OAB SÃO PAULO | Subseção Santos

LGPD E OS DIREITOS DOS TITULARES

CONHEÇA OS PODERES DE SUA AUTODETERMINAÇÃO INFORMATIVA

OAB SANTOS | Tempo de se conectar | GESTÃO 2022 • 2024 | 90 OAB SANTOS

ORDEM DOS ADVOGADOS DO BRASIL • SUBSEÇÃO SANTOS

RAPHAEL MEIRELLES
PRESIDENTE OAB/SANTOS

SERGIO FERNANDES MARQUES
VICE PRESIDENTE OAB/SANTOS

LEONARDO OLIVEIRA RAMOS DE ARAÚJO
SECRETÁRIO GERAL

JACKELINE PEREIRA DA SILVA
SECRETÁRIA GERAL ADJUNTA

DANIELLA LAFACE BORGES BERKOWITZ
TESOUREIRA

COMISSÃO DE PRIVACIDADE E PROTEÇÃO DE DADOS

JULIANE PASCOETO CAVALINI
PRESIDENTE

CAMILA STUDART
VICE PRESIDENTE

MARIANA SBAITE GONÇALVES
SECRETÁRIA

COORDENAÇÃO:

JULIANE PASCOETO CAVALINI

COLABORAÇÕES:

CAROLINA MOURA CAMPOS
LARA ISABEL MARCON SANTOS
LEONARDO GUTIERREZ ALVES
MANOEL RICARDO DE ANDRADE SEBASTIÃO
MATHEUS DOS SANTOS SOUZA BERNARDES
MARINA B. C. STODUTO
NILTON NASCIMENTO RAMOS

DESIGN E EDITORAÇÃO:

CHRISTIAN JAUCH
AGÊNCIA CELEIRO.BMD®

OAB/SANTOS • JUNHO/2023

ÍNDICE

INTRODUÇÃO

VOCÊ CONHECE A LEI GERAL DE PROTEÇÃO DE DADOS?

Certamente já leu algo, ou ouviu falar, sobre a Lei Geral de Proteção, mas você sabe, exatamente, qual a importância da LGPD em nossas vidas?

A LGPD trouxe regulamentação sobre a coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais gerenciados por empresas ou pessoas físicas que exercem atividade econômica, assim como os direitos que cada um possui em relação aos seus próprios dados.

A LGPD trouxe ao titular de dados a sua autodeterminação informativa, insculpida em um de seus princípios fundamentais.

VAMOS ENTENDER ALGUNS DOS CONCEITOS TRAZIDOS PELA LGPD?

TITULAR DE DADOS

O titular que é a pessoa natural a quem se refere os dados pessoais.

DADOS PESSOAIS

O conceito de dados pessoais está no artigo 5º da LGPD e dispõe que é toda informação que torna a pessoa identificada ou identificável, ou seja, que permite saber quem você é.

Esse dado é relacionado somente a pessoa natural (física), como por exemplo: nome, filiação, data de nascimento, RG, CPF, endereço, e-mail, ou qualquer outra informação que permita identificar a pessoa física.

DADOS SENSÍVEIS

Os dados sensíveis são relacionados a intimidade do cidadão e por isso eles demandam uma proteção maior. Podemos citar como exemplo as informações relacionadas a: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

DADO ANONIMIZADO (ANÔNIMOS)

São dados relativos ao titular que não poderá ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento. Esses dados estão fora da proteção da LGPD.

Exemplo: estatísticas sobre a idade de pessoas que realizaram a compra de determinado produto.

AGENTES DE TRATAMENTO
Controlador e Operador

CONTROLADOR
É a pessoa física ou jurídica, de direito público ou privado, que coleta os dados pessoais e toma as decisões em relação a forma do tratamento.

OPERADOR
É a pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

ENCARREGADO

É a pessoa indicada pelo controlador, que atua como canal de comunicação entre as partes (controlador, os titulares e a ANPD – Autoridade Nacional de Dados Pessoais)

OS 10 PRINCÍPIOS DA LGPD

A Lei Geral de Proteção de Dados possui 10 princípios que devem ser seguidos, rigorosamente, pelos agentes de tratamento.
Não existe hierarquia entre eles, portanto, todos precisam ser respeitados, sem exclusão de nenhum.

Vejamos:

1) FINALIDADE

O princípio da finalidade determina que o tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades

Por exemplo: Quando uma loja solicita o seu nome para cadastro e envio de propagandas personalizadas, temos uma finalidade configurada, no entanto, se o seu nome for coletado para outro fim, você deverá ser informado, caso contrário a loja estará em desacordo com a LGPD.

2) ADEQUAÇÃO

O princípio da adequação determina que o tratamento de dados pessoais deve ser compatível para com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

O tratamento de dados pessoais é realizado deve estar em harmonia, ou com ausência de conflitos com os propósitos do tratamento, considerando as peculiaridades, ou o conjunto de circunstâncias que acompanham a realização do tratamento.

Por exemplo: Seria adequado a loja que coletou o seu nome para envio de propagandas, passar a realizar ligações solicitando que você indique um amigo para obter um voucher de desconto?

3) NECESSIDADE

O tratamento de dados pessoais deve ser limitado ao mínimo necessário para o alcance das suas finalidades, abrangendo apenas os dados pertinentes, proporcionais e não excessivos em relação a estas finalidades.

A exigência de que o tratamento de dados pessoais se limite às atividades necessárias, de que os dados tratados sejam relevantes, importantes e apropriados, em quantidade e variedade equilibrada e não exagerada, desmedida, anormal ou abusiva, para alcançar os seus propósitos.

Temos aqui uma palavra chave: MINIMIZAÇÃO.

A empresa ao coletar o seu dado pessoal solicitará o menor número de informações possíveis, pois cada dado coletado exige uma finalidade conectada, e não sendo possível justificar a coleta realizada, teremos comprovada a violação do princípio da necessidade.
Note-se que o princípio da necessidade também é dependente e fortemente entrelaçado com o princípio da finalidade. Apesar de também se tratar de enunciado um pouco mais simples, mas que também iremos destrinchar para facilitar a compreensão.

AQUI TEMOS UM BOM EXEMPLO PRÁTICO:
Uma empresa trata seus dados pessoais com o propósito de “prospectar clientes”, encontra seu perfil profissional na rede social LinkedIn, coleta seu nome e informações de contato, e então, lhe envia um e-mail ou realiza uma ligação, informando onde obteve seus dados e por que motivo, questionando se você teria interesse em marcar uma reunião ou tratar do assunto por e-mail/telefone, ou ainda, se você gostaria de não ser mais contatado, e que a empresa eliminasse seus dados pessoais.

4) LIVRE ACESSO

O princípio do livre acesso determina que os agentes de tratamento de dados pessoais devem garantir aos titulares dos dados que tratam, meios facilitados e gratuitos de consulta sobre a forma e duração do tratamento, bem como à integralidade de seus dados pessoais tratados.

Por meios facilitados, entende-se que os meios devem ser de fácil compreensão e utilização sem dificuldade, já por meios gratuitos, entende-se que os meios não devem requerer pagamento.

Estes meios comumente tomam a forma de um Formulário de Solicitações de Titulares ou de um Portal de Privacidade, ou ainda, através de contato direito com o Encarregado pela Proteção de Dados ou Data Protection Officer (DPO).

Estes meios devem ser disponibilizados aos titulares de dados pessoais para obter informações sobre a forma, isto é, sobre as atividades realizadas durante o tratamento, e a sua duração, ou seja, o seu marco final, que pode ser uma data predeterminada ou uma data determinável.

EXEMPLO DE VIOLAÇÃO:
Uma empresa que não disponibiliza canais de comunicação específicos para o exercício de direitos de titulares, que os disponibiliza mediante cobrança, ou ainda, que os disponibiliza sem se preocupar com a facilidade de compreensão e utilização pelos titulares.

5) QUALIDADE DOS DADOS

O princípio da qualidade dos dados determina que os agentes de tratamento garantam aos titulares dos dados pessoais tratados que sejam exatos, claros, relevantes, atualizados, e de acordo com a necessidade para alcançar as finalidades do tratamento.

Por dados exatos, entende-se que os dados tratados devem ter grande precisão, não podendo conter erros. Já por dados claros, entende-se que estes sejam fáceis de entender, não oferecendo dúvidas ou incertezas. Dados relevantes, por sua vez, implicam que estes sejam importantes, ou seja, que sejam essenciais e necessários. Por dados atualizados, entende-se que estes devem refletir determinada situação em seu momento atual.

A importância de que os dados estejam acordo com a necessidade para alcançar as finalidades do tratamento estabelecendo um referencial de análise, para decidirmos se os dados são suficientemente precisos, fáceis de entender, importantes, essenciais e se refletem a situação a que se referem no momento atual, de modo a alcançar os propósitos do tratamento sem ultrapassar os limites estabelecidos pelo princípio da necessidade.

Exemplo: o titular tem o direito de exigir que os seus dados no cadastro de seu login, ou no cadastro da loja de roupas, ou no cadastro para concorrer a vaga de empregado estejam precisos, corretos, exatos com as suas informações pessoais e qualificações.

6) TRANSPARÊNCIA

O princípio da transparência determina que os agentes de tratamento disponibilizem aos titulares de dados pessoais informações claras, precisas e facilmente acessíveis sobre a realização do tratamento, e informe os respectivos agentes de tratamento, preservados os segredos comerciais e industriais.

Este se trata de um princípio muito similar ao princípio do livre acesso, mas a realidade é que ambos são faces opostas de uma mesma moeda. Enquanto, como explicado anteriormente, o princípio do livre acesso demanda uma postura mais passiva e responsiva das empresas, o princípio da transparência lhes demanda uma postura mais proativa.

Enquanto o princípio do livre acesso se materializa, em geral, através de Formulários de Solicitações de Titulares e Portais de Privacidade, o princípio da transparência, também em geral, se materializa através de Políticas ou Declarações de Privacidade ou Proteção de Dados, ou ainda em Disposições Contratuais, quando pertinente.

Por informações claras, entende-se as informações que são fáceis de entender e que não despertam dúvidas. Já por informações precisas, entende-se as informações que são exatas e que expressam fielmente e com clareza o pensamento. Por fim, por facilmente acessíveis, entende-se que tais informações devem poder ser acessadas sem dificuldade ou esforço pelos titulares.

Sobre as informações em si, devem ser disponibilizadas aquelas sobre a realização do tratamento e sobre os agentes de tratamento envolvidos (todas as empresas que tratam os seus dados pessoais), inclusive em relação ao compartilhamento de dados e transferência internacional.

Exemplo de transparência praticada pelas empresas é a disponibilização de políticas de governanças referentes a privacidade e proteção de dados. Dentre elas temos: Política de Privacidade, Política de Descarte, Política de Comunicação de Incidente de Informação, etc.

É importante que você, titular de dados, exija que as empresas e organizações que tratam dados pessoais disponibilizem, proativamente, aos titulares, informações sobre o tratamento e os agentes de tratamento envolvidos, geralmente, através de uma Política ou Declaração de Privacidade ou Proteção de Dados, ou através de Disposições Contratuais.

7) SEGURANÇA

O princípio da segurança determina que os agentes de tratamento utilizem medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Este princípio se refere à garantia da segurança da informação dos dados pessoais. A segurança da informação é composta por três pilares, a confidencialidade, a integridade e a disponibilidade.

A confidencialidade é o estado da informação que permanece secreta, sigilosa e não divulgada. A integridade é o estado da informação que permanece inteira, que não sofreu diminuição, agressão ou adulteração. A disponibilidade é o estado da informação da qual se pode ter controle ou tomar decisões sobre, e que está em prontidão para utilização.

Acessos não autorizados e situações acidentais e ilícitas de comunicação ou difusão implicam na perda da confidencialidade, situações acidentais ou ilícitas de alteração implicam na perda de integridade, e situações acidentais ou ilícitas de destruição e perda implicam na perda de disponibilidade dos dados pessoais.

Medidas técnicas de segurança se referem a implementação de ferramentas e soluções tecno-

lógicas de segurança, e as medidas administrativas se referem a implementação de processos seguros, programas de treinamento e conscientização, processos de responsabilização disciplinar de colaboradores e medidas de segurança física dos ambientes onde os dados pessoais são tratados.

O objetivo é que as empresas e organizações protejam a confidencialidade, integridade e disponibilidade dos dados pessoais tratados através da adoção de ferramentas e soluções tecnológicas, medidas de segurança física, implementação de processos seguros, de programas de treinamento e conscientização, e de processos de responsabilização disciplinar de colaboradores.

EXEMPLO DE EMPRESA INFRATORA:

Tratar os dados pessoais de seu acervo utilizando cópias falsificadas de sistemas de informação utilizados no tratamento. Não impor a utilização de senhas seguras em equipamentos e aplicações. Não realizar controle de visitantes nas suas instalações físicas. Não proteger salas e compartimentos que armazenam dados pessoais. Não implementar processos seguros. Não treinar ou conscientizar seus colaboradores, e não os responsabilizar pela utilização indevida ou insegura dos dados pessoais.

8) PREVENÇÃO

O princípio da prevenção é, de certa forma, similar ao princípio da segurança, no entanto, seu foco não reside na prevenção da perda da confidencialidade, integridade ou disponibilidade dos dados pessoais tratados, mas, sim, na prevenção da ocorrência de danos aos titulares.

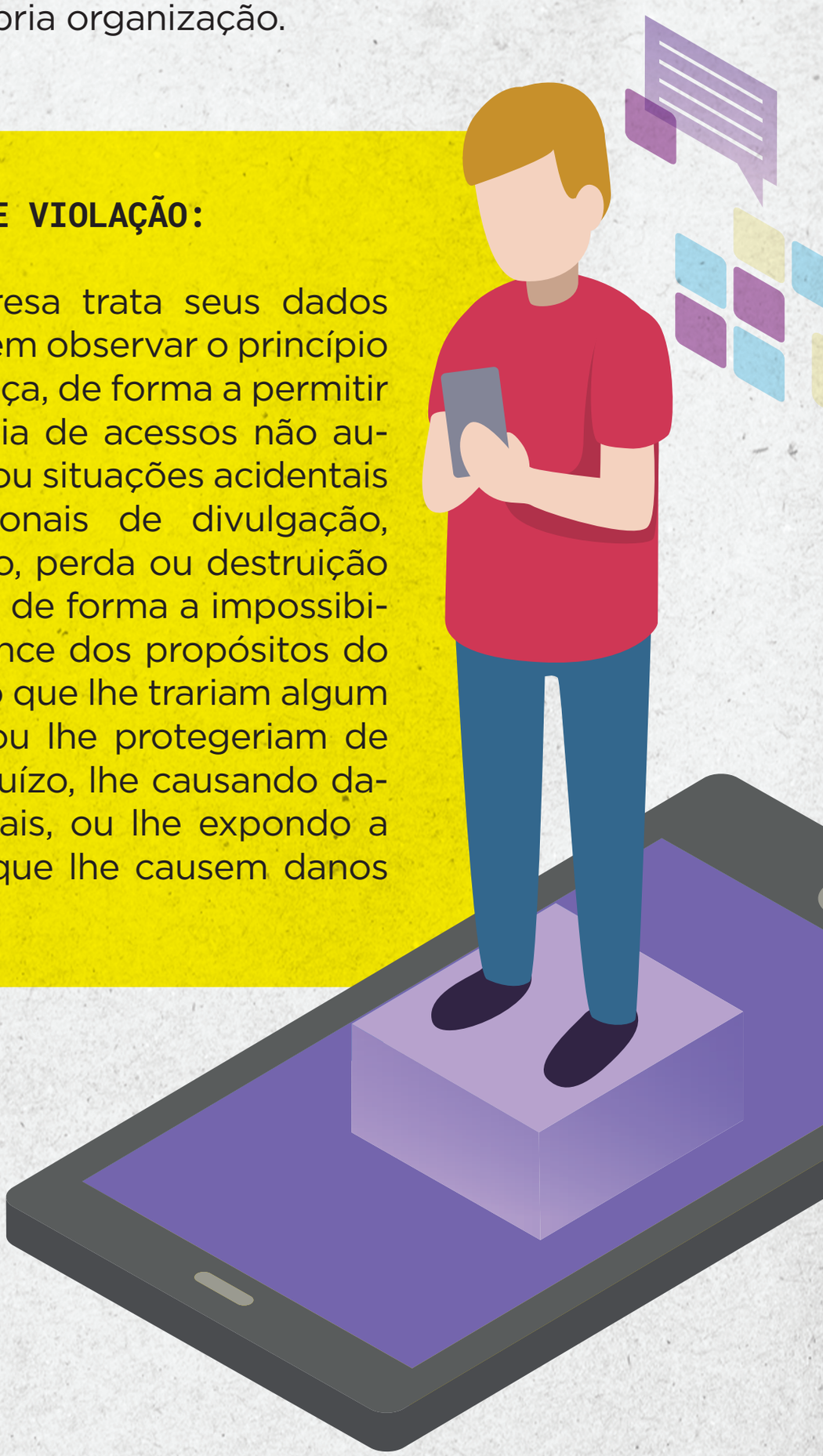
É indiscutível que a perda da confidencialidade, integridade ou disponibilidade, por si só, pode causar danos aos titulares, mas até mesmo um tratamento em que estas características dos dados pessoais não se percam, pode lhes ocasionar danos.

Por danos, entende-se não só danos materiais, mas danos morais também, como qualquer tipo de humilhação, constrangimento, discriminação, exposição da intimidade, dentre outras hipóteses. A princípio, a preservação da

confidencialidade, integridade e disponibilidade dos dados pessoais tratados é um bom começo para se prevenir tais danos, todavia, é importante também que as empresas adotem políticas e processos seguros, e implementem programas também de ética e integridade no tratamento de dados pessoais para prevenir o tratamento indevido dentro da própria organização.

EXEMPLO DE VIOLAÇÃO:

Uma empresa trata seus dados pessoais sem observar o princípio da segurança, de forma a permitir a ocorrência de acessos não autorizados, ou situações acidentais ou intencionais de divulgação, adulteração, perda ou destruição dos dados, de forma a impossibilitar o alcance dos propósitos do tratamento que lhe trariam algum benefício ou lhe protegeriam de algum prejuízo, lhe causando danos materiais, ou lhe expondo a situações que lhe causem danos morais.



9) NÃO DISCRIMINAÇÃO

O princípio da não discriminação proíbe o tratamento de dados pessoais para finalidades discriminatórias ilícitas ou abusivas.

Este é um princípio diretamente relacionado ao princípio da finalidade, que exige que os propósitos do tratamento de dados pessoais sejam justos e razoáveis. Um tratamento com finalidades discriminatórias ilícitas ou abusivas não é um tratamento com propósitos justos e razoáveis.

Popularmente, a expressão discriminação é automaticamente carregada de um significado extremamente negativo, mas a nível de LGPD podemos interpretá-la como o ato de perceber diferenças, distinguir, discernir, colocar à parte por algum critério, classificar, listar.

Desta forma, a discriminação quando é uma discriminação ilícita ou abusiva.

Exemplos de **discriminação ilícita** seriamaquelasrealizadasemrazão de origem étnica ou racial, de gênero, de idade ou de condições de saúde física ou mental. A mera classificação de titulares em razão destas características já viola este princípio, exceto se necessária para o cumprimento de alguma obrigação legal ou regulatória. Por exemplo, a LGPD

dispensa um tratamento diferenciado para dados pessoais de crianças e adolescentes (menores de 18 anos de idade), e Autoridade Nacional de Proteção de Dados (“ANPD”), tem expandido a interpretação da lei para conferir um grau de proteção maior aos idosos (maiores de 60 anos de idade) e pessoas com deficiência (física ou mental).

Exemplos de **discriminação abusiva** seriam a classificação de clientes utilizada para tirar proveito de clientes pouco instruídos e lhes impor condições mais rigorosas de contratação que as oferecidas aos demais, ou a prática de geopricing, que é a definição de preços diferenciados para clientes com base em sua geolocalização

10) RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

O princípio da responsabilização e prestação de contas impõe aos agentes de tratamento a obrigação de demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, bem como a eficácia destas medidas de forma específica.

Este é um princípio que afeta em maior grau a relação das empresas com a ANPD, outras entidades fiscalizatórias setoriais, órgãos de proteção ao consumidor, Sindicatos, Ministério Público do Trabalho e até mesmo perante o Poder Judiciário.

BOM EXEMPLO:
Uma empresa que trata seus dados pessoais desenvolve e mantém atualizada a documentação contendo as características das atividades de tratamento que realiza, compartilhando-as, em tempo hábil, com as autoridades competentes, quando requisitado.

BASES LEGAIS DE TRATAMENTO DE DADOS PESSOAIS

As bases legais fornecem uma estrutura jurídica para o tratamento de dados pessoais, buscando equilibrar a proteção da privacidade dos indivíduos com a necessidade de utilizar esses dados para finalidades legítimas.

Cada base legal tem suas próprias condições e requisitos específicos que devem ser observados para que o tratamento de dados seja considerado lícito.

No que se refere às bases legais, geralmente não é possível atribuir uma para toda a atividade de tratamento. Por vezes o volume e variedade de dados pessoais tratados impede que todos o sejam com fundamento na mesma base legal. Por isso, é essencial que cada tipo de dado pessoal tenha uma base legal atribuída, individualmente e, sendo identificada mais de uma, é necessário atribuir aquela que é mais adequada que as outras.

CONSENTIMENTO

A primeira base legal de tratamento é o Consentimento.

Esta base legal é passível de ser utilizada tanto para o tratamento de dados pessoais comuns como para o de dados pessoais sensíveis.

O consentimento é a primeira base legal de tratamento que vêm à mente da maioria das pessoas quando se pensa em LGPD, mas, em regra, é uma das bases legais mais complexas.

O consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o

tratamento de seus dados pessoais para uma finalidade determinada.

O consentimento, para ser considerado válido, deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular, baseado em uma finalidade determinada, considerando que finalidade genérica incorre em vício de consentimento, tornando-o inválido.

Outro ponto que merece ser discutido é o tratamento de dados pessoais de crianças e adolescentes, que, segundo a lei, deverá ser realizado com o consentimento específico e destacado de pelo menos um dos pais ou responsável legal.

É necessária a renovação do consentimento sempre que as finalidades, a forma e a duração do tratamento, a identificação do controlador e as características do tratamento acerca do uso compartilhado de dados pessoais forem alteradas isoladamente ou em conjunto.

E por fim, o consentimento também pode ser revogado, tema que será abordado posteriormente nesta cartilha.

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA PELO CONTROLADO

(PELO CONTROLADOR)

A segunda base legal de tratamento é o Cumprimento de Obrigação Legal ou Regulatória pelo Controlador.

Esta base legal é passível de ser utilizada, tanto para o tratamento de dados pessoais comuns quanto para o tratamento de dados pessoais sensíveis.

O cumprimento de obrigação legal ou regulatória, é uma base legal de tratamento relativamente simples, ela dispensa a necessidade de se obter o consentimento do titular, desde que a empresa possua alguma obrigação legal ou regulatória. Obrigações legais são aquelas previstas em leis propriamente ditas, obrigações regulatórias são aquelas previstas normas infralegais, como decretos, regulamentos, resoluções, instruções normativas, portarias, dentre outras.

Quando o cumprimento de obrigação legal ou regulatória for a base legal aplicada, é obrigação da empresa identificar a obrigação específica que enseja o tratamento do dado pessoal. Não basta afirmar "tratamos este dado pessoal para cumprir obrigações legais", deve-se afirmar "tratamos este dado pessoal para cumprir com o disposto no art. (X) da Lei (xxxx)".

EXECUÇÃO DE POLÍTICAS PÚBLICAS (PELA ADMINISTRAÇÃO PÚBLICA)

(PELA ADMINISTRAÇÃO PÚBLICA)

A terceira base legal de tratamento é a Execução de Políticas Públicas (pela Administração Pública).

Esta base legal é passível de ser utilizada tanto para o tratamento de dados pessoais comuns como para o tratamento de dados pessoais sensíveis.

O nome completo desta base legal é tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, fazendo-se referência ao capítulo que regula o tratamento de dados pessoais pelo Poder Público.

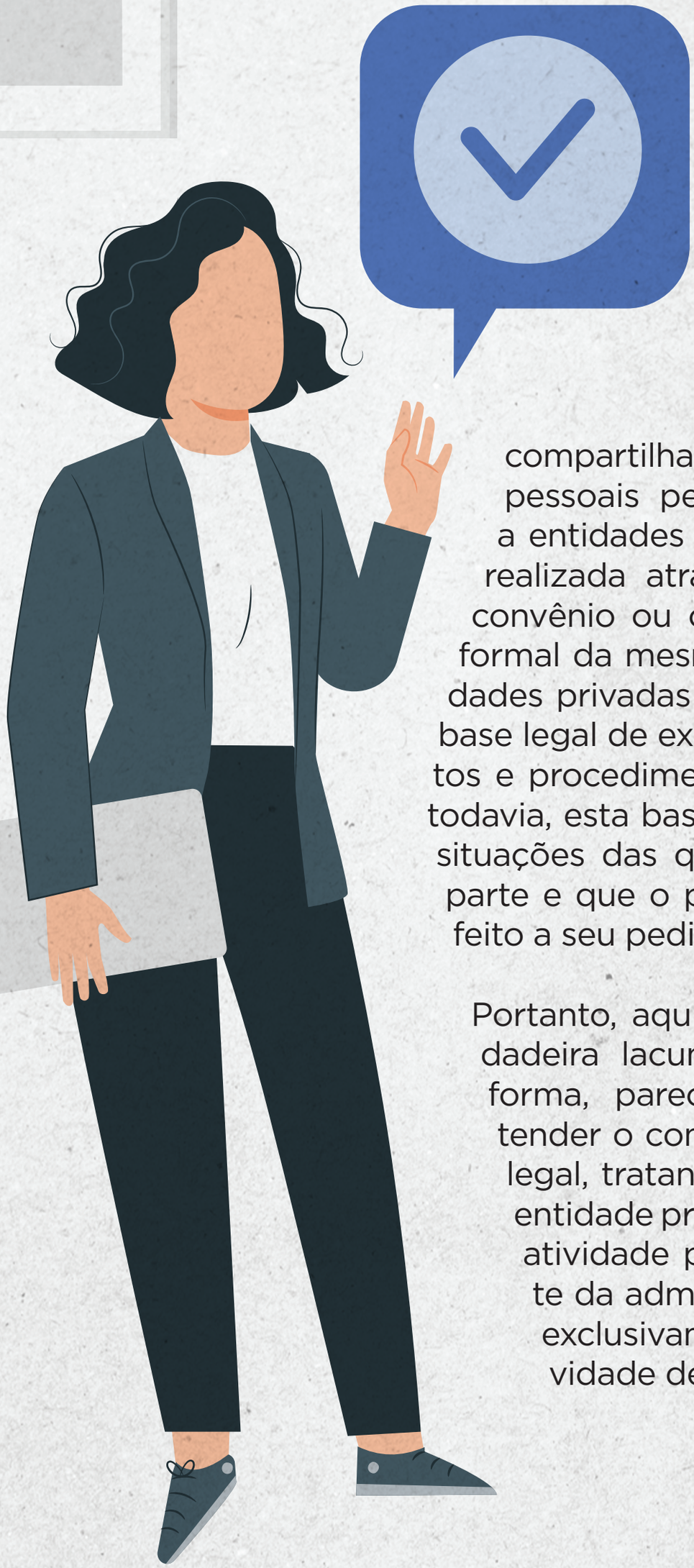
O tratamento de dados pessoais pelo Poder Público é um tema que mereceria uma cartilha própria, então não nos aprofundaremos nele aqui.

A presente base legal, a princípio, é aplicável à Administração Pública, no entanto, ela existe, para viabilizar a execução de políticas públicas..

E se uma política pública for executada por uma entidade privada, a base legal poderá ser aplicável?

A própria LGPD prevê a hipótese de transferência de dados pessoais pelo Poder Público a entidades privadas em casos de execução descentralizada da atividade pública que exija a transferência, exclusivamente para este fim específico e determinado; nos casos em que os dados forem publicamente acessíveis; quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; e na hipótese da transferência de 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.

Compreender-se-ia, considerando que qualquer transferência ou



compartilhamento de dados pessoais pelo Poder Público a entidades privadas deve ser realizada através de contrato, convênio ou outro instrumento formal da mesma natureza, entidades privadas deverão utilizar a base legal de execução de contratos e procedimentos preliminares, todavia, esta base legal se refere a situações das quais o titular seja parte e que o procedimento seja feito a seu pedido.

Portanto, aqui, temos uma verdadeira lacuna jurídica. Desta forma, parece adequado estender o conteúdo desta base legal, tratando por analogia a entidade privada que exerce a atividade pública como parte da administração pública, exclusivamente naquela atividade de tratamento.

Em resumo: as políticas públicas devem estar formalizadas através de leis, regulamentos, contratos, convênios ou instrumentos congêneres. Esta base legal não concede carta branca à Administração Pública para tratar os dados que desejar e como desejar, devendo tudo ser feito respeitando o princípio da legalidade, isto é, o princípio que limita a atuação do Poder Público ao que é expressamente permitido por lei.

REALIZAÇÃO DE ESTUDOS POR ÓRGÃOS DE PESQUISA

A quarta base legal de tratamento é a Realização de Estudos por Órgãos de Pesquisa.

Esta base legal é passível de ser utilizada tanto para o tratamento de dados pessoais comuns como para o de dados pessoais sensíveis.

A definição de órgãos de pesquisa já foi explorada anteriormente nesta cartilha, portanto, é importante mantê-la em mente. Não existem ressalvas ou controvérsias acerca

dos agentes a quem esta base legal se aplica, no entanto os dados tratados devem sempre limitar-se a finalidade de pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Em todos os casos, sempre que possível, os dados pessoais devem ser anonimizados, com a ressalva de que a anonimização deverá se pautar na aplicação de meios técnicos razoáveis e disponíveis no momento do tratamento, através do qual os dados pessoais perdem a possibilidade de associação direta ou indireta com o seu titular.

O texto não se aprofunda no significado da expressão "garantida, sempre que possível, a anonimização dos dados pessoais", portanto, podemos interpretar esta disposição como "sempre que se puder alcançar os resultados pretendidos com a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico sem os dados pessoais que podem ser associados direta

ou indiretamente com o seu titular, estes deverão ser obrigatoriamente anonimizados pelo órgão de pesquisa".

Na hipótese de alguns dados serem absolutamente necessários, e outros não, para se alcançar os resultados pretendidos com a pesquisa, será necessária a anonimização de todos aqueles que não forem indispensáveis.

EXECUÇÃO DE CONTRATOS OU PROCEDIMENTOS PRELIMINARES

A quinta base legal de tratamento é a Execução de Contratos ou Procedimentos Preliminares.

Esta base legal é passível de ser utilizada somente para o tratamento de dados pessoais comuns.

O nome completo desta base legal é execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

A presente base legal pressupõe a existência de um contrato existente, devidamente firmado pelas partes.

No que se refere aos procedimentos preliminares, podemos incluir, mas, definitivamente, não se limitar, à elaboração de propostas comerciais, minutas contratuais, acordos de confidencialidade, dentre outros documentos jurídicos pré-contratuais, desde que o titular seja parte.

Um possível questionamento neste ponto seria, esta base legal se aplica a um titular que assina um contrato como testemunha? Afinal, a testemunha não é parte. Faz sentido que sim, já que a outra opção seria a utilização da base legal do consentimento, que pode ser revogado. Em tal cenário, remoção posterior a assinatura da testemunha, que integrava o documento jurídico como um elemento essencial, lhe conferindo a natureza de título executivo extrajudicial (documento que pode ser cobrado judicialmente sem passar por uma análise aprofundada pelo Juiz), causaria grande insegurança jurídica em todas as contratações.

Por fim, quando se encerra o contrato, ou quando os procedimentos preliminares não culminam na celebração do contrato, deve-se encontrar outra base legal adequada para continuar o tratamento, ou encerrá-lo imediatamente.

EXERCÍCIO REGULAR DE DIREITOS EM PROCESSOS JUDICIAIS, ADMINISTRATIVOS OU ARBITRAIS

A sexta base legal de tratamento é o Exercício Regular de Direitos em Processos Judiciais, Administrativos ou Arbitrais.

Esta base legal é passível de ser utilizada tanto para o tratamento de dados pessoais comuns como para o tratamento de dados pessoais sensíveis.

Trata-se de uma base legal que permite o tratamento de dados pessoais quando necessário para garantir o acesso à justiça e o exercício dos direitos legais das partes envolvidas em um processo legal, desde que sejam observados os princípios e requisitos estabelecidos pela LGPD.

É importante ressaltar que o tratamento de dados pessoais utilizando a presente base legal deve ser realizado de forma restrita e proporcional ao objetivo pretendido. Os dados devem ser utilizados estritamente para o exercício dos direitos legais no processo em questão e não podem ser divulgados ou compartilhados de forma inadequada ou desproporcional.

Importante ressaltar que esta base legal geralmente será aplicável a advogados, sociedades de advogados, defensorias públicas, ou outros tipos de procuradores (na hipótese de processos arbitrais).

Na hipótese de um advogado ou sociedade de advogados representar os interesses do seu cliente, sempre existirá um contrato, ainda que verbal. Então como definir qual é a base legal adequada entre esta e a execução de contratos e procedimentos preliminares?

Esta não é uma questão bem definida, no entanto, entende-se que existe uma divisão entre dados pessoais que serão tratados especificamente para a atuação em processos e os que são utilizados para celebração e execução do contrato, análise esta que deverá ser realizada em cada situação específica, pois, encerrado o processo e encerrado o prazo para a propositura de ação rescisória, no caso de processo judicial, ou outras ações judiciais que visem anular processos administrativos ou arbitrais, deverá ocorrer o término do tratamento dos dados pessoais, mantendo-se, se e quando pertinente, aqueles tratados em virtude da execução do contrato.

PROTEÇÃO DA VIDA OU INCOLUMIDADE FÍSICA DO TITULAR OU DE TERCEIRO

A sétima base legal de tratamento é a Proteção da Vida ou Incolumidade Física do Titular ou de Terceiro.

Esta base legal é passível de ser utilizada tanto para o tratamento de dados pessoais comuns como para o tratamento de dados pessoas sensíveis.

A base legal de proteção da vida ou incolumidade física do titular ou de terceiro é autoexplicativa.

Havendo perigo real ou potencial à vida ou à incolumidade física do titular ou de tercei-

ros, a empresa poderá utilizar-se desta base legal. Todavia, há de se considerar que a empresa deverá ter o mínimo de interesse na proteção à vida ou incolumidade física destes sujeitos. Não é razoável que uma empresa colete, indiscriminadamente, dados de qualquer pessoa sob tal pretensão.

Espera-se que haja algum tipo de relação jurídica entre a empresa e o titular ou terceiro, ou, inexistindo tal relação com o terceiro, que este tenha algum tipo de relação com o titular que possui relação jurídica com a empresa. Há de se considerar se a empresa possui algum dever legal, regulatório ou contratual de agir ante o perigo real ou potencial identificado.

Um exemplo em que esta base legal de tratamento possa ser utilizada rotineiramente seria o cenário em que uma empresa de monitoramento e segurança patrimonial possui dever de agir na hipótese de invasão da residência do titular, e deverá armazenar as imagens das câmeras de monitoramento. Uma nuance a ser aqui considerada é se o objetivo principal é a proteção da vida do titular e sua família ou do seu patrimônio. Se for o segundo caso, a base legal de execução de contrato será mais apropriada.

Outro exemplo seria o da empresa, ou condomínio comercial/corporativo que identifica seus visitantes e controla seus horários de entrada e saída, e conjunto, setor, sala ou indivíduos a quem estão visitando. Pode-se argumentar que o objetivo aqui é proteger a vida e a incolumidade física de terceiros.

Em cenários não habituais, por exemplo, em que chegar ao conhecimento de uma empresa o fato de que o titular ou terceiro estão correndo perigo de perder a vida ou de ter sua integridade física prejudicada, a empresa poderá utilizar-se desta base legal para tomar as medidas cabíveis, como acionar as autoridades competentes ou serviços de saúde.

De qualquer forma, pode-se afirmar que esta é uma base legal de tratamento que não é tão comumente utilizada, pois raras são as atividades de tratamento que possuem como finalidade fornecer este tipo de proteção e, muitas das vezes, outras bases legais serão mais adequadas ao caso em questão, apesar da proteção à vida e incolumidade física do titular ou de terceiros serem uma preocupação da empresa.

TUTELA DA SAÚDE

(POR PROFISSIONAIS OU SERVIÇOS DE SAÚDE OU AUTORIDADES SANITÁRIAS)

A oitava base legal de tratamento é a Tutela da Saúde (por Profissionais ou Serviços de Saúde ou Autoridades Sanitárias).

Esta base legal é passível de ser utilizada tanto para o tratamento de dados pessoais comuns como para o de dados pessoais sensíveis.

A base legal de tutela da saúde por profissionais de saúde, serviços de saúde ou autoridades sanitárias, também é relativamente autoexplicativa.

Dentre profissionais de saúde, podemos destacar médicos, dentistas, psicólogos, nutricionistas, fisioterapeutas, enfermeiros, farmacêuticos, biomédicos e profissionais de educação física. Médicos veterinários, apesar de considerados profissionais de saúde, não exercem atividades de tutela da saúde de seres humanos, sujeitos de direito protegidos pela LGPD, portanto, podem ser excluídos da lista.

Dentre serviços de saúde, podemos destacar hospitais,

clínicas, consultórios, laboratórios, farmácias e bancos de sangue e de leite humano. Mas esta é uma lista apenas exemplificativa. Já dentre as autoridades sanitárias, podemos destacar a Agência Nacional de Vigilância Sanitária ("ANVISA") e os órgãos de vigilância sanitária estaduais e municipais.

A utilização desta base legal é limitada a estes agentes, e outros semelhantes que se enquadrem nos conceitos presentes no texto da base legal. O outro requisito é que estes agentes utilizem esta base legal quando de fato estiverem no exercício de atividades de tutela da saúde. O tratamento de dados pessoais por estes agentes não deve ser irrestritamente atribuído a esta base legal, devendo a cada caso, a cada tipo de dado, serem atribuídas as bases legais apropriadas.

Encerrando-se as atividades de tutela da saúde em relação a determinado titular, o profissional ou serviço de saúde, ou a autoridade sanitária, deverão encerrar o tratamento, ou atribuir outra base legal também aplicável para que possa continuar a tratá-los, se necessário.

Aqui é importante considerar as normativas dos conselhos de classe e das próprias autoridades sanitárias, pois, durante e após o encerramento da tutela da saúde, podem subsistir obrigações regulatórias aplicáveis acerca das atividades realizadas.

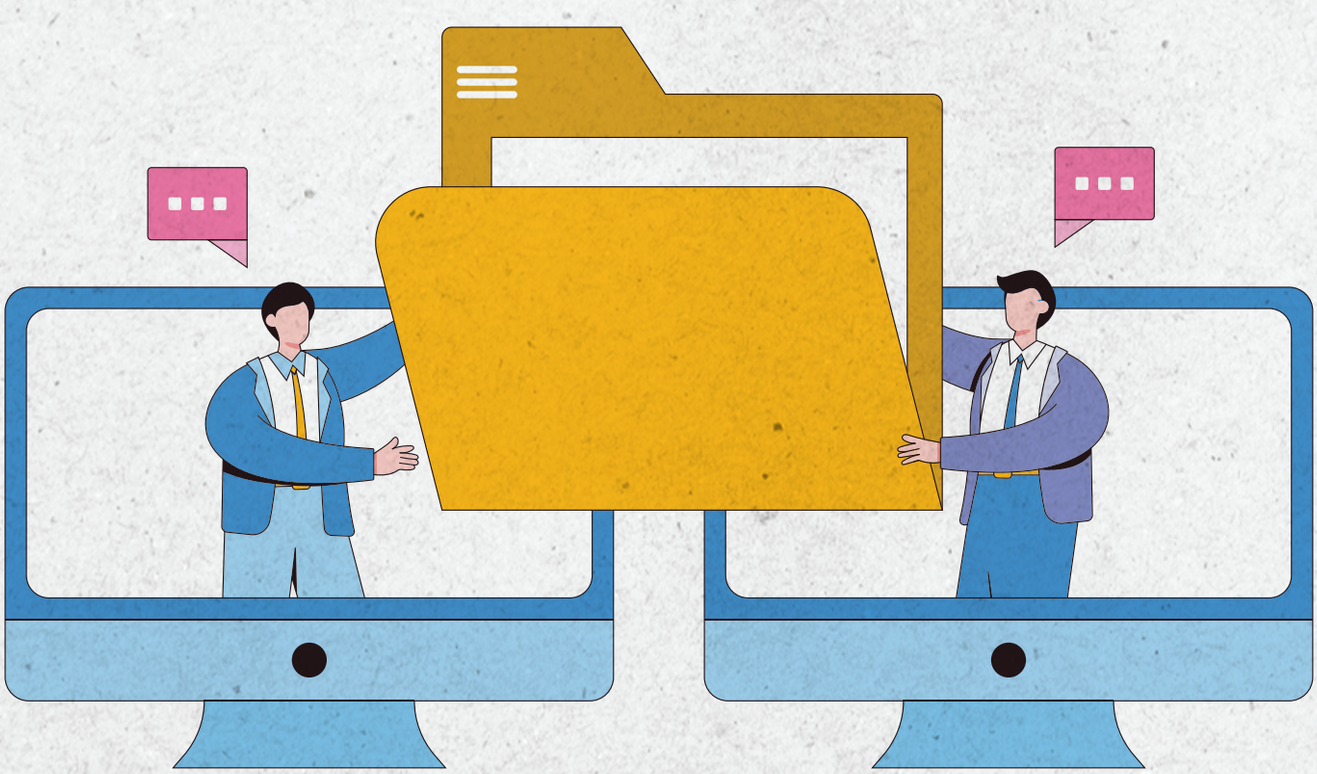
INTERESSE LEGÍTIMO

(DO CONTROLADOR OU DE TERCEIRO)

A nona base legal de tratamento é o Interesse Legítimo (do Controlador ou de Terceiro).

Esta base legal é passível de ser utilizada somente para o tratamento de dados pessoais comuns.

A base legal do interesse legítimo do controlador ou de terceiros também é uma das bases legais mais complexas. Ela é a base legal adequada para apoiar a promover as atividades do controlador, e para protegê-lo, em relação ao titular, do exercício regular de seus direitos ou da prestação de serviços que o beneficiem.



Em todos os casos, o interesse legítimo do controlador não se sustenta quando prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais. Também em todos os casos, quando houver tratamento de dados pessoais com fundamento nesta base legal, apenas os dados estritamente necessários para preservar o interesse legítimo deverão ser tratados

com base nela, devendo os demais dados serem eliminados ou terem outras bases legais adequadas atribuídas.

É importante ressaltar que a base legal do legítimo interesse não pode ser utilizada de forma indiscriminada ou abusiva. Os controladores de dados devem realizar uma análise cuidadosa para justificar o uso dessa base legal, levando em consideração os princípios da necessidade e adequação.

Além disso, é fundamental realizar uma avaliação de impacto sobre a proteção de dados (RIPD) quando o tratamento de dados com base no legítimo interesse apresentar riscos elevados aos direitos e liberdades dos titulares dos dados, preservados os segredos comerciais e industriais.

Caso o titular dos dados tenha objeção ao tratamento com base no legítimo interesse, é necessário que o controlador demonstre a prevalência dos interesses legítimos em relação aos direitos e liberdades individuais, ou então interrompa o tratamento dos dados.

A título de acréscimo, temos que de acordo com a GPDR (General Data Protection Regulation), regulamento da União Europeia, as empresas antes de optarem por utilizarem a base legal do Legítimo Interesse devem realizar

o LIA “Legitimate Interest Assessmen”t (“LIA”), ou Teste de Legítimo Interesse, levando em consideração: se existe de fato um interesse legítimo para a realização do tratamento; se o tratamento é de fato necessário para alcançar as finalidades almejadas; se existem impactos em interesses, direitos e liberdades dos indivíduos afetados, e se estes direitos prevalecem sobre os interesses da empresa, para enfim, chegar-se a uma conclusão.

Do ponto de vista do titular, em geral, é pouco útil conhecer o LIA, mas em um processo judicial que possui como objeto de análise o tratamento de dados pessoais realizado com fundamento na base legal do legítimo interesse, a possibilidade de se requerer a aplicação da GDPR, por analogia para exigir a demonstração de algum tipo de teste ou documentação da ponderação entre os interesses legítimos da empresa e os direitos e liberdades fundamentais do titular por parte da empresa, pode ser bem útil para se comprovar a ocorrência de um tratamento de dados pessoais ilícito..

PROTEÇÃO DO CRÉDITO

A décima base legal de tratamento é a Proteção do Crédito.

Esta base legal é passível de ser utilizada somente para o tratamento de dados pessoais comuns.

A base legal de proteção ao crédito não é por si só muito complexa. No entanto, há de se questionar a quem ela se destina. Qualquer empresa poderia tratar dados de titulares que possuem dívidas para com ela? Ou seria esta base legal restrita aos bureaux de crédito?

A lei não traz esta resposta. Em grande parte, esta base legal de tratamento de dados pessoais será de fato utilizada pelos bureaux de crédito, visto que na maior parte de suas atividades, não haveria outra base legal mais adequada. No que se refere a outros tipos de instituições, há de se questionar, o interesse primário da empresa reside em resguardar os seus próprios direitos ou em proteger o ecossistema de crédito nacional ou local?

Certamente, na maioria dos casos, o interesse primário das empresas residirá em resguardar seus próprios direitos, ainda que exista uma preocupação legítima em proteger o ecossistema de crédito. Portanto, nestes casos, deverão ser atribuídas outras bases legais mais adequadas, como por exemplo, o próprio legítimo interesse do controlador.

GARANTIA DA PREVENÇÃO À FRAUDE E À SEGURANÇA DO TITULAR

(NOS PROCESSOS DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE CADASTRO EM SISTEMAS ELETRÔNICOS)

Esta base legal é passível de ser utilizada somente para tratamento de dados pessoais sensíveis.

Melhor explicitando...

Os avanços da tecnologia têm nos permitido utilizar dados biométricos como: mecanismos de autenticação em diversos dispositivos eletrônicos, sistemas e aplicações. Dentre os tipos de dados biométricos mais utilizados para tais finalidades estão as impressões digitais, o reconhecimento facial e o reconhecimento de retina.

Instituições bancárias permitem o acesso às contas em caixas eletrônicos mediante utilização da impressão digital, sem necessidade uso de cartões, e bancos digitais que utilizam algoritmos que comparam fotografias com documentos de identidade enviados digitalmente para a abertura de contas.

O tratamento de dados biométricos para a prevenção à fraude e a garantia da segurança do titular, geralmente ocorrerá em cenários de transações financeiras ou outros tipos de aquisições. O texto da lei não limita a que tipo de segurança este tipo de tratamento se refere. Segurança física, jurídica, patrimonial? Não parece importar.
Se em algum momento, algum dado biométrico puder ser utilizado como mecanismo de autenticação para prevenir fraudes e garantir a segurança do titular, esta base legal poderá ser utilizada.

No entanto, cabe também ao titular concordar ou não, de alguma forma, com tal tratamento, ninguém é obrigado a fazer ou deixar fazer nada, senão em virtude de lei. Então ninguém poderá obrigar um titular de dados pessoais a registrar suas impressões digitais, suas características faciais ou os padrões de sua retina.

Alguns serviços, no entanto, podem impor este tipo de autenticação como requisito para o seu oferecimento. Nestes casos, caberá o titular optar por aderir ou não ao serviço, ou contestar judicialmente ou através dos órgãos de defesa do consumir a legitimidade de tal exigência.

AGORA VAMOS CONVERSAR SOBRE OS SEUS DIREITOS?
OS DIREITOS DOS TITULARES!

DIREITOS DO TITULAR

ART. 17 E SEGUINTES DA LGPD

1) CONFIRMAÇÃO DA EXISTÊNCIA DE TRATAMENTO

O tratamento é toda operação realizada com dados pessoais, como por exemplo a coleta, classificação, armazenamento, distribuição e eliminação. Em resumo, significa tudo que é feito com os dados pessoais, tanto por meio de arquivos físicos quanto digitais. O tratamento, por vezes, depende de consentimento do titular, objetivando a preservação da sua liberdade, intimidade e privacidade. Todo titular de dados tem direito de saber não só quais os dados que determinado controlador tem sobre ele, mas também qual o tratamento correspondente, ou seja, para qual finalidade estão sendo usadas tais informações, em atendimento ao princípio da transparência.

2) ACESSO AOS DADOS

Garante a consulta facilitada e gratuita sobre todos os dados disponíveis, além de como são tratados, incluindo forma e até duração do tratamento. É o direito de saber quais dados do titular são processados, como são processados e por qual motivo são processados, de maneira clara e precisa.

3) CORREÇÃO DE DADOS

Se os dados estiverem incorretos, incompletos ou desatualizados, o titular de dados tem o direito de corrigi-los ou completa-los. Importante mencionar que dados inexatos podem ocasionar consequências ao titular (como viabilizar fraudes), que se tornam ainda mais abrangentes quando há o repasse, da forma como estão, a outros agentes de tratamento.

4) ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO

O titular pode exigir que o processamento de seus dados pessoais seja limitado, especialmente se houver discussão sobre a precisão ou propósito do processamento. Pode exigir a anonimização (resultado de um procedimento para que o dado pessoal perca, irreversivelmente, a possibilidade de identificar uma pessoa natural), bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei. A lei garante ao titular, inclusive, oposição ao processamento de seus dados, em determinadas circunstâncias, como para fins de marketing direto, ou até que tais dados pessoais sejam apagados.

5) PORTABILIDADE

É o direito de solicitar que seus dados pessoais sejam transferidos a outro fornecedor de serviço ou produto, observados os requisitos de segurança e privacidade. O direito à portabilidade representa ao titular o poder de controlar, gerenciar e reutilizar seus dados pessoais, de forma segura e gratuita.

Surge, como consequência, o direito a um sistema de interoperabilidade entre os controladores, já que os dados deverão ser recebidos conforme enviados, sendo indispensável, para isso, a existência de meios tendentes à concretização de acesso na integralidade, por meio de compatibilidade. Os padrões de interoperabilidade devem observar o previsto pela ANPD.

6) ELIMINAÇÃO DOS DADOS TRATADOS COM CONSENTIMENTO

É o direito que o titular tem de revogar o consentimento anteriormente dado. Se o titular dos dados consentiu com o tratamento, mas não quer mais que o controlador trate seus dados pessoais, pode solicitar a eliminação desses dados.

Contudo, esse direito não poderá ser exercido quando surgir a necessidade de conservação desses dados, para cumprir obrigação legal ou regulatória.

7) INFORMAÇÃO SOBRE COMPARTILHAMENTO

A LGPD preza pelo princípio da transparência. Assim, o titular tem o direito de receber informações sobre com quem o controlador está compartilhando seus dados.

Caso exista o compartilhamento de dados com terceiros, o controlador deve, expressamente, informar com quem compartilha os dados do titular, não bastado a menção genérica.

8) INFORMAÇÃO SOBRE NÃO FORNECIMENTO DE CONSENTIMENTO E CONSEQUÊNCIAS

O consentimento do titular de dados para determinado tratamento deve ser solicitado e concedido de forma livre, clara, transparente e específica. Assim, o titular de dados tem o direito de ser informado sobre a possibilidade de não fornecer o consentimento e quais as consequências disso, caso o consentimento seja negado.

Por exemplo, quando um usuário precisa consentir ou não com o uso de cookies em um site. Se o não consentimento impedir o acesso a algumas funcionalidades do site, o usuário deve ser expressamente informado.

9) REVOGAÇÃO DO CONSENTIMENTO

É direito do titular a revogação do consentimento dado para o tratamento de dados pessoais.

O titular poderá manifestar seu interesse junto ao controlador de que não mais deseja consentir com o tratamento de dados.

Cumpre ressaltar que a revogação não significa eliminação do tratamento, mas somente o fim do consentimento anteriormente dado, já que a eliminação é um outro direito que o titular possui.

10) OUTROS

O direito do titular de dados de se manifestar contra o controlador na ANPD e nos órgãos de defesa do consumidor; O direito de opor-se ao tratamento realizado com dispensa de consentimento, caso não esteja em conformidade com a lei.

DECISÕES AUTOMATIZADAS

ART. 20 DA LGPD

A LGPD estabelece que o titular dos dados tem o direito de solicitar a revisão de decisões automatizadas que afetem seus interesses, especialmente aquelas que resultem em efeitos jurídicos significativos ou afetem de maneira relevante o titular dos dados.

As decisões automatizadas referem-se a processos que utilizam exclusivamente algoritmos e lógica computacional para analisar dados pessoais e tomar uma decisão, sem a participação direta de uma pessoa na tomada de decisão.

Ao solicitar a revisão, o titular dos dados tem o direito de receber informações claras e compreensíveis sobre a lógica utilizada na decisão automatizada, bem como sobre a importância e as consequências previstas dessa decisão para o titular.

CONCLUSÃO

A presente cartilha objetiva trazer uma visão geral de todo o contexto da Lei Geral de Proteção de Dados, seus princípios e bases legais, mas sobretudo, despertar no titular os poderes que lhe são conferidos através da consagração de sua autodeterminação informativa.

A autodeterminação informativa é o direito que os indivíduos têm de controlar e decidir sobre a coleta, o uso e a divulgação de suas informações pessoais.

Trata-se do poder que os titulares possuem para determinar como suas informações são tratadas pelas organizações, afinal de contas, os dados pessoais pertencem aos titulares de dados.

Ao reconhecer a importância da autodeterminação informativa, a LGPD estabelece uma série de direitos para os titulares.

Dentre eles:

- Confirmação e Existência de Tratamento

- Acesso aos Dados e Correção de Dados
- Anonimização, Bloqueio ou Eliminação
- Portabilidade
- Eliminação dos Dados Tratados com consentimento
- Informação sobre o Compartilhamento
- Informação sobre não fornecimento de consentimento e consequências
- Revogação do consentimento

E ainda, o direito de solicitar a revisão de decisões automatizadas que afetem seus interesses, especialmente aqueles que resultem em efeitos jurídicos significativos.

O objetivo da LGPD é colocar o titular no centro do controle de seus próprios dados pessoais, preservando a sua privacidade e o respeito às suas liberdades e garantias fundamentais.

BIBLIOGRAFIA

BRAMANTE, Ivani Contini. DE MARTINO, Ana Cecília Sampaio. ALVES, Leonardo Gutierrez. Proteção de Dados Pessoais Na Relação de Trabalho: Personal Data Compliance (LGPD - Lei 13.079/2018). Curitiba: Juruá, 2021.

CARLOTO, Selma.BRAMANTE, Ivani Contini. CAVALINI,Juliane Pascoeto. Lei Geral de Proteção de Dados e Segurança da Informação – Perguntas e Respostas – Vol. I. São Paulo: LTr, 2022

OAB SÃO PAULO | Subseção Santos

Design: Agência Celeiro.BMD®

OAB SANTOS | Tempo de se conectar | GESTÃO 2022 • 2024 | 90 OAB SANTOS