de processo administrativo, judicial ou arbitral um documento ou fotografia que contenha dados pessoais.

- ***Armazenamento de dados pessoais para prevenção à eventuais ações judiciais e/ou administrativas:*** como explicado no exemplo acima, poderá ser necessário juntar aos processos documentos que contenham dados pessoais dos titulares como meio de prova. No entanto, considerando que a empresa não sabe ao certo quando enfrentará as demandas judiciais ou administrativas nas quais será necessário fazer uso de tais provas, poderá utilizar dessa base legal para armazenar os dados pessoais de acordo com os prazos prescricionais e decadenciais do direito brasileiro.

7. Proteção da vida ou incolumidade física

O inciso VII do mesmo artigo 7 estabelece uma base legal que permite o tratamento de dados pessoais para a proteção da vida ou da incolumidade física do titular ou de terceiros. A mesma base legal ainda aparece para sustentar o tratamento de dados pessoais sensíveis, na ausência de consentimento, conforme previsto no artigo 11, inciso II "e" da LGPD.

Tendo como base de interpretação o GDPR, podemos entender que a proteção à vida neste caso tem o intuito de se referir aos interesses essenciais para a vida de uma pessoa, portanto essa base legal tem um escopo de aplicação bastante limitado.

Ainda sobre o GDPR, o *recital* 46 do regulamento europeu traz de forma explícita a possibilidade de tratamento de dados pessoais, quando necessário, para fins humanitários, incluindo o monitoramento de epidemias e da sua propagação:

> O tratamento de dados pessoais também deverá ser considerado lícito quando for necessário à proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa singular. Em princípio, o tratamento de dados pessoais com base no interesse vital de outra pessoa singular só pode ter lugar quando o tratamento não se puder basear manifestamente noutro fundamento jurídico. Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo o monitoramento de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana.

Em um cenário de pandemia, como o decorrente da COVID-19, o entendimento das autoridades europeias com relação ao tratamento de dados pessoais ainda não é uniforme, existindo autoridades com posturas mais permissivas, tais como Irlanda, Itália e Espanha, e outras mais restritivas, como Bélgica, França e Holanda, isso levando-se em conta, principalmente, divulgação de dados de empregados, obtenção de dados de saúde e compartilhamento.

Não obstante o enquadramento do tratamento proposto em uma das bases legais, o controlador ainda assim está sujeito à observância dos princípios da lei, e com a sensibilidade inerente ao tema da saúde, há de se dispensar especial atenção aos princípios da finalidade, adequação, necessidade e transparência.

Exemplos práticos

Acidente: situação em que o titular sofre um acidente e é levado inconsciente ao hospital. Neste caso, para poder atendê-lo da maneira adequada, os médicos deverão acessar seu histórico de saúde e ter acesso a dados pessoais e dados sensíveis, no entanto, respeitando os demais princípios da LGPD e também levando-se em consideração restrição de acesso, ou seja, apenas deve ter acesso aos dados aquele que efetivamente necessitar.

- ***Internação hospitalar de urgência:*** eventuais situações em que for necessário priorizar a integridade psicofísica do titular ou do terceiro, sobrepondo-se ao exercício de sua autonomia, seja por incapacidade ou pela urgência da situação.

- ***Programa de Vacinação:*** as empresas podem promover campanhas de vacinação para os seus colaboradores. O objetivo de tal campanha é promover medidas preventivas a doenças e, portanto, o tratamento de dados para essa finalidade poderá ser enquadrado nesta base legal. Importante destacar que o tratamento realizado pelas empresas dos dados pessoais dos colaboradores é justificado por essa base legal, ao passo que o tratamento relacionado à vacina em si – realizada por profissionais de saúde – poderá ser enquadrado em tutela da saúde.

8. Tutela da saúde

Com relação à saúde, a LGPD traz em seu artigo 7, inciso VIII a tutela da saúde como base legal para tratamento de dados pessoais, sendo aplicável exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Além disso, a tutela da saúde também aparece como base legal para tratamento de dados sensíveis (artigo 11, II, "f"), mas apenas nos casos em que o consentimento não for possível e quando o tratamento do dado sensível seja indispensável para a tutela da saúde.

O intuito da lei é justamente o de preservar os titulares e privilegiar a saúde, mesmo em casos em que não seja obtido previamente o consentimento, seja em prol do interesse público, seja em razão da impossibilidade prática de fazê-lo.

Para disciplinar o assunto, a LGPD veda o compartilhamento de dados de saúde entre controladores com o objetivo de obter vantagem econômica, exceto nas hipóteses relativas a (i) prestação de serviços de saúde; (ii) de assistência farmacêutica; (iii) de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia em benefício dos interesses dos titulares de dados; (iv) para permitir a portabilidade de dados quando solicitada pelo titular; ou (v) permitir as transações financeiras e administrativas resultantes do uso e da prestação dos serviços mencionados anteriormente.

Ainda, é vedado às operadoras de planos privados de 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. Tal vedação, a princípio vai de encontro à atual regulamentação da ANS, sendo que

o diálogo com a legislação setorial é de suma importância para o setor e para a segurança jurídica dos titulares.

Exemplos Práticos

Tratamento ou procedimento realizado por profissionais de saúde: por exemplo, em atendimento médico ou abertura de prontuário.

***Serviço de saúde*:** realização de exame médico ou envio de dados para análise laboratorial.

9. Legítimo Interesse

O legítimo interesse é, entre as bases legais previstas no artigo 7º da LGPD aquela que poderá levantar os maiores questionamentos, pois, apesar de ter sua definição escrita em lei, esta é bastante ampla, sem a certeza jurídica esperada de um conceito jurídico. O conceito de "interesse" está intimamente relacionado, porém ainda é distinto, do conceito de "propósito". Neste âmbito de proteção de dados pessoais, “propósito” seria o motivo, a finalidade, o objetivo pelo qual os dados são tratados, enquanto “interesse” é a participação ampla que o controlador possa ter durante o tratamento, ou o benefício que tanto o controlador quanto a sociedade possam obter com o tratamento desses dados.

A natureza desse interesse legítimo pode variar. Em alguns casos, ele é em prol da sociedade, como por exemplo, o interesse da imprensa em publicar informações sobre o governo, investigar casos de corrupção ou realizar análises de fraude. Em outros casos, o interesse legítimo beneficia menos a sociedade como um todo e mais a empresa que efetua o tratamento de dados pessoais, como por exemplo, quando uma empresa deseja saber o máximo possível sobre seus clientes em potencial para direcionar melhor anúncios sobre seus produtos ou serviços, fomentando seu negócio. (EC, 2014)

Bastaria, então, uma empresa alegar que possui um interesse legítimo para encontrar respaldo legislativo para tratar dados pessoais?

Em outras palavras, o que delimitaria de fato – e na prática – um interesse legítimo?

Para responder a essas questões é importante ressaltar que a LGPD possui como base o Regulamento Geral de Proteção de Dados Pessoais da União Europeia (“GDPR”) que carrega consigo 173 considerandos, os quais dissertam sobre sua aplicabilidade em diversos cenários, criando interpretações práticas

ao texto legal genérico. Alguns considerandos que versam sobre o legítimo interesse são:

> (47) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta.
>
> (48) Os responsáveis pelo tratamento que façam parte de um grupo empresarial ou de uma instituição associada a um organismo central poderão ter um interesse legítimo em transmitir dados pessoais no âmbito do grupo de empresas para fins administrativos internos, incluindo o tratamento de dados pessoais de clientes ou funcionários. Os princípios gerais que regem a transmissão de dados pessoais, no âmbito de um grupo empresarial, para uma

> empresa localizada num país terceiro mantêm-se inalterados.
>
> (49) O tratamento de dados pessoais, na medida estritamente necessária e proporcionada para assegurar a segurança da rede e das informações, ou seja, a capacidade de uma rede ou de um sistema informático de resistir, com um dado nível de confiança, a eventos acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais conservados ou transmitidos, bem como a segurança dos serviços conexos oferecidos ou acessíveis através destas redes e sistemas, pelas autoridades públicas, equipas de intervenção em caso de emergências informáticas (CERT), equipas de resposta a incidentes no domínio da segurança informática (CSIRT), fornecedores ou redes de serviços de comunicações eletrônicas e por fornecedores de tecnologias e serviços de segurança, constitui um interesse legítimo do responsável pelo tratamento. Pode ser esse o caso quando o tratamento vise, por exemplo, impedir o acesso não autorizado a redes de comunicações eletrônicas e a distribuição de códigos maliciosos e pôr termo a ataques de (negação de serviço) e a danos causados aos sistemas de comunicações informáticas e eletrônicas. (EU, 2016)

Como se vê, o fato do responsável pelo tratamento de dados pessoais possuir um legítimo interesse para o tratamento é apenas um ponto inicial para a análise da viabilidade da utilização da hipótese do artigo 6º, (f) do GDPR, sendo necessário analisar outros pontos, tais como indicados na redação do considerando 47.

Existem três elementos que justificam o uso do legítimo interesse, normalmente analisados como um teste de três partes, que consiste em: (i) identificar um interesse legítimo (teste da finalidade); (ii) mostrar que o tratamento é necessário para alcançá-lo (teste de necessidade); e (iii) equilibrá-lo contra os interesses, direitos e liberdades do indivíduo (teste de proporcionalidade).

É possível encontrar o teste de três partes na redação do artigo 10º da lei, conforme destacado abaixo:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas (***teste de finalidade***), consideradas a partir de situações concretas, que incluem, mas não se limitam a:

> I - apoio e promoção de atividades do controlador; e
> II - 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, nos termos desta Lei (***teste de proporcionalidade***).
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. (***teste da necessidade***)
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial. (BRASIL, 2018)
> Grifos nossos

Então, ao determinar o Legítimo Interesse na coleta e tratamento de dados pessoais, a empresa precisa identificar o propósito e analisar a necessidade, avaliando e destacando pontualmente quais dados pessoais serão utilizados e sua forma de tratamento para que, assim, não ocorra compartilhamento excessivo com terceiros ou uma má utilização que fuja da sua finalidade específica. Por fim, a empresa deverá realizar o teste de equilíbrio que leva em consideração a análise dos direitos, liberdades ou interesses fundamentais do titular dos dados.

Destaca-se que pelo artigo 10º da LGPD, o rol de finalidades não é taxativo, ao contrário, se encontra em uma linha exemplificativa. Além disso, as condições acima referem-se tão somente ao controlador, restando ausente qualquer extensão ao interesse legítimo do terceiro, resultando assim, em uma lacuna a ser esclarecida pela ANPD quanto ao atendimento ou não desses requisitos como base legal para terceiros.

Este ponto foi discutido por Marcel Leonardi ao explicar:

> "O legítimo interesse de terceiros engloba não apenas os terceiros em uma relação negocial, mas também a própria sociedade amplamente considerada, ou seja, o legítimo interesse de categorias de pessoas ou mesmo de toda a população, conforme o caso. No universo das atividades empresariais, a utilização do legítimo interesse como base legal de tratamento de dados pessoais pode ser, em tese, justificada por múltiplas perspectivas: do controlador, de terceiros e do titular. No entanto, cada

situação demandará uma análise específica, o que varia conforme o caso.” [7]

Exemplos Práticos

- ***Prospecção:*** Quando o controlador deseja prospectar novos clientes, é possível justificar este tratamento em legítimo interesse. Isso porque a empresa possui um interesse legítimo de divulgar um serviço ou produto. Desta forma, a empresa realiza o tratamento de dados pessoais a fim de localizar titulares possivelmente interessados em receber tal anúncio. No entanto, para garantir que o titular possua sua expectativa de tratamento alinhada, a empresa precisará dar a opção de “opt-out” (descadastramento da base de dados para marketing), pois, desta forma, caso o titular não possua interesse, a empresa saberá e poderá parar o tratamento para esta finalidade, de forma a sempre respeitar a legítima expectativa dos titulares.

- ***Investigação corporativa:*** Quando o controlador necessita realizar uma investigação interna sobre um ou mais titulares de dados o tratamento poderá ser justificado em legítimo interesse. Isso porque a empresa possui um interesse legítimo em averiguar denúncias e tomar as devidas medidas. O titular, que no caso seria um colaborador, possui a transparência e com isso a legítima expectativa de que seus dados corporativos serão tratados e monitorados a fim de se manter o zelo nas relações de trabalho.

- ***Análise de fraude:*** A sociedade como um todo possui a expectativa legítima de não sofrer fraudes. Portanto, empresas que possuem mecanismos de análise de fraudes podem enquadrar seus serviços em legítimo interesse. Afinal, é de interesse legítimo de todos que as ocorrências de fraudes sejam mitigadas.

- ***Análise Comportamental:*** Empresas podem estudar o comportamento dos usuários em suas plataformas/aplicativos com a finalidade de oferecer produtos e/ou serviços que sejam do interesse específico de cada usuário. Essas análises devem ser transparentes aos seus usuários. Exemplo disso: seleção de *playlists* específicas do Spotify com base no gosto musical de cada usuário.

[7] LEONARDI, M. Principais Bases Legais de Tratamento de Dados Pessoais no Setor Privado. In: LUCCA, N., FILHO, A.S., LIMA, C.R.P., MACIEL, M, M. (Org.). Direito & Internet IV: Sistema de Proteção de Dados Pessoais Cirurgia Vascular,1. ed. São Paulo: 2019. cap. 14, p.327

10. Proteção ao crédito

A base legal de proteção ao crédito é uma base inovadora em regulações de proteção de dados pessoais.

A LGPD em seu artigo art. 7º, X, assim dispõe:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...)
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Note-se que no texto original dos Projetos de Lei apresentados não havia tal base legal, que foi incluída apenas no texto substitutivo apresentado no Parecer proferido em 28/05/2018 pela comissão especial do PL nº 4060/2012 (no qual o PL nº 5276/16 foi apensado), sob o seguinte fundamento[8]:

> [Art. 7º] – Hipóteses de tratamento
> Cotejando os Projetos de Lei em análise propomos dez hipóteses para o tratamento de dados pessoais, sendo, a principal delas, mediante a obtenção de consentimento livre, informado e inequívoco. Prevemos o tratamento no cumprimento de obrigação legal, regulatória, contratual, estudos, processos judiciais, entre outros. **Ademais, julgamos pertinente incluir (inciso X) recepção expressa à possibilidade de abertura de cadastro de consumidores para proteção do crédito, tal como consagrada no art. 43 do Código de Defesa do Consumidor.**

O texto proposto previa o seguinte:

> X – para proteção do crédito de acordo com o art. 43 da Lei no 8.078, de 11 de setembro de 1990, que dispõe sobre a proteção do consumidor.

Este texto foi encaminhado para aprovação do Senado e o Relator, Senador Ricardo Ferraço, apresentou parecer favorável ao substitutivo, com algumas alterações, dentre elas a alteração do inciso X do art. 7º[9]:

> I) Alteração no art. 7º, inc. X.
> A melhor técnica legislativa recomenda a remissão expressa de lei quando indispensável à disciplina do alcance da norma ou para afastar obscuridades redacionais. Do contrário, assim não sendo, a redação

[8] https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=22C2323ABCE9B5C09FF7E82A9AF982FE.proposicoesWebExterno1?codteor=1663305&filename=Tramitacao-PL+4060/2012 - Acesso em 18 de maio de 2020.

[9] https://legis.senado.leg.br/sdleg-getter/documento?dm=7751566&ts=1571776637073&disposition=inline. Acesso em 18 de maio de 2020.

> atrai insegurança jurídica, tornando dificultosa a aplicação da lei. **No caso presente, a proteção de crédito, como base para o tratamento de dados, tem um arcabouço legislativo que vai além do disposto no CDC, como, por exemplo, a própria Lei do Cadastro Positivo. Daí ser mais adequada a referência complementar da lei pertinente.**

A partir das alterações propostas, podemos identificar que a restrição antes imposta no contexto exclusivo para justificar a formação de cadastros de consumidores, nos termos do CDC, para a base legal de proteção ao crédito, foi acertadamente excluída para que a base legal de proteção ao crédito pudesse ser considerada em outras situações que não apenas a formação de cadastros com base no art. 43 do CDC.

Contudo, mesmo que o texto final tenha sido alterado, ainda pairam dúvidas sobre como a ANPD, o Judiciário e a doutrina irão interpretar a amplitude dos contextos de tratamento de dados pessoais em que será possível ao controlador utilizar tal base legal, bem como se haverá algum tipo de restrição sobre quais dados pessoais poderiam eventualmente serem tratados neste escopo.

Isto porque, se adotarmos uma interpretação restritiva, estaríamos diante de um escopo de aplicação restrito aos cadastros de inadimplentes (CDC) e adimplentes (cadastro positivo), em que a base de proteção ao crédito somente poderia ser utilizada para tais fins e os dados pessoais tratados envolvem apenas o escopo de dados de adimplência e inadimplência, visto que a existência destes cadastros foi claramente o propulsor para que tal base legal fosse incluída na LGPD.

Por outro lado, podemos verificar que existem diversas outras situações em que há o tratamento de dados pessoais não inseridos no contexto dos cadastros de inadimplentes e adimplentes que, por sua vez, tem por finalidade reduzir riscos financeiros, não apenas em operações específicas de crédito de forma direta, como por exemplo, vendas a prazo, ofertas de produtos de crédito, serviços com pagamento posterior a sua prestação, cuja finalidade encontra-se intimamente ligada com a proteção ao crédito.

Exemplo desta interconexão foi posto pelo Exmo. Ministro Paulo e Tarso Sanseverino em seu voto proferido quando da análise da legalidade do *credit scoring* no REsp 1419697 / RS[10] :

---

10 https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=39037908&num_registro=201303862850&data=20141117&tipo=51&formato=PDF. Acesso em 18 de maio de 2020.

> Relembre-se que, até hoje, antes da celebração dos contratos tradicionais (v.g. compra e venda de um imóvel), em um período pré-contratual, é realizada pelos interessados uma avaliação recíproca da idoneidade da outra parte e de sua capacidade financeira de honrar o negócio jurídico a ser celebrado.
> Essa avaliação do risco de celebração do contrato envolve um conhecimento da pessoa do outro contratante, do objeto do contrato e do próprio conteúdo do contrato a ser celebrado, fazendo-se, assim, uma análise recíproca do risco do negócio a ser celebrado (risco do crédito).

Ademais, importa ressaltarmos que não apenas dados de inadimplência e adimplência são tratados para a análise de crédito. Exemplo disto são os scores de crédito que não utilizam apenas dados de adimplência e inadimplência para sua composição e, inclusive não constitui banco de dados, conforme definido pela Súmula nº 550 do STJ.

Exemplos Práticos

Interpretação restritiva: Criação de banco de dados de cadastros de inadimplentes e adimplentes; e Compartilhamento de dados pessoais constantes em banco de dados de cadastros de inadimplentes e adimplentes para avaliação do risco de crédito quando o Titular solicita um empréstimo ou financiamento.

Interpretação extensiva: Avaliação de crédito, com utilização de dados pessoais de composição de patrimônio, dados de inadimplência e adimplência, para que o Titular possa contratar serviço pós pago; e Avaliação de crédito do Titular cliente de Instituição Financeira para que a Instituição possa oferecer crédito pré-aprovado de cheque especial.

III. Tratamento de Dados Pessoais sensíveis

O artigo 11 da LGPD traz o rol de hipóteses que autorizam o tratamento de dados pessoais sensíveis, sendo o **consentimento** a base legal principal nesse caso, devendo ocorrer de forma específica e destacada, para finalidades específicas.

O tratamento desses dados, também é possível **sem fornecimento de consentimento** do titular, nas hipóteses em que for **indispensável** para uma das seguintes opções: (i) cumprimento de obrigação legal ou regulatória pelo controlador; (ii) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; (iii) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; (iv) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; (v) proteção da vida ou da incolumidade física do titular ou de terceiro; (vi) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; (vii) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (viii) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

A seguir, detalharemos as aplicações práticas dessas bases legais, que poderão ser aplicadas quando forem indispensáveis para a realização do tratamento.

1. Consentimento

Como mencionado, o consentimento é a base legal principal para tratamento de dados pessoais classificados como sensíveis. No caso do tratamento de dados sensíveis, a lei qualifica o consentimento de forma diversa da prevista ao tratamento de dados pessoais em geral, enaltecendo a necessidade de o consentimento ser específico, inequívoco e expresso e para finalidades determinadas (art. 11, I).

Para mais informações sobre a utilização da base legal de consentimento, vide item II.1, acima.

2. Cumprimento de obrigação legal ou regulatória

Da mesma forma como ocorre com os dados pessoais em geral, dados pessoais sensíveis poderão ser tratados para fins de cumprimento de uma obrigação ou regulatória pelo controlador.

Para mais informações sobre a utilização dessa base legal e exemplos de sua aplicação prática, vide item II. 2, acima.

3. Tratamento compartilhado de dados necessários à execução, de políticas públicas

A LGPD autoriza o tratamento de dados pessoais sensíveis quando estes forem indispensáveis para tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos.

Para mais informações sobre a utilização da base legal pelo poder público, vide item II. 3, acima.

4. Estudos por órgão de pesquisa

Da mesma forma como ocorre com os dados pessoais em geral, dados pessoais sensíveis poderão ser tratados para fins de realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis.

Para mais informações sobre a utilização dessa base legal e exemplos de sua aplicação prática, vide item II. 4, acima.

5. Exercício regular de direitos, inclusive em contrato e em processo

Como já mencionado, o artigo 11 da LGPD traz em seu inciso II, "d" a hipótese legal de exercício regular de direitos como possibilidade de tratamento de dados sensíveis sem consentimento do titular, mas apenas quando o uso dos dados sensíveis for indispensável para que se alcance o regular exercício de direitos e ainda assim em estrita observância aos princípios previstos no artigo 6 da LGPD.

A redação do dispositivo legal mencionado acima, estabelece, atualmente, que o tratamento de dados pessoais sensíveis pode ocorrer sem o consentimento do titular nas hipóteses em que for indispensável para:

> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem).

Analisando-se as alterações propostas ao texto do PL 5.276/2016 até o texto final da LGPD, é possível notar que a redação inicial deste inciso não contemplava menção expressa a contrato, mas limitava-se a estabelecer "exercício regular de direitos em processo judicial ou administrativo".

A adição do termo "inclusive em contrato" acabou sendo uma forma didática de evitar eventuais dúvidas advindas do uso de contrato para o exercício regular de um direito, mas, em realidade, se há um direito a ser exercido, pouco importa se aquele que necessitar valer-se de tal direito tiver amparo em contrato ou processo, e que demande para isso tratamento de dados pessoais sensíveis, caso indispensável para fazer valer de fato o direito em voga. Tal direito há de ter reconhecida também sua existência, e há de ser lícito o tratamento de dados sensíveis para essa finalidade.

No entanto, uma vez que não há hipótese legal de tratamento de dados sensíveis para a execução de contrato ou de procedimentos preliminares, o exercício regular de direitos não engloba procedimentos preliminares à execução do contrato. Aqui há de ficar claro que não há referência expressa ao inciso V do artigo 7 da LGPD, portanto, inaplicável uma interpretação extensiva para possibilitar o tratamento de dados sensíveis para procedimentos preliminares à execução do contrato.

Considerando que existem inspirações da LGPD na GDPR, o Regulamento Europeu serve como fonte de estudo para algumas disposições que apresentam similaridade (sempre com o devido cuidado de considerar as características da legislação e do próprio mercado brasileiro). Ocorre que a hipótese de tratamento de exercício regular de direitos é uma das que não possui correspondente idêntico no GPDR nas categorias de bases legais, mas que, ainda assim, é citada como uma das exceções para que seja lícito o tratamento de categorias especiais[11] de dados pessoais, que compreende os dados sensíveis.

O GDPR é expresso ao determinar que o tratamento de dados pessoais sensíveis não será proibido se uma das hipóteses do parágrafo 2 do artigo 9 for aplicável, dentre elas a hipótese prevista na alínea (f) "*processing is necessary*

[11] Art. 9 (1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity."

Ao discorrer sobre o que seria a defesa em ações judiciais, a Autoridade de Proteção de Dados Pessoais do Reino Unido, o ICO (*Information Commissioner's Office*)[12] estabelece que este conceito não se limita a um procedimento judicial já em andamento, podendo tal hipótese de tratamento ser interpretada abrangendo procedimentos judiciais futuros, obtenção de orientação jurídica ou outra forma de defesa legal para exercício de direitos.

Por fim, com relação ao uso de dados pessoais sensíveis como prova em processo judicial, vale apenas lembrar que devem ser usados quando forem indispensáveis para a defesa do controlador e, em casos práticos, vale considerar a necessidade de requerer ao juiz segredo de justiça para que os dados fiquem de fato disponibilizados apenas para que cumpram determinada finalidade, e também para evitar que mais pessoas tenham acesso, protegendo-se assim o titular dos dados.

Exemplos Práticos

- ***Prova em processo judicial:*** pode ser necessário acostar aos autos de processo administrativo, judicial ou arbitral um documento que contenha dados pessoais sensíveis.

- ***Compartilhamento de dado entre o hospital e plano de saúde:*** Situação em que o titular de dados é cliente de um determinado plano de saúde e precisa realizar exames em rede hospitalar. Nessa ocasião, o hospital poderá compartilhar os dados pessoais (incluindo sensíveis) como o plano de saúde, por exemplo, para validação e aprovação do plano de saúde.

6. Proteção da vida ou da incolumidade física

Da mesma forma como ocorre com os dados pessoais em geral, dados pessoais sensíveis poderão ser tratados para fins de proteção da vida ou da incolumidade física do titular ou de terceiros.

Para mais informações sobre a utilização dessa base legal e exemplos de sua aplicação prática, vide item II. 7, acima.

---

[12] ICO. Conditions for processing. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/>. Acesso em 15 de julho de 2020.

7. Tutela da saúde

Da mesma forma como ocorre com os dados pessoais em geral, naturalmente, dados pessoais sensíveis poderão ser tratados para fins de tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Para mais informações sobre a utilização dessa base legal e exemplos de sua aplicação prática, vide item II. 8, acima.

8. Prevenção à fraude e à segurança

O artigo 11 da LGPD dispõe sobre o tratamento de dados sensíveis, que somente poderá ocorrer quando houver o consentimento do titular de dados (inciso I) ou quando for indispensável para o cumprimento de uma das hipóteses previstas no inciso II. Dentre elas, a alínea "g" diz respeito à:

> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Essa base legal se refere, portanto, aos dados sensíveis que serão obtidos quando estes forem indispensáveis para cumprir a finalidade de prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. Nesse sentido, dentre os tipos de dados sensíveis, envolve especialmente o tratamento de dados biométricos que servirão para autenticação e identificação do titular de dados em meios eletrônicos.

Os sistemas biométricos abrangem uma variedade de tecnologias que são utilizadas para atribuir identificadores únicos baseados nas características biológicas de um indivíduo, como as digitais, a retina ou a voz[13] . A definição de dados pessoais sensíveis disposta no artigo 5º, inciso II da LGPD inclui o dado genético e biométrico quando os mesmos são vinculados a uma pessoa natural, no entanto, a lei não trouxe uma definição legal específica para dados biométricos. Por outro lado, o GDPR prevê em seu artigo 4º (14) que os dados biométricos são definidos como "*dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a*

[13] https://www.biometricsinstitute.org/what-is-biometrics/

identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos".

O dado biométrico a ser utilizado pode estar em um formato bruto, como a imagem obtida a partir de uma digital, ou em um formato biométrico, que é a representação das características de um indivíduo extraídas por meio da tecnologia utilizada a partir do formato bruto obtido. Assim como disposto na base legal aqui discutida, os dados biométricos servem principalmente ao propósito de autenticação e identificação. No caso de identificação, se relaciona ao ato de individualizar o titular de dados, identificando-o de forma única, efetiva e comprovada. No caso de autenticação, se relaciona com o ato de confirmar a identidade do titular de dados, ou seja, verificar se o mesmo é o indivíduo que alega ser.

Cabe observar, ainda, que essa base legal se refere à identificação e à autenticação de cadastro em sistemas eletrônicos, o que é compreensível se lembrarmos da definição de sistemas biométricos e da utilização de tecnologia para gerar identificadores únicos para as características biológicas do titular de dados.

Importante notar que, por determinação expressa dessa base legal, é indispensável que haja um balanceamento entre a finalidade pretendida e os direitos do titular resguardados no artigo 9º e demais direitos e liberdades fundamentais do titular de dados que exijam a proteção dos dados pessoais. Ou seja, não se pode realizar o tratamento focando somente na finalidade de prevenção à fraude e à segurança do titular. Deve-se ter em mente o respeito aos direitos do titular, levando-se em consideração, principalmente, os riscos a estes direitos e liberdades fundamentais que podem ser acarretados.

Por conta de tais determinações, o princípio do livre acesso (art. 6º, IV) e da transparência (art. 6º, VI) ganham uma importância ainda maior no contexto dessa base legal, pois o titular de dados deve ter garantido o seu direito de obter informações, de forma facilitada, sobre a forma, a duração, os agentes de tratamento e todo o contexto envolvendo o tratamento de seus dados pessoais, como forma de resguardar e proteger seus direitos previstos no artigo 9º.

Ressalta-se que essa base legal não possui correspondência com nenhuma das bases gerais para tratamento de dados dispostas no artigo 7º da LGPD, embora exista uma aproximação quanto a base relativa ao legítimo interesse (art. 7º, IX). Essa aproximação ocorre porque, assim como a base legal referente ao legítimo interesse, a base relativa à prevenção à fraude exige uma ponderação entre a finalidade pretendida e aos direitos e liberdades fundamentais do titular de dados, conforme já mencionado.

Exemplos Práticos

Quanto aos exemplos de aplicação prática dessa base legal, cabe realizar primeiramente algumas observações. A primeira é quanto à finalidade com que a mesma será utilizada. Conforme leitura do artigo 11, II e da alínea "g", a garantia de prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos deve ser indispensável para o enquadramento nesta hipótese. Isso faz com que não haja muita margem para enquadramento nessa hipótese, pois o texto da lei intencionalmente já faz com que a finalidade funcione de forma mais restritiva para cumprimento.

Além disso, é importante alertar para a importância do equilíbrio entre a real necessidade de enquadramento nessa hipótese para prevenção à fraude e os direitos e liberdades do titular de dados. Isso significa dizer que a sua aplicação deverá levar em conta esse balanço e não apenas o interesse do controlador em utilizá-la para fins de prevenção à fraude. Um exemplo dessa aplicação errônea é utilizar tal base legal quando se poderia realizar a identificação do titular com outros dados pessoais (não sensíveis, quando possível) que alcançariam da mesma forma a finalidade pretendida.

Na base aqui discutida, é importante que se tenha a certeza de que os dados a serem tratados serão realmente indispensáveis para se alcançar a finalidade de prevenir fraudes e de resguardar a segurança do titular. É, portanto, utilizada em um contexto em que se necessita de mais segurança para a correta identificação e autenticação de titular de dados, também levando-se em consideração o cumprimento do princípio da necessidade. Além disso, deve-se observar o período de conservação dos dados coletados, de forma que os mesmos sejam excluídos após o término do tratamento (art. 16).

Alguns exemplos práticos de aplicação dessa base legal são:

- ***Criação de conta digital, utilizando aplicativos de celular:*** Essa base legal pode ser bastante aproveitada em contextos em que se necessite prevenir fraudes em processos de identificação ou confirmação de identidade por meio de aplicativos utilizados nos smartphones, como, por exemplo, para criação de uma conta digital.

- ***Confirmação de transações bancárias:*** Neste caso, geralmente utilizadas por meio de reconhecimento facial ou impressão digital no intuito de confirmar a identidade do titular de dados.

- ***Prestação de serviço de plano de saúde:*** Utilizada nesse caso para autenticação de identidade para prevenir fraude na prestação de serviços a serem utilizados pelo beneficiário de plano de saúde.

- ***Acesso a locais restritos:*** Tanto para identificar quanto para autenticar, como forma de permitir o acesso do titular de dados a um local de acesso privativo. Importante ressaltar que o tratamento deve levar em consideração a real necessidade do uso dos dados biométricos, ou seja, especialmente no caso de o uso de dados não sensíveis não ser efetivo o suficiente para proteção à fraude e à segurança do titular.

IV. Tratamento de dados de crianças e adolescentes◇◇◇

A LGDP, em observância as leis que a precedem, Constituição Federal e Estatuto da Criança e do Adolescente (ECA) - que estabelecem garantias adicionais as crianças e aos adolescentes tratou de maneira diferenciada este grupo de vulneráveis, estabelecendo que o tratamento dos dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse e estabeleceu que, no caso de crianças, deverá ser realizado mediante consentimento específico, em destaque dado por pelo menos um dos pais ou pelo responsável legal (que deverá, por meio de todos os esforços razoáveis, ser verificado para confirmação de que foi de fato dado pelo responsável da criança, consideradas as tecnologias disponíveis). Além disto, a LGPD enalteceu algumas das obrigações do controlador, como o de primar pela transparência, mantendo de maneira pública a informação sobre os tipos de dados coletados da criança e do adolescente, a forma de utilização e os procedimentos para revogar o consentimento, dentre outras responsabilidades.

No que se refere à GDPR, importante ressaltar que esta estabeleceu um tópico especial para proteger os dados de crianças, permitindo, todavia, que o consentimento do detentor da responsabilidade parental não seja necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança. De forma semelhante, a LGPD também incluiu uma ressalva para a coleta de dados pessoais de crianças sem consentimento parental, quando ocorrer para fins de sua proteção e salvaguarda, bem como quando necessária para contatar os pais ou o responsável legal, desde que utilizados uma única vez e sem armazenamento.

Ainda neste contexto e no melhor interesse das crianças e adolescentes, a LGPD estabeleceu regras específicas a serem observadas na disponibilização de jogos, aplicações de internet ou outras atividades oferecidas, a participação dos vulneráveis não deve estar condicionada à coleta de seus dados pessoais, salvo quando estritamente necessário à atividade oferecida.

V. Conclusão

A LGPD é, por vezes, de maneira equivocada vista como uma lei que potencialmente restringiria as entidades públicas e privadas de realizarem tratamento de dados pessoais da forma como faziam anteriormente, quando, na realidade, ela apenas procura regulamentar os tratamentos, inclusive flexibilizando as possibilidades para o tratamento adequado de dados pessoais, legitimando-as.

Tanto é que a lei criou a figura de dez bases legais para dados pessoais em geral (exceto sensíveis) e oito bases legais para dados sensíveis, a serem analisadas e aplicadas conforme cada contexto de tratamento de dados.

A aplicação adequada das bases legais é um ponto de extrema relevância para o cumprimento adequado da LGPD e de leis de proteção de dados pelo mundo, sendo, inclusive, o tipo de penalidade mais aplicada em relação ao GDPR, com um total de 125 multas pautadas na insuficiência de base legal para o GDPR (considerando até o início de julho de 2020).

Além desse aspecto, a utilização adequada das bases legais é mais uma forma de proporcionar ao titular a efetivação de sua proteção, já que seus dados serão pautados em hipóteses legítimas e específicas trazidas pela lei, com a sua devida regulamentação e evitando excessos e injustiças.

Dada a relevância do tema, para facilitar a aplicação prática e disseminar o conhecimento sobre essas hipóteses de tratamento de dados pessoais trazidas pela LGPD, buscamos, de forma não exaustiva, por meio do presente e-book, trazer uma visão explicativa das bases legais, suas controvérsias e os principais pontos de discussão sobre o tema.

Créditos

Autoras

Fernanda Maia
Advogada especializada em
Direito Digital e Proteção de Dados
Coordenadora Leonardi Legal Learning
Co-Fundadora LGPD Acadêmico

Aline Fachinetti
Advogada
Fellow of Information Privacy
Co-fundadora Juventude Privada

Adriana Wagatsuma
Executiva Jurídico
Compliance & DPO
IAPP Member

Mariana Caparelli
Advogada especializada em
Direito Digital e Proteção de Dados
IAPP Member
Data Protection Officer

Angela Rosso
Cientista da Computação
especialista em Direito Digital
Co-fundadora LGPD Acadêmico

Rachel Gonzaga
Advogada especialista em
Direito Empresarial e Direito Digital
CIPP/E

Nuria Baxauli
Advogada especializada em
Tecnologia e Proteção de Dados
Mestranda na Tilburg University

Amanda Alencar
Advogada especializada em
Direito Digital e Proteção de Dados
CIPP/E

Autoras por Capítulo

Fernanda Maia
Cumprimento de obrigação legal ou regulatória
Proteção da vida ou incolumidade física
Legítimo interesse

Adriana Tocchet Wagatsuma
Consentimento
Tratamento de dados de crianças e adolescentes

Angela Maria Rosso
Execução de Políticas Públicas

Aline Fuke Fachinetti
Estudos por órgão de pesquisa

Núria Baxauli
Execução de contrato ou procedimentos preliminares

Mariana de Souza Cruz Caparelli
Exercício Regular de Direitos
Exercício Regular de Direitos, Inclusive em Contrato
Tutela da saúde

Rachel Rosa Gonzaga
Proteção ao crédito

Amanda Alencar
Prevenção à fraude e à segurança

Revisão

Marcel Leonardi
Sócio de Leonardi Advogados
Fundador Leonardi Legal Learning
CIPP/E
CIPP/US

Essa é a versão 1.0 do e-book, atualizada até julho de 2020. O e-book será atualizado conforme novos regulamentos e recomendações sejam emitidos pela autoridade competente.

Estamos em constante aprimoramento de nossos materiais. Se quiser enviar uma sugestão ou comentário para o ***LGPD Acadêmico****, contate-nos por meio de nossas redes sociais.*

Material elaborado pelo LGPD Acadêmico - Creative Commons

Publicado em 19.08.2020