PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

Ana Carolina Cavalcanti Franco de Godoy

A LEI GERAL DE PROTEÇÃO DE DADOS E OS REFLEXOS NAS RELAÇÕES DE TRABALHO

SÃO PAULO

2021

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

Ana Carolina Cavalcanti Franco de Godoy

A LEI GERAL DE PROTEÇÃO DE DADOS E OS REFLEXOS NAS RELAÇÕES DE TRABALHO

Monografia apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de ESPECIALISTA em Direito do Trabalho, sob a orientação da Prof., Dra. Cristina Paranhos Olmos.

SÃO PAULO

2021

Banca Examinadora

Professor (a) Doutor (a)

Instituição: _____

Julgamento: _____

Assinatura: _____

Professor (a) Doutor (a)_____

Instituição: _____

Julgamento: _____

Assinatura: _____

Professor (a) Doutor (a)_____

Instituição: _____

Julgamento: _____

Assinatura: _____

AGRADECIMENTOS

Agradeço aos meus pais - Orlando Godoy e Ana Maria Cavalcanti - e aos meus irmãos - Pedro Henrique e Orlando Neto - por todo amor, dedicação, apoio e incentivo que serviram de alicerce para as minhas realizações.

Agradeço o apoio e incentivo dos sócios - Carla Teresa Martins Romar, Carla Lobo Olim Marote e Tulio de Oliveira Massoni - que me apresentaram o Direito do Trabalho e servem de inspiração para a minha atuação profissional.

Agradeço aos colegas do escritório Romar, Massoni e Lobo Advogados pelo apoio e troca diária de conhecimento, em especial ao Dr. Túlio de Oliveira Massoni, Dra. Milena Guarda e ao Dr. Wallace Dias Silva, pelo compartilhamento de livros, artigos e ideias, que foram primordiais para a elaboração deste trabalho.

Agradeço à professora Dra. Cris Olmos e ao professor Dr. Werner Keller, por toda dedicação durante o curso que propiciaram um ensino de alta qualidade.

Agradeço, ainda, a todos familiares e amigos que, direta ou indiretamente, contribuíram para a realização deste trabalho.

RESUMO

O direito fundamental de proteção de dados entrou em vigor recentemente no Brasil, através da Lei nº 13.709/2018. O objetivo do presente trabalho é o estudo da chamada Lei Geral de Proteção de Dados, bem como os seus impactos nas relações de trabalho. No presente trabalho é explorado como esta referida Lei protege a informação pessoal do indivíduo trabalhador e os reflexos que esta lei traz nos dados pessoais do empregado em posse de seu empregador, além de analisarmos sua base legal, como a apresentação dos seus princípios, conceitos e principais hipóteses de tratamento no contexto laboral a fim de garantir a efetividade da norma nas relações de trabalho. Analisaremos, por fim, a possibilidade de negociação coletiva para o tratamento dos dados pessoais, as sanções administrativas para os empregadores, quando em posse dos dados de seus empregados, bem como a responsabilidade civil, sob o prisma da Lei Geral de Proteção de Dados.

Palavras-chave: Lei geral de proteção de dados; proteção de dados pessoais; consentimento; privacidade; direito fundamental.

ABSTRACT

The fundamental data protection right recently came into force in Brazil, through Law No. 13,709 / 2018. The purpose of this paper is to study the so-called General Data Protection Law, as well as its impacts on labor relations. This work explores how this Law protects the personal information of the individual worker and the effects that this law brings on the personal data of the employee in possession of his employer, besides analyzing its legal basis, such as the presentation of its principles, concepts and main hypotheses of treatment in the labor context in order to guarantee the effectiveness of the norm in labor relations. Finally, we will analyze the possibility of collective bargaining for the treatment of personal data, administrative sanctions for employers when in possession of their employees data, as well as civil liability, under the prism of the General Data Protection Law.

Keywords: General data protection law; protection of personal data; consent; privacy; fundamental right.

LISTA DE ABREVIATURAS

ART	Artigo
ANPD	Autoridade Nacional de Proteção de Dados
CC	Código Civil
CDC	Código de Defesa do Consumido
CF	Constituição Federal de 1988
CLT	Consolidação das Leis do Trabalho
CPC	Código de Processo Civil
CTPS	Carteira de Trabalho e Previdência Social
FGTS	Fundo de Garantia do Tempo de Serviço
LGPD	Lei Geral de Proteção de Dados

SUMÁRIO

INTRODUÇÃO

Estamos vivenciando a era mais importante da revolução tecnológica, onde cria-se constantemente mecanismos capazes de processar e transmitir informações em quantidades e velocidades jamais experimentadas.

Essa nova era ora denominada como a “Quarta Revolução Industrial”, foi apresentada pelo presidente do Fórum Econômico Mundial de Davos, Klaus Schwab, como uma revolução tecnológica que veio para alterar “fundamentalmente o modo como vivemos, trabalhamos e nos relacionamos[1]”.

A partir de então, vivenciamos uma nova forma de organização, onde a tecnologia é fundamental para o desenvolvimento da economia, especialmente com o avanço da “*big data*”, tornou-se possível a organização e análise de informações de modo escalável.

Com a intensificação dessa tecnologia, que possibilita estruturar e analisar um volume antes inimaginável de dados para os mais variados tipos de finalidades, surgiu um novo mercado onde os dados pessoais passaram a ser processados e valorados economicamente, sendo considerados, inclusive, como o principal insumo da sociedade contemporânea.

Isso porque, a coleta de dados torna possível não só a identificação e interpretação de certas informações, mas também a recombinação de informações que, por meio de algoritmos derivados da “*big data*” e demais tecnologias, permite identificar diversos padrões de comportamentos individuais e inferir, inclusive, a sua recorrência no futuro.

Essas previsões ganharam relevância em ações publicitárias, onde o consumidor passou a ser monitorado e as empresas passaram a prever e manipular o seu comportamento. Ao consentir com os termos de privacidade, essas empresas

[1] SCHWAB, Klaus. A Quarta Revolução Industrial, Edipro, 1ª edição, 2016, São Paulo, pág.19.

passam a mapear as suas preferências, hábitos de consumos e, com isso, dirigir publicidades de forma mais eficiente, produtiva e estratégica.

Um dos exemplos clássicos sobre a utilização da “*big data*”, é a ação que a americana Target promoveu ao mapear o “perfil” de cada consumidor, com base em dados demográficos e comportamentais, com intuito de oferecer, antecipadamente, os produtos que aquele consumidor estava mais propenso a comprar. O modelo permitiu à Target identificar quais das clientes estavam grávidas e, com isso, direcionar vendas de produtos de bebês, tendo um aumento de 30% nas vendas desse segmento.

Desse modo, os dados pessoais dos consumidores passaram a ser utilizados para a promoção de bens de consumo, sendo possível afirmar que, no cenário atual, a economia é comandada por dados e, justamente em razão dessa nova comodificação, onde o uso frenético de dados passou a ser matéria prima para diversas formas de controle social que, invariavelmente levanta a questão da liberdade e privacidade dos indivíduos, é que a regulação do uso de dados ganhou muito mais notoriedade e passou a ser assunto central em vários países.

No âmbito das relações do trabalho, o tema também se mostra relevante, pois a utilização de novas tecnologia está cada vez mais presente, abrangendo diversas questões, principalmente a preocupação com a proteção da privacidade e intimidade do trabalhador, na medida em que a subordinação jurídica existente no contexto laboral pode dar origem a abusos e interferências na vida particular dos trabalhadores.

Isso porque o uso de geolocalizadores, câmeras de segurança, audiovigilância, dados biométricos, reconhecimento facial, permitem ao empregador o monitoramento, não só no mundo do trabalho, como também a vida íntima dos trabalhadores.

No mesmo sentido, o uso da inteligência artificial vem sido comumente utilizada pelas empresas para aferir a produtividade dos trabalhadores, para sua promoção ou desligamento, como também sendo utilizada no recrutamento de

trabalhadores em processos seletivos, cabendo relembrar o famoso caso da "amazon"[2], onde a empresa utilizou-se da inteligência artificial para selecionar novos talentos e, no fim, a decisão automatizada acabou realizando a discriminação de gênero contra as mulheres.

A era da *"big data"* trouxe, portanto, inúmeros desafios nas relações do trabalho, pois, diante da possibilidade de uso indevido e abusivo de dados obtidos através das tecnologias citadas acima, que podem originar, inclusive, discriminações, é que a proteção dos dados pessoais se tornou um direito fundamental global.

A União Europeia foi uma das pioneiras na regulamentação do uso de dados, com a implementação, em 25 de maio de 2018, da "*General Data Protection Regulation*" (GDPR), e é a mais completa regulamentação sobre proteção de dados pessoais em vigor na Europa, sendo aplicada para todas as pessoas da União Europeia e empresas que operem no espaço econômico Europeu.

Tendo o regulamento do direito Europeu como inspiração, em agosto de 2018 o Senado Brasileiro aprovou a Lei n. 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD).

Assim como a GDPR, a LGPD no Brasil veio para garantir a transparência em todas as operações realizadas com os dados do pessoal natural, como a coleta, o processamento, arquivamento, eliminação e compartilhamento dos dados pessoais.

Ela tem como escopo resguardar os dados pessoais dos seus titulares ou pessoas naturais, não é somente em meios digitais, mas também em outros meios físicos.

Como é uma lei geral, possui influência em todas as áreas do direito, inclusive nas relações jurídicas firmadas entre empregador e empregado, na qual há intensa

[2] Ferramentas de recrutamento da Amazon com AI discriminava candidatas mulheres. Disponível em: https://tecnoblog.net/meiobit/391571/ferramenta-de-recrutamento-amazon-ai-discriminava-mulheres/ Disponível em: 08 de janeiro de 2021.

coleta de dados, desde o momento da candidatura ao emprego até o período pós-contratual, sendo o principal enfoque deste trabalho.

Nesse sentido, cabe analisar os princípios, conceitos e fundamentos de aplicabilidade propostos na norma, assim como direitos da parte titular e deveres das empresas para que atuem em conformidade com a lei, respeitando à privacidade e à proteção de dados pessoais dos trabalhadores.

1 PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

Os princípios da LGPD são a base para informar e orientar as empresas a terem boas práticas no tratamento de dados pessoais e possuem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme disposição do artigo 1º da LGPD:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018).

A principiologia da lei geral de proteção de dados está prevista no artigo 6ª, o qual traz os preceptivos dos princípios a serem observados pelas empresas no momento do tratamento de dados, seja de consumidores, seja de trabalhadores:

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

> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL, 2018).

Os princípios visam orientar a aplicação da norma e devem ser ponderados quando do tratamento dos dados pessoais.

No âmbito trabalhista, verifica-se ser cabível a aplicação dos princípios trazidos na norma, pois se trata de uma relação contratual norteada pelos princípios basilares do Direito do Trabalho.

Vejamos cada um deles.

1.1 Da boa-fé

Observa-se que o princípio da boa-fé é trazido, de plano, como introdução no caput do artigo 6º da Lei Geral de Proteção de Dados.

A intenção do legislador, ao elencar o princípio da boa-fé como recomendação introdutória, é incentivar à observância de boas práticas para o tratamento de dados pessoais.

Considerando as dimensões de tratamentos que decorrem da coleta de dados, a boa-fé demonstra-se imprescindível para a efetiva aplicação dos princípios em sua totalidade.

A boa-fé é um princípio consagrado em todas as áreas do direito, tal como verifica-se nos artigos 113 e 422 do Código Civil, cuja premissa é estabelecer uma conduta ética entre as partes em suas relações obrigacionais:

> Art. 113. Os negócios jurídicos devem ser interpretados conforme a boa-fé e os usos do lugar de sua celebração.
> [...]
>
> Art. 422. Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé. (BRASIL, 2015).

O princípio da boa-fé, assim como em todas as relações jurídicas, é fundamental para o equilíbrio na coleta de dados, sendo o alicerce para a aplicação imediata dos demais princípios elencados no artigo 6º, os quais são meros desdobramentos da boa-fé no tratamento de dados pessoais.

Deste modo, a aplicação efetiva dos princípios da Lei Geral de Proteção de dados, torna-se possível, somente, se respeitada a boa-fé, a qual se relaciona com honestidade e lealdade que o titular dos dados deposita no controlador ao fornecer os seus dados.

No direito do trabalho, como ramo do direito que é, as relações contratuais são regidas sob a égide da transparência e da boa-fé, até porque a CLT expressamente autoriza a incidência dos princípios gerais de direito naquilo em que ela é omissa.

Portanto, diante do dever de lealdade processual que rege as relações do trabalho, o empregador deve ter em seu poder somente os dados pessoais dos seus empregados que tenham propósitos legítimos para cumprimento de obrigação legal do contrato de trabalho.

1.2 Princípio da finalidade

O princípio da finalidade é o primeiro dos princípios trazidos no artigo 6º da Lei Geral de Proteção de dados.

O normativo dispõe que a realização do tratamento dos dados pessoais deve observar fins legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Por fins legítimos, entende-se que o normativo se refere a uma finalidade movida pela legalidade e bons costumes.

Fins específicos, para que o tratamento seja realizado com observância ao objetivo que foi determinado no momento da coleta.

Por fins explícitos, o normativo enfatiza que o tratamento deve ser claro e objetivo, visando a transparência do objetivo da coleta ao titular dos dados. Não sendo o tratamento objetivo e claro, a lei dispõe que esse será nulo:

> Art.8º, § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. (BRASIL, 2018).

O normativo ainda define que os dados não poderão ser tratados posteriormente sem observar os propósitos para o qual foram coletados.

Os propósitos legítimos, específicos e explícitos integram o objetivo do princípio finalidade, visando garantir que os dados coletados não serão indevidamente utilizados para fins não especificados.

O princípio da finalidade garante ao titular que os dados coletados não serão destinados para outras finalidades, senão aquelas explícitas e específicas que foram informadas no momento da coleta.

Logo, pode-se afirmar que o princípio da finalidade é um limitador, o qual exige que a coleta de dados deve ser pautada com fins específicos e legítimos, devendo ficar claro ao titular a finalidade que se busca com a coleta dos seus dados pessoais, como por exemplo, a coleta de dados na fase de seleção de empregados. Nessa fase pré-contratual, que envolve uma imensa coleta de dados, sendo que muitas dessas informações podem efetivamente afetar a privacidade do titular, cabe ao empregador coletar somente os dados relevantes para atender a finalidade de contratação vaga.

Nesse sentido, Uría Menéndez assevera que o princípio da finalidade pressupõe que os dados devem ser armazenados somente durante o tempo necessário para assegurar as finalidades de tratamento, devendo ser destruídos ao alcançar a finalidade que se buscou com a coleta:

> Este princípio surge intimamente relacionado com o princípio da finalidade, uma vez que pressupõe que os dados apenas devem ser conservados durante o período estritamente necessário para assegurar as finalidades do tratamento. Assim, os dados pessoais recolhidos de um candidato a emprego que tenha sido excluído do processo de selecção devem ser destruídos, porque a finalidade a que o tratamento se destinava deixa de existir a partir desse momento[3] (URIA MENEZES).

A exigência de antecedentes criminais, somente se mostra legítima se tiver aparada em profissão onde é necessária uma fidúcia. No mesmo sentido, a coleta de informações se a candidato possui alguma deficiência física somente será legítima se a finalidade for para contratar empregados para ocupar as vagas destinados aos PCD.

Assim, cabe ao empregador coletar somente os dados necessários, com propósitos legítimos, específicos e explícitos informados ao titular, seja na fase pré-contratual, seja para manutenção do contrato de trabalho, seja após o término do contrato, sem a possibilidade de tratamento posterior de forma incompatível com a finalidade a que se destinou.

A finalidade que se busca com a coleta do dado pessoal deve ser descrita de forma clara e precisa para o titular. Esse requisito é um instrumento que traz proteção ao titular, pois obriga o controlador de dados a respeitar os direitos fundamentais à privacidade, liberdade e não discriminação.

---

3 MENEDÉZ, Uria. O impacto das novas tecnologias no direito do trabalho e a tutela dos direitos da personalidade do trabalhador. Disponível em: https://www.uria.com/documentos/publicaciones/2242/documento/068apa.pdf?id=1948. Acesso em: 03 de abril de 2021

1.3 Princípio da adequação

Previsto no inciso segundo do artigo 6º da Lei Geral de Proteção de dados, o princípio da adequação possui o seguinte conceito “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”.

Os dados não podem ser utilizados de forma contraditória à finalidade destinada, e sim, utilizados de acordo com a finalidade que foi declarada ao titular, de acordo com o contexto do tratamento e limitadas ao mínimo necessário.

Esse princípio se adequa às relações de trabalho, até mesmo em razão da boa-fé, pois os dados pessoais devem ser adequados de acordo com a finalidade que se busca no seu tratamento.

1.4 Princípio da necessidade

O princípio da necessidade estipula que a coleta de dados deve ocorrer de maneira restritiva, limitando-se ao mínimo necessário para o atendimento da finalidade pretendida.

Esse princípio visa garantir que somente sejam tratados os dados pertinentes e imprescindíveis para o fim pretendido.

Desse modo, dados pessoais excessivos não devem ser coletados se não forem essenciais para a consecução pretendida, evitando-se, assim, exposições pessoais desnecessárias ao titular.

1.5 Princípio do acesso livre

O princípio do livre acesso está disposto no inciso IV do artigo 6º da LGPD e garante ao titular dos dados a garantia de livre acesso gratuito sobre a forma e a duração do tratamento, além da integralidade de seus dados pessoais.

Esse princípio, portanto, assegura ao titular o acesso fácil e gratuito às informações sobre o tratamento integral dos seus dados, principalmente após terem sidos tratados.

O acesso à essas informações, garante ao titular a análise precisa dos seus dados para, se necessário, solicitar a alteração, exclusão ou a interrupção do tratamento de dados pessoais não necessários para a finalidade à qual consentiu.

Igualmente, o artigo 18 da LGPD dispõe que o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. (BRASIL, 2018).

E, no mesmo sentido, o artigo 20 da LGPD dispõe que:

> [...] o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (BRASIL, 2018).

Bem como seu § 1º*:* “cabe ao controlador fornecer informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial”. (BRASIL, 2018).

1.6 Princípio da qualidade de dados

Por esse princípio, é garantido aos titulares dos dados a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Esse princípio visa garantir ao titular de dados a possibilidade de correção de dados incompletos, inexatos ou desatualizados, para que os dados armazenados sejam verdadeiros e estejam atualizados, tal como diretriz prevista também no artigo 18, III, da LGPD.

1.7 Princípio da transparência

O princípio da transparência está previsto no artigo 6º, VI, da LGPD e garante aos titulares, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e agentes de tratamento, resguardados os segredos industriais e comerciais.

Qualquer informação de coleta de dados deve ser transparente e informada ao titular.

Nesse sentido, o artigo 10, § 2º, prevê que

> [...] o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse" e, no artigo 20, § 1º, impõe que o controlador forneça, sempre que solicitado, "informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. (BRASIL, 2018).

1.8 Princípio da segurança

O princípio da segurança está previsto no inciso VII, do artigo 6º, e compreende a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Esse princípio garante que os dados pessoais deverão ser tratados de uma forma segura e confidencial. Para tanto, cabe aos agentes de tratamento utilizar técnicas de segurança para evitar o acesso e manuseio indevido dos dados do tratamento.

Nesse mesmo sentido, o artigo 46, caput, da LGD, dispõe que os agentes de tratamento devem adotar as medidas de segurança para proteger os dados pessoais de acessos não autorizados e, conforme artigo 47, cabe aos agentes de tratamento ou qualquer pessoa que intervenha em uma das fases do tratamento, garantir a segurança dos dados pessoais, mesmo após o término do tratamento. (BRASIL, 2018).

Ainda, visando à segurança, a lei estabelece no artigo 48, que cabe ao controlador comunicar à autoridade nacional e ao titular a ocorrência de incidentes de segurança que possa acarretar risco ou dano relevante aos titulares e determina que a comunicação deve ser feita em prazo razoável visando evitar maiores prejuízos ao titular dos dados.

1.9 Princípio da prevenção

No mesmo sentido da segurança, está o princípio da proteção que visa a adoção de medidas para prevenção dos danos que possam ocorrem em virtude do tratamento de dados pessoais, conforme artigo 6º, VIII, da LGPD. (BRASIL, 2018).

Esse princípio reforça a necessidade de prevenção que as empresas devem adotar para evitar a ocorrência de prejuízos em decorrência do tratamento de dados pessoais.

Com fundamento nesse princípio, a Autoridade Nacional pode solicitar aos agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público, conforme disposição trazida no artigo 32 da LGPD. (BRASIL, 2018).

No artigo 50, *caput*, a lei recomenda que os controladores e operadores formulem regras de boas práticas e governança que estabeleçam condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. (BRASIL, 2018)

Portanto, para que o princípio da prevenção seja efetivado, cabe às empresas a adoção de medidas preventivas para o sucesso da proteção de dados pessoais dos seus empregados.

1.10 Princípio da não discriminação

O tratamento de dados pessoais jamais pode ser utilizado com propósito de promover discriminação contra os seus titulares.

Esse princípio está previsto no artigo 6º, IX da LGPD e expõe que a não discriminação envolve a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Tal princípio encontra respaldo em um dos princípios fundamentais da República Federativa do Brasil (artigo 3º, IV, CF/88), que é promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação. (BRASIL, 2016)

No âmbito das relações no trabalho, os reflexos do princípio da não discriminação estão insculpidos no artigo 7ª da Constituição Federal, que dispõe sobre a proibição de diferenças de salários, de exercício de funções e de critérios de admissão por motivos de sexo, idade, cor ou estado civil ou de diferenças de critérios de admissão e de salário em razão de deficiência física. (BRASIL, 2016)

Deste modo, não pode o empregador realizar o tratamento de dados dos empregados de forma discriminatória com objetivo de dispensar ou perseguir os empregados.

A utilização de dados pessoais para discriminação de empregados é bastante discutida no exterior, tendo diversos casos polêmicos levados à mídia, tal como o caso da “amazon” já citado, cabendo o comentário sobre o caso da empresa sueca conhecida como H&M[4].

Após uma falha em seu banco de dados, a empresa teve vazado diversos dados pessoais de seus empregados, contendo informações desde a vida particular, como problemas familiares, opinião política, crença religiosa e saúde.

Esses dados pessoais eram coletados em conversas informais, o que eles chamavam de “W*elcome Back Talk”,* onde o supervisor “despretensiosamente” obtinha informações sobre os acontecimentos ocorrido durante as férias e afastamentos, inclusive para futuros diagnósticos de doenças.

O banco de dados contendo o perfil dos empregados era utilizado para embasar a adoção de medidas e decisões internas em relação ao empregado, desde decisões para promoções até demissões.

A autoridade de proteção de dados, ao tomar conhecimento do vazamento desses dados, aplicou a multa de 35,63 milhões de euros à empresa H&M, diante da

4 Varejista H&M leva multa milionária por espionar funcionários na Alemanha. Disponível em: https://vocesa.abril.com.br/mercado/varejista-hm-leva-multa-milionaria-por-espionar-funcionarios-na-alemanha/. Acesso em: 20 de fevereiro 2021

comprovação de gravíssima violação aos direitos fundamentos e ao regulamento de dados pessoais. Foi considerada a mais alta multa aplicada na Alemanha e a segunda maior na Europa. O valor recorde de multa foi aplicado ao site Google, que 2019 foi multado no valor de 50 milhões de euros pela agência francesa de proteção de dados pessoais[5].

No Brasil, em nível infraconstitucional, a Lei nº 9.029/1995, proíbe a exigência de atestado de gravidez, esterilização e outras práticas discriminatórias para admissão ou permanência no emprego e, no seu artigo 1º, prevê a proibição da adoção de qualquer prática discriminatória e limitativa para efeito de acesso à relação de emprego, ou sua manutenção, por motivo de sexo, origem, raça, cor, estado civil, situação familiar ou idade, ressalvadas, nesse último caso, as hipóteses de proteção à criança e ao adolescentes previstas no inciso XXXIII do artigo 7º da CF. (BRASIL, 1995).

Portanto, pelo princípio da não discriminação, os dados coletados pelo empregador necessitam atender à finalidade e não podem ser tratados de forma a gerar qualquer tipo de discriminação ou retaliação aos empregados titulares dos dados pessoais.

1.11 Princípio da responsabilidade e prestação de contas

Esse princípio está disposto no inciso X, do artigo 6º da LGPD e expõe que é responsabilidade e prestação de contas do agente a demonstração da “adoção de medidas eficazes e capazes de comprovar a observância e cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas”. (BRASIL, 2018).

Portanto, incube ao controlador e operador a prestação de contas, com o fim de comprovarem o efetivo cumprimento da lei.

---

5 BUTCHER, Isabel. Google: Conselho de Estado francês confirma multa de 50 milhões de euros. Disponível em: https://www.mobiletime.com.br/noticias/19/06/2020/google-conselho-de-estado-frances-confirma-multa-de-50-milhoes-de-euros/. Acesso em: 20 de fevereiro de 2021.

E nesse sentido, visando garantir maior efetividade desse princípio, criou-se a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República, que compete realizar a fiscalização do cumprimento da Lei geral de Proteção de Dados, de acordo as competências estabelecidas no artigo 55-H da LGPD.

> Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019)
> I - zelar pela proteção dos dados pessoais, nos termos da legislação;
> II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;
> III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
> V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
> VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
> VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
> VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;
> IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
> X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;
> XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;
> XII - elaborar relatórios de gestão anuais acerca de suas atividades;
> XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;
> XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;
> XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;
> XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;
> XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação

> contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;
> XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;
> XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);
> XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;
> XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;
> XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;
> XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;
> XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (BRASIL, 2018)

1.12 Conceitos da legislação de proteção de dados brasileira

A Lei Geral de Proteção de Dados elenca no artigo 5°, alguns conceitos básicos de dados:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX - agentes de tratamento: o controlador e o operador;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
> XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
> XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
> XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
> XVIII - órgão de pesquisa: 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;
> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (BRASIL, 2018)

Vejamos detalhadamente cada um deles.

1.11 Dado pessoal

Como visto, o artigo 5º, I, da LGPD traz o conceito geral de dado pessoal, sendo definido como a informação que diz respeito à pessoa natural identificada ou identificável.

São o conjunto de informações que levam à identificação de determinadas pessoas, tal como, nome ou apelido, RG, CPF, título de eleitor, número de passaporte, número de telefone, endereço, endereço eletrônico (e-mail), estado civil, profissão.

O Grupo de Trabalho de proteção de dados da União Europeia, define que dados pessoais como:

> [...] qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social[...].[6]

Catarina Sarmento e Castro, jurista portuguesa, em sua obra de Direito da Informática, privacidade e dados pessoais, definiu dado pessoal como

> Qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável e define como titular dos dados a pessoa que possa ser identificável direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural e local[7].

Portanto, um dado é considerado pessoal quando ele permite a identificação, direta ou indireta, da pessoa natural através da coleta dos dados. Os dados pessoais direitos, são aqueles que identificam a pessoa inequivocamente, ou seja, sem qualquer informação adicional, como por exemplo, pelo número do RG, CPG, número do passaporte. E os dados pessoais indiretos, são aqueles que necessitam de informações complementares para identificação do titulas, como: endereço, data de nascimento, profissão, geolocalização, entre outros.

1.12 Dado pessoal sensível

O artigo 6º da convenção 108 do conselho da Europa, regulou condições em que podem ser tratados os dados de “categoriais especiais (ou específicas), que a doutrina passou a denominar de “dados sensíveis”, os quais referem-se aos dados pessoais que “oferecem uma vulnerabilidade especial, na medida em que a partir dos

6 Comité Europeu para a Proteção de Dados. Parecer 4/2007 sobre o conceito de dados pessoais no Grupo de Trabalho de proteção de Dados do Artigo 29º. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf Acesso em: 21 de março de 2021.

7 CASTRO, Catarina Sarmento e Castro. Direito da informática, privacidade e dados pessoais. Coimbra: Almedina, 2005, pag. 339.

mesmos é possível adotar decisões discriminatórias ou que, de algum modo, podem causar aos seus titulares prejuízos mais graves de carácter pessoal”[8]

A Lei brasileira, difere o dado pessoal do dado pessoal sensível, que são aqueles 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, quando vinculado a uma pessoa natural (artigo 5º, inciso II, da LGPD).

A doutrina, conceitua os dados sensíveis como sendo "uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação"[9].

Portanto, diante do potencial discriminatório que as coletas desses dados podem gerar, é que o legislador dedicou um regime jurídico mais protetivo em relação aos dados pessoais sensíveis, autorizando a coleta desses dados somente quando houver o consentimento do titular para finalidades determinadas ou para cumprimento de obrigação legal.

Sobre o consentimento, para ser considerado legítimo, este deve vir qualificado com a finalidade do tratamento, sendo vedado expressamente por lei, manifestações genéricas autorizando o tratamento de dados.

Deste modo, exceto para um cumprimento de um dever legal pelo empregador ou para o exercício do direito de defesa em processo judicial, administrativo ou arbitral entre outras exceções tratadas na lei, os dados pessoais dos trabalhadores só poderão ser tratados com base no seu consentimento.

8 HIGUEIRAS. Manuel Heredero. La Directiva Comunitaria de Protección de los datos de Carácter Personal, Arrazandi Editorial, 1997, pág. 116.
9 BIONI, Bruno. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: GEN/Forense, 2020. Pag. 83

Para cumprimento de obrigação legal, é certo que a LGPD não tratou, de forma expressa, sobre as relações de trabalho.

Destaca-se que o artigo 5º da LGPD traz como dados sensíveis a coleta de dados sobre a filiação a sindicato e coleta de dados biométricos. Entretanto, no âmbito das relações de trabalho, a coleta desses dados não traduz, necessariamente, uma discriminação.

Em relação ao primeiro, com a extinção da contribuição compulsória tratada na reforma trabalhista, que prevê que o empregado deve autorizar o desconto de forma prévia, voluntária, individual e expressa, revela-se necessária à coleta dessa informação pelo empregador para que não haja desconto indevido.

No tocante à coleta de biometria, destaca-se que esta pode ser obtida a partir da face, íris, voz.

Nas relações de trabalho, a coleta de dados biométricos é frequentemente utilizada para fins de registro de ponto. O artigo 74 da CLT, estabelece que:

> Art. 74 - Para os estabelecimentos de mais de dez trabalhadores será obrigatória a anotação da hora de entrada e de saída, em registro manual, mecânico ou eletrônico, conforme instruções a serem expedidas pelo Ministério do Trabalho, devendo haver pré-assinalação do período de repouso. (BRASIL, 2018).

No mesmo sentido, o registro de ponto eletrônico é regulamentado pela Portaria 1.510/09 do Ministério do Trabalho.

Não obstante seja possível o controle de jornada por outros meios de controle menos invasivos, é certo que o registro biométrico eletrônico, revela-se o mais eficaz para assegurar a lisura dos horários lançados nos cartões de ponto, inclusive, para assegurar a própria autoria do trabalhador. Deste modo, conclui-se que a coleta de dados biométricos para controle de jornada está devidamente assegurada para cumprimento de uma obrigação legal.

Ademais, a coleta de biometria também é frequentemente utilizada como formas de controle de acesso e segurança nas empresas, situações essas que também legitima a desnecessidade de consentimento do titular, conforme alínea “g” para “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.” (BRASIL, 2018).

Destaca-se, entretanto, que a coleta desses dados sensíveis deverá cumprir a estrita finalidade para o qual foram obtidos, sob pena de violação à Lei Geral de Proteção de dados.

Logo, conclui-se que o rol do artigo 5º da LGPD é um rol exemplificativo, pois a depender do âmbito de aplicação, não será tipo como uma coleta de dados que leva a discriminação, mas sim, para o cumprimento de uma obrigação legal.

1.13 Dado anonimizado e anonimização

Conforme ensina Bruno Bioni, “a antítese de dado pessoal seria um dado anônimo, ou seja, aquele que é incapaz de revelar a identidade de uma pessoa. Diante do próprio significado do termo, anônimo seria aquele que não tem nome nem rosto”[10].

A anonimização dos dados consiste no procedimento de desvincular o dado ao seu respectivo titular e é considerado um grande atrativo para as empresas, pois afasta a incidência da lei de proteção de dados.

Portanto, dados que não identificam uma pessoa natural não são tidos como dados pessoais e não são considerados para os fins previstos na LGPD (artigo 12º da LGPD).

10 BIONI, Bruno. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: GEN/Forense, 2020.Pág. 87.

1.14 Banco de dados

Conforme disciplina o inciso IV, banco de dados consiste em “conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico”.

Importante destacar que a lei é expressa ao mencionar em “suporte eletrônico ou físico”, logo, o banco de dados refere-se ao local onde as informações pessoais são armazenadas, seja em meio eletrônico, seja em meio físico.

1.14 Titular

O artigo 5º, inciso V, prevê que “o titular será a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento” (BRASIL, 2018).

Ou seja, o titular dos dados é o responsável pela existência da Lei Geral de proteção de Dados, pois é ele quem terá os seus dados pessoais tratados.

Destaca-se que o titular nunca perderá essa condição ao fornecer os seus dados, por se tratar de um direito personalíssimo.

1.15 Controlador

Trata-se de pessoa física ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais (artigo 5º, inciso VI, da LGPD).

A definição do controlador no âmbito empresarial, revela-se de suma importância, pois define o responsável por eventuais danos que causar durante o processo de tratamento de dados pessoais.

Na GDPR, o controlador é definido como “a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto

com outras determina as finalidades e os meios de tratamento de dados pessoais" (artigo 4º, item 7, da GDPR).

As principais responsabilidades do controlador são: 1) assegurar aos titulares a garantia de direitos fundamentos de liberdade, intimidade e de privacidade; 2) elaborar relatórios de impacto de proteção de dados pessoais, determinados pela Autoridade Nacional; 3) notificar sobre ocorrência de incidentes de segurança que acarrete riscos ou danos ao titular; 4) adoção de medidas de segurança, técnicas e administrativas; 5) estabelecer regras de boas práticas e de governança; 6) manter o registro das operações de tratamento de dados; 7) dever de transparência; e 8) dever de sigilo.

No âmbito do contexto laboral, o empregador é que desempenhará a figura do controlador, pois será ele quem desempenhará as operações de tratamento dos dados dos empregados-titulares.

No tocante à responsabilização do controlador, o artigo 42 da LGPD e seguintes dispõem que o controlador de dados deve reparar dano patrimonial, coletivo, moral ou individual causado a terceiro.

1.16 Operador

Segundo o artigo 5º, inciso VII, da LGPD, o operador é a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (BRASIL, 2018).

Enquanto ao controlador cabe a tomada de decisões referentes ao tratamento de dados, o operador é quem realizará o tratamento de dados pessoais em nome do controlador. A diferença entre ambos está no poder decisão que cabe ao controlador e subordinação do operador ao controlador.

O artigo 39 da LGPD, prevê que “o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria” (BRASIL, 2018).

Portanto, além das obrigações acima relacionados ao controlador, incumbe ao operador realizar o tratamento de dados de acordo com as instruções do controlador.

É de suma importância a observância da subordinação do operador em relação ao controlador, pois, em caso de inobservância das diretrizes passadas pelo controlador, o operador equipara-se ao controlador (§ 1º do artigo 42 da LGPD).

Nas relações do trabalho, a figura do operador existirá quando o empregador-controlador realizar a contratação de uma pessoa natural ou jurídica para realizar o tratamento de dados em seu nome.

Cabe ressaltar que não é vedado que o encargo de operador seja assumido por empregados da empresa. Nessa hipótese, os empregados que tratarem os dados por ordem do empregador-controlador ostentariam a condição de operadores.

Em recente resolução editada pelo Tribunal de Justiça do Distrito Federal de nº 9, de setembro de 2020, ao instituir a política de privacidade naquele tribunal, o Presidente do Tribunal foi classificado como sendo o controlador e os servidores como sendo os operadores.

No tocante à responsabilidade do operador, este responde solidariamente ao controlador, nos termos do artigo 42 da LGPD.

1.17 Encarregado

O encarregado de proteção de dados, também conhecido como DPO na legislação europeia, é o profissional especialista em proteção de danos, que deve ser nomeado pelo controlador para atuar como “canal de comunicação entre o

controlador, os titulares dos dados e a Autoridade Nacional de Proteção da Dados". (artigo 5º, VIII da LGPD).

Suas atividades estão previstas no § 2º do artigo 41 da LGPD:

> § 2º As atividades do encarregado consistem em:
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. (BRASIL, 2018).

O § 3º do referido artigo disciplina que a ANPD "poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados" (BRASIL, 2018). Portanto, extrai-se que as atividades previstas no §2º são meramente exemplificativas, além de que as empresas não são obrigadas a indicar um controlador.

No § 1º, a norma dispõe que "identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador". (BRASIL, 2018).

O encarregado da proteção de dados pessoais deve possuir domínio da LGPD e sobre proteção de dados, pois será o responsável por administrar todo o fluxo de coleta e tratamento de dados pessoais.

No tocante à responsabilização, diferentemente do controlador e operador, o encarregado não será responsabilizado por danos causados através do exercício de atividades de tratamento de dados pessoais, exceto se comprovado que agiu com dolo.

1.18 Tratamento

Tratamento de dados pessoais significa toda operação ou atividade realizada com os dados pessoais, desde a coleta até a sua eliminação:

> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (BRASIL, 2018).

A Lei Geral de Proteção de Dados é aplicável a todo tratamento de dados pessoais, realizados por pessoa física ou jurídica, com abrangência em todo o território nacional.

Para que o tratamento de um dado seja considerado legítimo, as hipóteses de tratamento têm que se encaixar no artigo 7º ou 11 da LGPD, bem como em observância aos princípios da boa –fé, necessidade, finalidade e adequação.

1.18 Consentimento

O consentimento é definido na LGPD como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (artigo 5º, inciso XII, da LGPD).

O titular dos dados pessoais é o protagonista da LGPD, sendo o seu consentimento uma das hipóteses legais da lei de suma importância para que haja o respeito à liberdade de escolha, a qual deve ser livre, informada, inequívoca e determinada.

Importante destacar que o consentimento não é a única base legal para o tratamento de dados. Entretanto, é inegável que o a figura no consentimento é premissa determinante para a legalidade ou ilegalidade no tratamento de dados pessoais nas relações de consumo.

Não obstante, o mesmo já não se mostra tão eficaz nas relações de trabalho, pois, dado a dependência econômica do empregado e a posição de hierarquia ocupada o empregador, o consentimento não é uma base escolhida como frequência pelas empresas para tratar os dados de seus empregados.

Logo, tutelar o consentimento como justificava legitima para o tratamento de dados nas relações de trabalho não se revela como a mais segura, pois o consentimento deve ser obtido de forma livre, clara e inequívoca com finalidade específica e transparente, sob pena de alegação de vício de vontade.

Neste sentido, Uría Menéndez leciona:

> Apesar de o consentimento poder ser a todo o tempo revogado, ao abrigo do disposto no art. 81.º, n.º 2 do Código Civil, temos muitas dúvidas quanto à eficácia desta norma no âmbito do ambiente laboral, onde os direitos de personalidade se encontram especialmente comprimidos. Talvez tivesse sido mais eficaz que o legislador se limitasse a elencar as situações em que o tratamento de dados dos trabalhadores era permitido, ao invés de colocar a questão exclusivamente dependente do consentimento dos trabalhadores, os quais se encontram numa posição especialmente desconfortável para negar essa pretensão ao empregador. (Uría Menéndez)[11]

Assim, o consentimento no tratamento de dados nas relações de trabalho deve ser analisado à luz de uma relação assimétrica, de hipossuficiência do empregado em reação ao empregador. Desse modo, em razão da subordinação jurídica, o empregado pode encontrar dificuldades para recusar seu consentimento, temendo sofrer represálias se o fizer, o que pode ocasionar em um consentimento com vícios na declaração de vontade e, consequentemente, ser considerada nula de pleno direito[12].

---

[11] MENEDÉZ, Uria. O impacto das novas tecnologias no direito do trabalho e a tutela dos direitos da personalidade do trabalhador. Disponível em: https://www.uria.com/documentos/publicaciones/2242/documento/068apa.pdf?id=1948. Acesso em: 03 de abril de 2021

[12] GASPAR, Gabriela Curi Ramos. LGPD e o tratamento de dados sensíveis nas organizações de tendência. Artigo disponível em: MIZIARA, Raphael. Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Thomson Reuters/Revista dos Tribunais, 2020. Pag. 217

Sobre o livre consentimento dos empregados, no seu parecer 13/2011 sobre o tratamento de dados pessoais no contexto laboral, o Grupo de Trabalho 29 recomendou que as empresas evitem coletar os dados com base no consentimento:

> Quando se pedir a um trabalhador o seu consentimento e ele for potencial ou efetivamente penalizado se o recusar, o consentimento não é válido nos termos do artigo 7.º ou do artigo 8.º, uma vez que não é dado livremente. Se o trabalhador não tiver a possibilidade de o recusar, não existe consentimento. (...) Uma situação problemática é aquela em que o consentimento é uma condição para o recrutamento. O trabalhador pode, em teoria, recusar dar o seu consentimento, mas a consequência pode ser a perda de uma oportunidade de emprego. Nestas circunstâncias, o consentimento não é dado livremente, pelo que não é válido[13].

Neste aspecto, cabe apontar que razões não faltam para questionar se o consentimento de fato se dará de maneira livre, tendo em vista a condição de hipossuficiente do trabalhador diante do empregador. Decerto, dificilmente um candidato a emprego ou um empregado se sentirá à vontade em deixar de consentir com o tratamento de algum dado pessoal requisitado. Afinal, é relativamente presumível que, para o candidato, haverá receio de não conseguir o emprego, ao passo que, na situação do empregado, a intenção é a de ser manter seu emprego, além de estabelecer um bom relacionamento com o empregador.[14]

Ademais, o § 5º do artigo 8º da LGPD dispõe que consentimento pode ser revogado a qualquer tempo pelo titular de dado pessoal. Logo, o tratamento de dados somente com base no consentimento do empregado é considerado como um grande risco, dada essa vulnerabilidade de revogação a qualquer momento.

Quanto ao ônus da prova da validade do consentimento, dado o caráter protetivo da LGPD, incumbirá ao empregador- controlador o ônus de provar que o consentimento do titular de dados pessoais foi fornecido conforme os requisitos legais.

---

[13] Directiva 95/46/CE. Parecer 13/2011 sobre serviços de geolocalização em dispositivos móveis inteligentes. Disponível em: https://www.gpdp.gov.mo/uploadfile/2014/0505/20140505071557367.pdf Acesso em: 04 de abril de 2021

[14] CALCINI, Ricardo Souza; MACHADO, Gustavo Carvalho. Efeitos da Lei Geral de Proteção de Dados nas relações de trabalho. Disponível em: https://www.irib.org.br/noticias/detalhes/artigo-efeitos-da-lei-geral-de-protecao-de-dados-nas-relacoes-de-trabalho-undefined-por-gustavo-carvalho-machado-e-ricardo-souza-calcini

Por fim, a LGPD traz algumas hipóteses justificadores em que o consentimento pode ser dispensado, como por exemplo, para cumprimento de obrigação legal ou regulatória, sendo hipóteses de tratamento mais seguras a seguir nas relações de trabalho.

No âmbito das relações de trabalho, prescindirá de consentimento o tratamento de dados promovido em função de cumprimento de obrigações legais ou regulatórias pelos agentes do tratamento (por exemplo, envio de dados ao Ministério do Trabalho, INSS e Caixa Econômica Federal por meio de Caged, Rais e Sefip), ou, ainda, para fins de execução de políticas públicas pela administração federal (por exemplo, seguro-desemprego e abono salarial)[15].

1.19 Bloqueio

O titular dos dados pessoais tem o direito de requerer ao controlador a qualquer momento, o bloqueio ou a eliminação dos seus dados que foram tratados de forma desnecessária, excessiva ou em desconformidade, nos termos do artigo 18, inciso IV, da LGPD:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> (...)
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei. (BRASIL, 2018).

Os agentes de tratamento de dados que cometer infrações às normas previstas na LGPD, terão bloqueados os dados pessoais até que se regularize a infração cometida, conforme disposição trazida no artigo 52, da LGPD:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> (...)

15 CALCINI, Ricardo Souza; MACHADO, Gustavo Carvalho. Efeitos da Lei Geral de Proteção de Dados nas relações de trabalho. Disponível em: https://www.irib.org.br/noticias/detalhes/artigo-efeitos-da-lei-geral-de-protecao-de-dados-nas-relacoes-de-trabalho-undefined-por-gustavo-carvalho-machado-e-ricardo-souza-calcini

> V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização. (BRASIL, 2018).

1.20 Eliminação

De acordo com o artigo 18, inciso VI, o titular de dados tem o direito de obter do controlador a qualquer momento a eliminação dos dados pessoais tratados com o consentimento do titular.

Se os agentes de tratamento de dados pessoais não realizarem o tratamento de dados dentro das hipóteses legais previstas na LGPD, deverão realizar a eliminação desses dados pessoais.

Os dados pessoais também deverão ser eliminados após atingirem a finalidade a qual se buscou o tratamento. Nesse sentido, a eliminação deverá ocorrer nas seguintes hipóteses previstas na lei:

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
> II - fim do período de tratamento;
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
> IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. (BRASIL, 2018)

Há situações, entretanto, que a lei autoriza a conservação dos dados, mesmo após o término do seu tratamento. São as hipóteses previstas no artigo 16 da LGPD:

> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
> I - cumprimento de obrigação legal ou regulatória pelo controlador;
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL, 2018)

No âmbito das relações do trabalho, o prazo que todo empregador deverá guardar os dados de seu empregado é de dois anos da data da extinção da relação contratual.

1.21 Transferência internacional de dados

Com a entrada em vigor da LGPD, enfim o Brasil passou a ter legislação específica sobre a transferência internacional de dados, possibilitando que as brasileiras alcancem o mesmo patamar das empresas internacionais que se adequaram ao regulamento europeu e que agora podem realizar transações comerciais com o Brasil com o mesmo nível de segurança praticado nos demais países que também possuem políticas de privacidade de dados.

De acordo com o artigo 33 da LGPD, as empresas estão autorizadas a realizarem transferências de dados pessoais para outros países, desde que proporcionem adequadamente a proteção de dados pessoais de acordo com a lei brasileira.

Destaca-se que o artigo 33 é taxativo, sendo permitido, portanto, a transferência internacional de dados somente nas nove hipóteses elencadas nos incisos inseridos no referido artigo.

1.22 Uso compartilhado de dados

De acordo com Selma Carloto[16], quando os dados pessoais forem tratados com base no consentimento e haver a necessidade de compartilhamento pelo controlador com outros controladores, este deverá obter novo consentimento específico para esta nova finalidade, salvo se a nova hipótese ensejadora de tratamento tiver outro fundamento legal, com base no artigo 7º ou 11º da LGPD.

16CARLOTO, Selma. Lei Geral da Proteção de Dados: enfoque nas relações de trabalho. São Paulo: LTr, 2020. Pág. 78.

1.22 Relatórios de impacto à proteção de dados pessoais

Denominado como uma nova ferramenta de *compliance,* segundo o artigo 5º, inciso XVII, da LGPD, o Relatório de Impacto à Proteção de Dados Pessoais – DPIA, é o instrumento utilizado pelo controlador nas hipóteses em que o tratamento de dados pessoais possa gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais, servindo como mecanismo de mitigação de riscos.

Conforme previsão contida no artigo 38 da LGPD, a ANPD poderá exigir do controlador a elaboração do relatório referente às operações de tratamento, observados os segredos comercial e industrial. Ademais, o referido artigo dispõe que

> [...] o relatório deverá conter, no mínimo, descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. (BRASIL, 2018)

A LGPD menciona explicitamente algumas condições básicas sobre quando o relatório de impacto se faz necessário: a) quando o tratamento de dados pessoais tiver como fundamento o interesse legítimo do Controlador. (Art. 10º, II, § 3º, LGPD); b) quando o tratamento de dados pessoais gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. (Art. 5º, XVII, LGPD); c) quando ocorrer o tratamento de dados pessoais sensíveis, especialmente em grandes volumes. (Art. 38º, LGPD); d) quando o tratamento for relativo a dados pessoais provenientes de fora do território nacional e que não sejam objeto de comunicação, no uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência. (Art. 4º, IV, § 3º, LGPD).

O relatório de impacto à proteção de dados pessoais tem a finalidade de minimizar sistematicamente os riscos que possam advir da coleta de dados, avaliando e mapeando os riscos no tratamento dos dados que serão objeto do relatório.

Fabrício Mota Alves[17], disciplina que o relatório de impacto é uma forma eficaz de mostrar conformidade com a lei e agrega valor às atividades econômicas:

> [...] O investimento de tempo e de recursos econômicos ou de pessoal para esse tipo de procedimento agrega valor às atividades corporativas de uma empresa, na medida em que reforçam a permanente preocupação de mitigação de riscos ao titular de dados pessoais.

A elaboração do relatório se inicia com o detalhamento de todos as fases de tratamento pelos quais os dados pessoais passam na operação, assim como das bases legais aplicáveis e as medidas de segurança adotadas. Esse detalhamento permite identificar os pontos de fragilidade da operação, que podem representar algum risco aos direitos dos titulares dos dados e, diante dessa identificação, poder endereçar quais medidas devem ser tomadas, como a implementação de novas medidas e mecanismos que demonstrem o cumprimento da Lei, como até mesmo, a descontinuidade do projeto.

Deste modo, recomenda-se que ele seja elaborado antes do início do projeto de tratamento de dados pessoais, para que o controlador visualize antecipadamente se todos os requisitos legais estão sendo cumpridos, colaborando, inclusive, com o cumprimento de adoção de medidas protetivas à privacidade e segurança dos dados.

Ademais, a elaboração antecipada do relatório, além de trazer benefícios para empresa na prevenção e mitigação dos riscos, se mostra relevante para demonstrar para a ANPD que a empresa está agindo em conformidade com as normas legais.

Portanto, o relatório de impacto à proteção de dados dá sustentação ao princípio de responsabilização e prestação de contas, pois com este documento o controlador demonstrará “a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais” (artigo 6º, X, da LGPD).

---

17 ALVES, Fabricio da Mota. Avaliação de impactos sobre a proteção de dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. Comentários ao GDPR. São Paulo: Thompson Reuters, 2018. Pág. 186.

1.23 Autoridade Nacional de Proteção de Dados

A Autoridade Nacional de Proteção de Dados (ANPD), surgiu após a sanção da Medida Provisória 869/18, convertida na Lei 13.853/19, sendo responsável por fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais.

Conforme disposto no artigo 5º, XIX, da LGPD, a Autoridade Nacional é um "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei", sendo composta pelo Conselho Diretor, órgão máximo de direção; Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; Corregedoria; Ouvidoria; órgão de assessoramento jurídico próprio; e unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta lei (Artigo 55-C, da LGPD).

O artigo 55-5 da LGPD elenca as atribuições da ANPD, cabendo destaque o dever de zelar pela proteção dos dados pessoais e pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei.

Caberá à ANPD elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, bem como de regulamentos, orientações, procedimentos e relatórios de impacto.

Ademais, a ANPD além de zelar pela privacidade e proteção dos dados, é o órgão responsável por fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo, o qual deverá assegurar o contraditório, a ampla defesa e o direito de recurso.

Por fim, a ANPD tem como objetivo auxiliar as empresas, sociedade e o governo a criar a cultura da proteção de dados pessoais, orientando-as sobre como agir e se adequar às normas da LGPD.

2 FUNDAMENTOS DA LEI GERAL DE PROTEÇÃO DE DADOS

O artigo 2º da LGPD disciplina que a proteção de dados tem como fundamentos:

> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018)

A proteção aos direitos fundamentais, revela-se evidente no referido artigo, guardando relação ao respeito à privacidade, à inviolabilidade da intimidade, da honra e da imagem previstos no artigo 5º, X, da CF/88 e a liberdade de expressão, previsto no artigo 5º, IX, da CF/88.

Verifica-se que o direito à autodeterminação específica não encontra previsão expressa na Constituição Federal. Entretanto, é reconhecida pela doutrina como direito fundamental, tendo relação direta com o direito à privacidade e à intimidade.

O direito de autodeterminação informativa foi delineado pelo Tribunal Constitucional Alemão no julgamento do caso da Lei do Censo de 1983, quando foi determinado que os cidadãos fornecessem seus dados pessoais para auferir estatisticamente a distribuição espacial e geográfica da população do país. A lei previa, contudo, a possibilidade de cruzamento dos dados com os registros públicos para a finalidade de execução de “atividades administrativa”, o que foi considerado inconstitucional pelo Tribunal alemão, que determinou que os dados somente fossem utilizados para fins de recenseamento[18].

De acordo com Bruno Bioni, a decisão estabeleceu importantes precedentes para o direto à proteção de dados, tais como:

18 BIONI, Bruno. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: GEN/Forense, 2020. Pág. 97.

> a) a proteção de dados pessoais como um direito de personalidade autônomo e a compreensão do termo autodeterminação informacional para além do consentimento; b) a função e os limites do consentimento do titular dos dados".19 .

O julgado consagrou o conceito de autodeterminação informativa como o direito que o cidadão possui em determinar e controlar a utilização de seus dados pessoais por terceiros. Trata-se de empoderar o titular na gestão e controle de seus dados[20].

Rony Vainzof[21], conceitua autodeterminação informativa como:

> O controle pessoal sobre o trânsito de dados relativo ao próprio titular – e, portanto, uma extensão de liberdades do indivíduo – conjuga as duas já mencionadas concepções de privacidade de dados: a primeira de caráter negativo e estático; e a moderna, em que a intervenção (proteção) é dinâmica, durante todo o ciclo de vida dos dados nos mais variados meios em que possa circular.

Portanto, assim é o exercício do conceito determinado de autodeterminação informativa, onde o titular dos dados pessoais exerce o efetivo controle sobre utilização dos seus dados pessoais, pois, com base na sua autonomia de vontade, decidirá se os seus dados pessoais poderão ser objeto de tratamento por terceiros.

Diante da relevância do controle de dados pelo titular, o conceito da autodeterminação informativa se firmou como fundamento para a proteção de dados na LGPD, no inciso II do artigo 2º, estando compreendida dentro dos direitos da personalidade do indivíduo.

Portanto, para que titular de dados tenha o completo direito à privacidade, é fundamental que tenha o controle da destinação dos sobre os seus próprios dados pessoais.

---

19 BIONI, Bruno. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: GEN/Forense, 2020. Pág. 97 e 98.
20 YOSHIDA, Victoria Melo. Autodeterminação informativa, riscos cibernéticos e proteção de dados pessoais: a emergência de um novo compliance. In Revista do curso de direito da Unifacs. Porto Alegre. Paixão Editores. V. 19, 2019. Pág. 295.
21 RONY VAINZOF. LGPD: Lei Geral de Proteção de Dados Pessoais comentada. Viviane Nóbrega Maldonado e Renato Opice Blum, coordenadores. São Paulo: Thomson Reuters Brasil, 2019. Pág. 27.

Destaca-se, entretanto, que o direito à privacidade não é absoluto, o qual é relativizado pela vontade do próprio titular, bem como nas hipóteses que pode haver o tratamento de dados para cumprimento de obrigação legal.

3 TRATAMENTO DE DADOS PESSOAIS NAS RELAÇÕES DE TRABALHO

As hipóteses de tratamento de dados pessoais que mais refletirão nas relações de trabalho serão para: a) fundada no consentimento; b) para cumprimento de obrigação legal ou regulatória; b) para execução de contrato ou procedimentos preliminares relacionados ao contrato; c) para o exercício regular de direitos em processo judicial, administrativo ou arbitral.; d) para a proteção da vida ou da incolumidade física do titular ou de terceiro; e) interesses legítimos do controlador ou de terceiro.

3.1 Consentimento

De acordo com o conceito de consentimento, para que seja possível o tratamento de dados pessoais, é necessário que haja a manifestação livre, informada e inequívoca por parte do empregado-titular, o qual deve consentir com o tratamento de dados pessoais para uma finalidade determinada e específica.

Conforme já explanado às folhas 25, o consentimento não será válido se o empregado o proceder somente com medo de sofrer retaliações pelo empregador se assim não o fizer.

Em razão disso, é que o tratamento de dados, pautado apenas no consentimento, não ser traduz na melhor hipótese para o tratamento de dados na relação empregatícia, exceto se o tratamento realizado demonstrar inequívocas vantagens ao trabalho, hipótese que poderá ser utilizado com segurança como fundamento para o tratamento de dados nas relações empregatícias.

3.2 Obrigação legal

O cumprimento de obrigação legal ou regulatória é a segunda hipótese em que o tratamento de dados pessoais é permitido e é a hipótese mais segura de tratamento nas relações de trabalho.

No contexto laboral, a coleta de dados pessoais dos empregados ocorre, não só para a execução do contrato, como também para a observância de obrigações legais.

De acordo com Ana Frazão, a intenção do legislador, ao incluir a hipótese de obrigações legais para o tratamento de dados, foi atender ao interesse público, porém, deixando evidente que, mesmo nessas hipóteses, há que ser observar a os princípios previstos da lei:

> O inciso II do art. 7º da LGDP traz a hipótese de cumprimento de obrigação legal ou regulatória pelo controlador. Com efeito, em casos assim, o tratamento de dados é considerado necessário para atender o interesse público que justifica a obrigação legal ou regulatória. Todavia, mesmo nesse caso, os controladores deverão observar os princípios pertinentes, especialmente no que toca (i) à adstrição do tratamento à finalidade específica de cumprimento da determinação legal, (ii) à adoção dos meios adequados e necessários para tal, bem como (iii) à preocupação com todos os direitos do titular, dentre os quais se destaca o direito de ser informado do tratamento de dados (§ 1º, do art. 7º, da LGPD) e o direito de ter os dados disponibilizados nos exatos termos do que for especificado pela autoridade nacional (§ 2º, do art. 7º, da LGPD). [22]

Portanto, se o empregador necessitar coletar os dados pessoais do empregado-titular para cumprimento de uma obrigação legal, a lei autoriza o tratamento de dados pessoais e sensíveis visando cumprir tal exigência legal.

Por exemplo, a apresentação da RAIS e do e-social que o empregador precisa apresentar para gestão governamental; informações repassadas ao INSS para viabilizar concessões de benefícios; para fins de recolhimento do FGTS; coleta de dados bancários para pagamento de remuneração; coleta da biometria para controle

22 FRAZÃO, Ana. Nova LGPD: as demais hipóteses de tratamento de dados pessoais. Disponível em: www.jota.info/opiniao-e-analise/artigos/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018. Acesso em 01 de abril de 2021

de ponto; entre outras obrigações que será necessário o tratamento de dados pelo empregador para execução do contrato e para cumprimento de obrigações legais.

Nesses casos, não há que se falar no consentimento do empregado-titular, pois a coleta se dá para fins de cumprimento de obrigações legais e/ou regulatórias pelo empregador-controlador.

Não obstante, não se pode olvidar o dever do empregador de informar ao empregado-titular sobre a finalidade, forma e duração de tratamento de seus dados, além da observância aos princípios que sustentam a base da LGPD.

3.3 Execução de contrato ou procedimentos preliminares relacionados ao contrato

Outra hipótese lícita para tratamento de dados pessoais, ora prevista no inciso V, do artigo 7 da LGPD, é para a execução de contrato ou de procedimentos preliminares relacionados ao contrato.

No âmbito das relações do trabalho, são inúmeras as informações coletadas nas fases pré-contratuais, contratual e pós-contratual.

Portanto, os dados pessoais poderão ser tratados, tanto para procedimentos preliminares na fase pré-contratual, como também, em decorrência das obrigações contratuais firmadas que o titular figure como integrante.

3.4 Exercício regular de direitos em processo judicial, administrativo ou arbitral

Outra hipótese de manuseio lícito de dados pessoais é aquele referente às operações que visem o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Essa hipótese é assegurada, inclusive, em decorrência dos princípios do contraditório e da ampla defesa assegurados constitucionalmente

Neste sentido, Ana Frazão esclarece que essa ressalva foi expressamente incluída para deixar claro o direito que as partes têm de produzir provas umas contra as outras:

> Outra importante hipótese de tratamento de dados é o exercício regular de direitos em processo judicial, administrativo ou arbitral (art. 7º, VI, da LGPD), ressalva fundamental para deixar claro que a proteção aos dados pessoais não compromete o necessário direito que as partes têm de produzir provas umas contra as outras, ainda que estas se refiram a dados pessoais do adversário[23].

Deste modo, é lícito o empregador armazenar os dados do ex-empregado durante o período prescricional útil à propositura de eventual demanda trabalhista, ou seja, até o limite de dois anos após extinto o contrato de trabalho.

3.5 Proteção da vida ou da incolumidade física do titular ou de terceiro

Outra hipótese de tratamento lícito assegurada por lei é quando se tratar de hipótese de tratamento de dados necessária para proteção da vida ou incolumidade física do titular, cabendo até mesmo, a flexibilização do direito à privacidade.

No cenário atual de pandemia decorrente do coronavírus, facilmente encontramos situações onde as empresas medem a temperatura dos funcionários com intuito de evitar a proliferação vírus, sendo necessário tratar esse dado para proteger a vida do próprio empregado.

Deste modo, havendo risco à vida e incolumidade física do empregado-titular, o empregador está autorizado a tratar os dados pessoais, inclusive os dados sensíveis (artigo 11, II, e da LGPD), sem o consentimento do titular, haja vista a garantia do direito à vida que encontra previsão no artigo 5º da Constituição Federal.

---

23 FRAZÃO, Ana. Nova LGPD: as demais hipóteses de tratamento de dados pessoais. Disponível em: www.jota.info/opiniao-e-analise/artigos/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018. Acesso em 01 de abril de 2021

3.6 Interesses legítimos do controlador ou de terceiro

O tratamento de dados pode ter base legal o legítimo interesse do empregador-controlador.

Tal como o consentimento, a utilização dessa base legal requer cautelas, sendo recomendável sua utilização somente quando não houver outra base legal aplicável.

Não há definição legal no ordenamento jurídico brasileiro acerca da definição do legítimo interesse. Entretanto, o artigo 10 da LGPD, preconiza que o legítimo interesse do controlador somente poderá justificar-se para finalidade legítimas, desde que respeitados os direitos e liberdades fundamentais do titular, conforme rol exemplificativo descrito abaixo:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, 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. (BRASIL, 2018)

O legítimo interesse do controlador, destaca-se dentre as demais bases legais dado a elasticidade de hipóteses de aplicação proporcionada ao controlador, as quais, repisa-se, merecem cautelas quando aplicadas, sendo, preferencialmente precedidas de testes de ponderação quando o controlador optar por utilizá-la.

No contexto laboral, para que se justifique o interesse do empregador no tratamento de dados dos empregados há que se demonstrar que a situação concreta é necessária para o apoio e promoção de atividades do controlador, visando melhorias no desenvolvimento da atividade empresarial, por exemplo, em hipóteses em que a empresa realiza pesquisas de satisfação entre os colaboradores, visando a promoção de melhoria do ambiente de trabalho, como também pesquisas de vi para melhoria estrutural, as quais podem resultar em uma melhoria no desempenho da produção, entre outras.

Fabiano Zavanella, sobre a utilização dos dados pessoais do trabalhador e o legítimo interesse do empregado a partir do poder de direção, esclarece que:

> Pode-se sustentar que a existência da relação jurídica laboral (o contrato de emprego), por si, já consista em suporte fático da provável existência de interesse patronal no tocante aos dados do empregado, porém, a premissa seria equivocada.
> Ocorre que a situação concreta exigida pela LGPD há de ser verificada no bojo da relação jurídica preexistente e não na simples existência daquela. O que se pretende afirmar é que, dentro da relação jurídica, no seu desenvolvimento, há de se ter uma situação concreta que justifique o interesse do empregador no tratamento de dados. Observe-se que esse interesse não pode ser devido à necessidade do tratamento dos dados, de modo imperioso e imprescindível, para fim de cumprimento de obrigação legal, pois, neste caso, a base legal seria outra (inciso II). Logo, o legítimo interesse deve ter outro suporte fático, ou seja, decorrer de situação concreta distinta da exigência da informação para fim de cumprir o que a ordem posta impõe ao empregador.

Quanto à segunda hipótese, o artigo 10, inciso II da LGPD, exige que as ações realizadas pelo controlador para apoio e promoção de atividades, devem representar ao titular de dados proteção 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.

Para proteção do titular e do regular exercício de seus direitos, é legítimo o controlador realizar o tratamento de dados nas situações ligadas à segurança que possa beneficiar o titular de dados, observando-se a finalidade do tratamento no caso concreto.

Neste aspecto, a diretriz n° 3/2019 da EDPB (*European Data Protection Board*)[24], traz orientações sobre o processamento de dados pessoais por meio de câmeras se segurança:

> Antes da utilização, as finalidades do tratamento têm de ser determinadas em pormenor (artigo 5.º, n.º 1, alínea b)). A videovigilância pode servir muitas finalidades, por exemplo apoiar a proteção de bens e de outros ativos, apoiar a proteção da vida e da integridade física dos indivíduos e recolher provas para ações cíveis6 . Estas finalidades do controlo devem ser documentadas por escrito (artigo 5.º, n.º 2) e têm de ser especificadas para cada câmara de

[24] Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf Acesso em: 28 de março de 2021.

> vigilância em utilização. As câmaras que são utilizadas para a mesma finalidade por um único responsável pelo tratamento podem ser documentadas em conjunto. Além disso, os titulares dos dados devem ser informados sobre a(s) finalidade(s) do tratamento em conformidade com o artigo 13.º (ver secção 7, Obrigações em matéria de transparência e informação). A videovigilância baseada na mera finalidade de «segurança» ou «salvaguarda da segurança» não é suficientemente específica (artigo 5.º, n.º 1, alínea b)). Além disso, é contrária ao princípio de que os dados pessoais devem ser objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados (ver artigo 5.º, n.º 1, alínea a).
>
> [...]
>
> Partindo do princípio de que a videovigilância é necessária para proteger os interesses legítimos de um responsável pelo tratamento, um sistema de videovigilância só pode ser acionado se aos interesses legítimos do responsável pelo tratamento ou de terceiros (por exemplo, proteção de bens ou da integridade física) não se sobrepuserem os interesses ou os direitos e liberdades fundamentais do titular dos dados. O responsável pelo tratamento tem de considerar 1) em que medida o controlo afeta os interesses e os direitos e liberdades fundamentais dos indivíduos e 2) se este controlo resulta em violações ou consequências negativas no que diz respeito aos direitos do titular dos dados. Na verdade, a ponderação dos interesses é obrigatória. Os direitos e liberdades fundamentais, por um lado, e os interesses legítimos do responsável pelo tratamento, por outro, têm de ser cuidadosamente avaliados e ponderados.

Nesse sentido, destaca-se que os parágrafos 1º, 2º e 3º do artigo 10º da LPGD disciplinam que, quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, além de que o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

Destaca-se que o artigo 10 expressamente certifica que o uso do legítimo interesse deve ocorrer somente para situações concretas e para o atendimento de determinada finalidade, estando sujeito a eventual apresentação de relatório de impacto à proteção de dados pessoais (§ 3º, do artigo 10 da LGPD).

Importante destacar que o legítimo interesse não é aplicável para o tratamento de dados sensíveis (artigo 11, da LGPD).

Portanto, para ser considerado legítimo o interesse nessa hipótese legal, os agentes de tratamento devem se pautar nos princípios de proteção de dados para que não seja violado nenhum direito do titular de dados pessoais.

4 NEGOCIAÇÃO COLETIVA PARA O TRATAMENTO DE DADOS PESSOAIS

A LGPD não tratou expressamente em seus dispositivos a possibilidade de regulamentação de tratamento de dados por meio de normas coletivas.

Diferentemente, o Regulamento Europeu de Proteção de Dados, reconhecendo esse caráter específico do trâmite de dados nas relações de emprego, prevê, no seu artigo 88, a sua possibilidade de pactuação por meio de negociação coletiva:

> Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.

Da leitura do artigo 88, verifica-se que o Parlamento Europeu admite que, na ordem interna de cada Estados-Membros, seja adotado disposições mais específicas para garantir a defesa dos direitos e liberdades dos trabalhadores no que diz respeito ao tratamento de seus dados pessoais.

Não obstante a ausência de previsão legal na LGPD em relações às relações de trabalho, é oportuno destacar que a reforma trabalhista consagrou a prevalência do negociado sobre o legislado, ampliando significativamente as hipóteses em que a convenção coletiva e o acordo coletivo prevalecem sobre a legislação.

Há que se observar, entretanto, as proteções constitucionais do trabalhador, tais como o direito à privacidade e à intimidade, que não podem ser objeto de negociação coletiva. No mesmo sentido, não seria válida norma coletiva que dispense o consentimento do trabalhador, naquelas hipóteses nas quais é necessário haver o seu consentimento.

É relevante destacar que a proposta de emenda à Constituição 17/19[25] insere a proteção de dados pessoais na lista de garantias fundamentais do cidadão. Logo, para que a norma coletiva seja considerada válida, deve ser interpretado o artigo 7º, inciso XXVI, da Constituição Federal, que estabelece o reconhecimento das convenções e acordos coletivos de trabalho, mas, apenas, como direito dos trabalhadores que visem à melhoria de sua condição social, nunca retrocedente.

Deste modo, tendo como fundamento o artigo 611-A da CLT e o artigo 7º XXVI da Constituição Federal, os sindicatos e as empresas podem realizar ajustes questões específicas sobre o tratamento de dados em acordos ou convenções coletivas, desde que observados e garantidos os princípios fundamentais constitucionais, ora garantidos, inclusive, pela própria LGPD (artigo 2º).

5 SANÇÕES ADMINISTRATIVAS PREVISTAS PELA LEI GERAL DE PROTEÇÃO DE DADOS

O descumprimento aos direitos previstos na Lei Gral de Proteção de Dados, implicará às empresas a aplicação de multas que podem alcançar o valor de 50 milhões de reais por infração, sem prejuízo de responder por outras sanções administrativas aplicadas pela Autoridade Nacional de Proteção de Dados.

A ANPD é o órgão responsável por zelar, implementar e fiscalizar o cumprimento efetivo da norma.

Portanto, se identificada o descumprimento ou falta de adequação às normas, as empresas poderão ser penalizadas com multas aplicadas por parte da ANPD, destacando que, apesar de estar em vigor desde 18 de setembro de 2020, as sanções administrativas somente serão aplicadas a partir de agosto de 2021.

[25] Proposta de Emenda à Constituição n° 17, de 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594 Acesso em: 01 de abril de 2021.

O artigo 52 da LGPD dispõe sobre as sanções que os agentes de tratamento estarão sujeitos em razão das infrações cometidas às normas previstas na lei:

> Artigo 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I. advertência, com indicação de prazo para adoção de medidas corretivas;
> I. multa simples, de até 2% do faturamento da pessoa jurídica de Direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50 milhões por infração;
> III. multa diária, observado o limite total a que se refere o inciso II;
> IV. publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V. bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI. eliminação dos dados pessoais a que se refere a infração;
> VII.(vetado);
> VIII(vetado);
> IX.(vetado).
> X. suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI. suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período;
> XII. proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (BRASIL, 2018).

As sanções previstas no artigo 52 são severas e podem impactar drasticamente a atividade empresarial, não só no âmbito financeiro, como também no ponto de vista reputacional, pois, além das sanções aplicadas e a possibilidade de bloqueio e/ou eliminação dos dados pessoais, a empresa que violar a norma estará sujeita à “publicitação da infração após devidamente apurada e confirmada a sua ocorrência”. (artigo 52, inciso IV, da LGPD).

Não obstante, qualquer punição somente será aplicada após o regular procedimento administrativo que garanta a observância do princípio constitucional do contraditório e da ampla defesa.

6 RESPONSABILIDADE CIVIL E DO RESSARCIMENTO DE DANOS NA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados possui um capítulo dedicado à responsabilidade civil em decorrência da violação ao direito à intimidade ou à privacidade decorrente do tratamento de dados pessoais.

O artigo 42 da LGPD, prevê a possibilidade de reparação por danos patrimoniais ou morais, quando houver violação à legislação de proteção de dados pessoais.

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso. (BRASIL, 2018)

Destaca-se, a lei não traz a culpa, de forma expressa, como elemento necessário para configuração da responsabilidade subjetiva, tampouco faz qualquer alusão ao nexo causal, requisito necessário para configuração da responsabilidade objetiva, havendo, portanto, divergências na doutrina quanto à natureza jurídica da responsabilidade civil em relação aos atos cometidos pelos agentes de tratamento.

Gustavo Tepedino, Aline de Miranda Terra e Gisela Sampaio da Cruz Guedes, na obra “fundamentos do direito civil”, analisam a responsabilidade civil na LGPD e entendem que o regime adotado pelo o legislador foi o da responsabilidade subjetiva:

> O único dispositivo da LGPD que remetia para a responsabilidade objetiva foi retirado no trâmite legislativo, o que é um dado significativo para a interpretação da lei. O próprio histórico de tramitação do projeto de lei que deu origem à LGPD evidencia, portanto, a opção do legislador pela responsabilidade subjetiva. A versão inicial do Projeto de Lei n.º 5276 trazia, no Capítulo sobre "Transferências internacionais de dados”, uma regra geral expressa de responsabilidade solidária e objetiva desses agentes pelos danos causados em virtude do tratamento de dados (art. 35). (...) Diferentemente desse primeiro texto, todas as versões subsequentes do projeto, até a versão finalmente sancionada da LGPD, passaram a não mais mencionar, como regra geral, um regime de solidariedade ou objetividade na responsabilidade pelos danos decorrentes do tratamento de dados pessoais. A referência expressa à responsabilidade objetiva foi completamente eliminada do texto legal. Paralelamente a isso, ainda no período de tramitação do projeto, o caput do art. 42 da LGPD sofreu uma alteração importante: a expressão"em violação à legislação de proteção de dados pessoais" foi acrescentada, o que também evidencia a opção do legislador pela responsabilidade subjetiva. Os agentes de tratamento não responderão em toda e qualquer situação em que causarem danos a terceiros, mas apenas quando isso ocorrer em violação à legislação de proteção de dados pessoais, ou seja, quando a sua conduta não se adequar ao standard estabelecido pelo próprio legislador"
>
> Quando se discute cumprimento de deveres, o que no fundo está sendo analisado é se o agente atuou ou não com culpa. Assim, apesar de a LGPD não ser explícita em relação à natureza da responsabilidade dos agentes de tratamento de dados, como é o Código de Defesa do Consumidor ao adotar a responsabilidade objetiva, a interpretação sistemática da LGPD leva à conclusão de que o regime adotado por este diploma foi mesmo o da responsabilidade subjetiva.
>
> Não obstante as semelhanças com o Código de Defesa do Consumidor, é essencial destacar que, enquanto o Código de Defesa do Consumidor tem pelo menos dois artigos expressamente indicando a natureza objetiva da responsabilidade (arts. 12 e 14 – ambos se valem da expressão “independentemente de culpa”, que deixa clara a opção do legislador pela responsabilidade objetiva), não há qualquer norma análoga na LGPD. O art. 42 da LGPD não faz referência expressa à culpa como elemento da responsabilidade civil, mas também não faz qualquer alusão ao risco como fundamento da responsabilidade objetiva.[26]

Portanto, entendem os autores que, caso fosse a intenção do legislador atribuir a responsabilidade objetiva, assim como ocorre no código de defesa do consumidor, não caberia a discussão de cumprimento ou descumprimento de obrigações da legislação de proteção de dados.

---

[26] TEPEDINO, Gustavo; TERRA, Aline de Miranda; GUEDES, Gisela Sampaio. Fundamentos do Direito Civil. Volume 4. Editora Forense. 2020. Págs. 236-252.

> A lógica da responsabilidade objetiva é outra: não cabe discutir cumprimento de deveres, porque a responsabilidade objetiva não decorre do descumprimento de qualquer dever jurídico". Quando se discute cumprimento de deveres, o que no fundo está sendo analisado é se o agente atuou ou não com culpa. Assim, apesar de a LGPD não ser explícita em relação à natureza da responsabilidade dos agentes de tratamento de dados, como é o Código de Defesa do Consumidor ao adotar a responsabilidade objetiva, a interpretação sistemática da LGPD leva à conclusão de que o regime adotado por este diploma foi mesmo o da responsabilidade subjetiva. Não obstante as semelhanças com o Código de Defesa do Consumidor, é essencial destacar que, enquanto o Código de Defesa do Consumidor tem pelo menos dois artigos expressamente indicando a natureza objetiva da responsabilidade (arts. 12 e 14 – ambos se valem da expressão “independentemente de culpa”, que deixa clara a opção do legislador pela responsabilidade objetiva), não há qualquer norma análoga na LGPD. O art. 42 da LGPD não faz referência expressa à culpa como elemento da responsabilidade civil, mas também não faz qualquer alusão ao risco como fundamento da responsabilidade objetiva.

Selma Carloto, por outro lado, entende que se a atividade de tratamento envolver risco para as liberados civis e os direitos fundamentais dos titulares de dados, a responsabilidade deixa de ser subjetiva e passa a ser objetiva, de acordo com o artigo 977, parágrafo único do Código Civil:

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.(BRASIL, 2002)

Para os que defendem essa teoria, o exercício da atividade de tratamento de pessoais está vinculado a um risco inerente, pois a lei adota o princípio da necessidade, o qual impõe *a* "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (artigo 6, III, da LGPD).

Defensores dessa teoria citam ainda que a lei, ao adotar a inversão do ônus da prova, tal como o Código de Defesa do consumidor, revela a opção do legislado à aplicação da responsabilidade objetiva.

Não obstante, extrai-se do texto legal que não basta meramente que a atividade desempenhada seja considerada de risco para que seja atribuída ao agente

a responsabilidade civil (artigo 43, II da LGPD), mas sim, é necessário que a conduta do agente viole diretamente a lei de proteção dados, conforme previsões contidas nos artigos 42 e 44 da LGPD.

Nesse sentido, o entendimento de Gisela Sampaio:

> O inciso II (do art. 43) reflete, portanto, o regime subjetivo de responsabilidade adotado pela LGPD para o tratamento de dados, porque está intrinsicamente vinculado ao elemento culpa e, exatamente por isso, sua redação não se assemelha à do CDC. Enquanto o CDC isenta de responsabilidade o fornecedor que demonstrar que o defeito inexiste, que é um parâmetro mais objetivo, a LGPD exime do dever de indenizar o agente de tratamento que não tiver violado a lei ao exercer o tratamento de dados que lhe era atribuído.[27]

Deste modo, denota-se que a responsabilidade prevista na LGPD é subjetiva, necessitando da demonstração da culpabilidade do agente de tratamento de dados.

6.1 Responsabilidade solidaria dos agentes

De acordo com o artigo 42 da LGPD, tanto o controlador, como o operador serão responsáveis, de forma solidária, pelos danos patrimoniais, morais, individuais e coletivos que causarem a outrem no tratamento de dados pessoais, em violação à legislação de proteção de dados pessoais.

Entretanto, há algumas ressalvas em que os agentes de tratamentos que causarem de danos aos titulares não responderão de acordo com os regramentos previstos na LGPD.

Primero, quanto às relações de consumo, o artigo 45 da LGPD dispõe que “as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente” (BRASIL, 2018).

---

[27] GUEDES, Gisela Sampaio da Cruz. Regime de responsabilidade adotada pela Lei de proteção de dados. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). Caderno Especial: Lei Geral de Proteção de Dados (PGPD). São Paulo: Revista dos Tribunais, 2019. Pág. 180.

Desse modo, no âmbito das relações de consumo, a responsabilidade dos agentes seguirá às regras do código de defesa do consumidor.

Segundo, nas relações mantidas com pessoas jurídicas de direito público e privadas prestadoras de serviços públicos, é defino que os agentes de tratamento responderão pelos danos que causarem ao titular de forma objetiva, sendo observado a possibilidade de ressarcimento se demonstrado o dolo ou culpa, conforme artigo 37, § 6º da CF.

Quanto as demais relações, a responsabilidade dos agentes de tratamento será estabelecida de acordo com os princípios e regras da LGPD, as quais estabelecem medidas e técnicas de segurança que os controlares e operadores devem adotar, sob pena de responsabilidade.

De acordo com o princípio da prestação de contas, os agentes devem demonstrar a “adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas” (artigo 6, inciso X, da LGPD).

Portanto, o controlador e operador devem demonstram que adotaram medidas eficazes para observância da lei e, inclusive, a eficácia que essas medidas resultaram, pois, caso contrário, o tratamento será tido como irregular e os agentes serão responsabilizados. Nesse sentido, o artigo 44 da LGPD, é expresso:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. (BRASIL, 2018).

Ademais, o artigo 43 da LGPD traz as hipóteses de excludentes da responsabilidade civil dos agentes no tratamento de dados:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (BRASIL, 2018).

A primeira das hipóteses consiste na exclusão de culpabilidade quando o agente não tiver realizado o tratamento de dados pessoais. Essa hipótese tratada pela lei seria abrangida nos casos em que há a negativa de autoria.

A segunda hipótese, mesmo que haja danos ao titular de dados, os agentes de tratamento não serão responsabilizados quando realizarem o tratamento de acordo os preceitos estabelecidos na norma, ou seja, que agiu de acordo com o exercício regular do direito.

E, por fim, quando o dano resultar em culpa exclusiva do titular de dados ou de terceiros. Por terceiros, entende-se por outras pessoas que não sejam o controlador ou operador e, por culpa exclusiva do titular, quando o dano decorre de ato exclusivo do titular.

Verifica-se, portanto, que a LGPD estipula aos agentes de tratamento a comprovação de que no decorrer do tratamento não foram violadas as leis de proteção de dados e que foram adotadas medidas eficazes para o cumprimento da norma, situações essas, se comprovadas, serão capazes de afastar eventuais responsabilização do controlador e operador.

7 CONSIDERAÇÕES FINAIS

Diante do desenvolvimento tecnológico e uso desenfreado de dados pessoais, a lei geral de proteção de dados tem como objetivo proteger e resguardar os direitos fundamentais de liberdade e de privacidade dos indivíduos.

Em que pese não ser uma lei constituída e voltada diretamente para as relações do trabalho, a lei tem como escopo a proteção da privacidade e intimidade dos indivíduos. Deste modo, diante do alcance do direito fundamental, a LGPD se mostra aplicável e prescindível no âmbito do contexto laboral.

As novas tecnologias permitem ao empregador o tratamento de informação pessoal dos trabalhadores para as mais variadas finalidades e a observância dos princípios e fundamentos da lei devem ser respeitados durante a fase pré-contratual, contratual e pós-contratual.

Destaca-se que a lei de proteção de dados visa garantir o empoderamento do titular em relação aos seus dados e o direito de autodeterminação informativa, regulamentando o legítimo interesse, sob pena de responsabilização pelo mau uso.

Na fase pré-contratual, as empresas deverão coletar os dados dos candidatos de forma objetiva, para fins específicos e por tempo determinando. Devem garantir que as informações coletadas na seleção não impliquem em discriminações em razão do gênero, da raça, da origem social. Desse modo, nessa fase, as empresas devem solicitar o mínimo de informações pessoais, além de obter o expresso consentimento expresso dos candidatos para o tratamento dos seus dados durante a seleção.

O período contratual é regido por uma imensa coleta de dados pessoais dos empregados, demandando maior atenção e responsabilidade do empregador no tocante à coleta, tratamento, compartilhamento e armazenamento. Nesse período, o empregador deve coletar somente os dados primordiais para execução do contrato, observando-se os princípios da finalidade, adequação e necessidade, além do

expresso consentimento do empregado nas hipóteses em que o tratamento não decorrer para cumprimento de obrigações legais.

Quanto ao período pós-contratual, os dados pessoais poderão ser armazenados para cumprimento de obrigações legais ou regulatórias, devendo-se observar os prazos prescricionais previstos em lei.

Portanto, é inegável que a proteção de dados pessoais abrange todo o contexto laboral e a observância da lei deve ser respeitada pelo empregador em todas essas fases, visando garantir a dignidade humana do trabalhador.

E nesse sentido, caberá à Autoridade Nacional disseminar o conhecimento sobre a proteção de dados e da privacidade à população, visando a natureza preventiva de eventuais falhas decorrentes do irregular tratamento de dados, além da efetiva fiscalização e penalização em casos de descumprimento da legislação.

8 REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Fabricio da Mota. Avaliação de impactos sobre a proteção de dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. Comentários ao GDPR. São Paulo: Thompson Reuters, 2018.

BIONI, Bruno. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: GEN/Forense, 2020.

CARLOTO, Selma. Lei Geral da Proteção de Dados: enfoque nas relações de trabalho. São Paulo: LTr, 2020.

CASTRO, Catarina Sarmento e Castro. Direito da informática, privacidade e dados pessoais. Coimbra: Almedina, 2005.

DONEDA, Danilo. Da privacidade à Proteção de Dados. Rio de Janeiro: Renovar, 2006.

GASPAR, Gabriela Curi Ramos. LGPD e o tratamento de dados sensíveis nas organizações de tendência. Artigo disponível em: MIZIARA, Raphael. Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Thomson Reuters/Revista dos Tribunais, 2020.

GUEDES, Gisela Sampaio da Cruz. Regime de responsabilidade adotado pela Lei de Proteção de Dados brasileira. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). Caderno Especial: Lei Geral de Proteção de Dados (PGPD). São Paulo: Revista dos Tribunais, 2019.

HIGUEIRAS. Manuel Heredero. La Directiva Comunitaria de Protección de los datos de Carácter Personal, Arrazandi Editorial, 1997.

SCHWAB, Klaus. A Quarta Revolução Industrial, Edipro, 1ª edição, 2016, São Paulo.

MALDONADO, Viviane Nóbrega e OPICE BLUM, Renato; coord. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019.

MIZIARA, Raphael. Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Thomson Reuters/Revista dos Tribunais, 2020.

RONY VAINZOF. LGPD: Lei Geral de Proteção de Dados Pessoais comentada. Viviane Nóbrega Maldonado e Renato Opice Blum, coordenadores. São Paulo: Thomson Reuters Brasil, 2019.

TEPEDINO, Gustavo; TERRA, Aline de Miranda; GUEDES, Gisela Sampaio. Fundamentos do Direito Civil. Volume 4. Editora Forense. 2020.

YOSHIDA, Victoria Melo. Autodeterminação informativa, riscos cibernéticos e proteção de dados pessoais: a emergência de um novo compliance. In Revista do curso de direito da Unifacs. Porto Alegre. Paixão Editores. V. 19, 2019.

SITES

BUTCHER, Isabel. Google: Conselho de Estado francês confirma multa de 50 milhões de euros. Disponível em: https://www.mobiletime.com.br/noticias/19/06/2020/google-conselho-de-estado-frances-confirma-multa-de-50-milhoes-de-euros/. Acesso em: 20 de fevereiro de 2021.

CALCINI, Ricardo Souza; MACHADO, Gustavo Carvalho. Efeitos da Lei Geral de Proteção de Dados nas relações de trabalho. Disponível em: https://www.irib.org.br/noticias/detalhes/artigo-efeitos-da-lei-geral-de-protecao-de-dados-nas-relacoes-de-trabalho-undefined-por-gustavo-carvalho-machado-e-ricardo-souza-calcini

Comité Europeu para a Proteção de Dados. Directiva 95/46/CE. Parecer 4/2007 sobre o conceito de dados pessoais no Grupo de Trabalho de proteção de Dados do Artigo 29º. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf

Comité Europeu para a Proteção de Dados. Directiva 95/46/CE. Parecer 13/2011 sobre serviços de geolocalização em dispositivos móveis inteligentes. Disponível em: https://www.gpdp.gov.mo/uploadfile/2014/0505/20140505071557367.pdf

ELLIS, Nick. Ferramentas de recrutamento da Amazon com AI discriminava candidatas mulheres. Disponível em: https://tecnoblog.net/meiobit/391571/ferramenta-de-recrutamento-amazon-ai-discriminava-mulheres/. Acesso em: 08 de janeiro de 2021.

FRAZÃO, Ana. Nova LGPD: as demais hipóteses de tratamento de dados pessoais. Disponível em: www.jota.info/opiniao-e-analise/artigos/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018. Acesso em 01 de abril de 2021
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf

MENÉDEZ, Uría. O impacto das novas tecnologias no direito do trabalho e a tutela dos direitos da personalidade do trabalhador. Disponível em: https://www.uria.com/documentos/publicaciones/2242/documento/068apa.pdf?id=1948. Acesso em: 03 de abril de 2021

Redação. Varejista H&M leva multa milionária por espionar funcionários na Alemanha Disponível em: https://vocesa.abril.com.br/mercado/varejista-hm-leva-multa-milionaria-por-espionar-funcionarios-na-alemanha/ Acesso em: 20 de fevereiro 2021

LEGISLAÇÃO

BRASIL. **Constituição da República Federativa do Brasil**. Texto constitucional promulgado em 5 de outubro de 1988, com as alterações determinadas pelas Emendas Constitucionais de Revisão 1 a 6/94, pelas Emendas Constitucionais 1/92 a 91/2016 e pelo Decreto Legislativo 186/2008. Brasília: Senado Federal, Coordenação de Edições Técnicas, 2016.
Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRASIL. **Decreto-Lei n. 5.452, de 1º de maio de 1943**. Aprova a Consolidação das Leis do Trabalho. Diário Oficial da União. 09 ago. 1943. Retificado pelo Decreto-Lei n. 6.353, de 1944 e retificado pelo Decreto-Lei n. 9.797, de 1946.
Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm

BRASIL. **Lei n. 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União. 12 set. 1990. Edição extra e retificado em 10 jan. 2007.
Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm

BRASIL. **Lei n. 9.029, de 13 de abril de 1995.** Proíbe a exigência de atestados de gravidez e esterilização, e outras práticas discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9029.htm

BRASIL. **Lei n. 13.105, de 16 de março de 2015.** Código de processo civil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 de março de 2021.

BRASIL. **Proposta de Emenda à Constituição n° 17, de 2019**. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594