UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE CIÊNCIAS JURÍDICAS

FACULDADE DE DIREITO DO RECIFE

MARIANA DE ARAÚJO MELO

BREVE ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E SEUS PRINCIPAIS IMPACTOS NAS RELAÇÕES DE TRABALHO

Recife

2023

MARIANA DE ARAÚJO MELO

BREVE ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E SEUS PRINCIPAIS IMPACTOS NAS RELAÇÕES DE TRABALHO

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, como requisito parcial para a obtenção do título de bacharel(a) em Direito.

Área de concentração: Direito do Trabalho.

Orientador(a): Sergio Torres Teixeira.

Recife

2023

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Melo, Mariana de Araújo .
Breve análise da Lei Geral de Proteção de Dados (LGPD) e seus principais impactos nas relações de trabalho / Mariana de Araújo Melo. - Recife, 2023.
48 p

Orientador(a): Sérgio Torres Teixeira
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, Direito - Bacharelado, 2023.

1. Lei Geral de Proteção de Dados (LGPD). 2. Dados pessoais . 3. Dados Pessoais Sensíveis. 4. Acesso à informação. 5. Direito à privacidade . I. Teixeira , Sérgio Torres. (Orientação). II. Título.

340 CDD (22.ed.)

MARIANA DE ARAÚJO MELO

BREVE ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E SEUS PRINCIPAIS IMPACTOS NAS RELAÇÕES DE TRABALHO

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, como requisito parcial para a obtenção do título de bacharel(a) em Direito.

Aprovado em: 11/09/2023.

BANCA EXAMINADORA

_____

Profº. Doutor Sérgio Torres Teixeira (Orientador)

Universidade Federal dePernambuco

_____

Profª. Mestra Camilla Montanha de Lima (Examinador Interno)

Universidade Federal de Pernambuco

_____

Daniel Rodrigues Corte Real (Examinador Externo)

Mestrando PPGD/Universidade de Lisboa

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, meu alicerce, presente em todas as etapas da minha vida.

Agradeço, também, a minha mãe, avô, tios, namorado e amigas por serem os maiores incentivadores dos meus sonhos, sempre acreditando em mim quando eu mesma não acreditava.

Sou grata ao Profº. Doutor Sérgio Torres Teixeira por prontamente aceitar ser meu orientador no início desse projeto, com compreensão, organização, disponibilidade e sábios conselhos que levarei para a vida.

Por fim, agradeço a todos os professores e funcionários da Faculdade de Direito do Recife.

RESUMO

O presente trabalho tem como objetivo a análise da aplicação da Lei Geral de Proteção de Dados (LGPD) como regulamentação para mitigar riscos relacionados ao tratamento indevido e abusivo de dados pessoais, garantindo ao cidadão o direito à privacidade. Tendo em vista o impacto da LGPD nos negócios de empresas brasileiras e estrangeiras que oferecem produtos ou serviços ao Brasil, o estudo aborda os princípios e fundamentos da LGPD, discute seus impactos nas relações de trabalho, as etapas de tratamento de dados e a efetiva aplicabilidade da Lei na seara trabalhista brasileira.

Palavras-chave: Lei Geral de Proteção de Dados (LGPD); Dados pessoais; Dados Pessoais Sensíveis; Acesso à Informação; Direito à Privacidade.

ABSTRACT

The present work aims to analyze the application of the General Data Protection Law (LGPD) as a regulation to mitigate risks related to improper and abusive treatment of personal data, guaranteeing citizens the right to privacy. Bearing in mind the impact of the LGPD on the business of Brazilian and foreign companies that offer products or services to Brazil, the study addresses the principles and fundamentals of the LGPD, discusses its impacts on labor relations, the stages of data processing and the effective applicability of the Law in the Brazilian labor field.

Keywords: General Data Protection Law (LGPD); Personal data; Sensitive Personal Data; Access to information; Right to Privacy.

SUMÁRIO

1 INTRODUÇÃO

O constante fluxo de informações e o avanço da tecnologia da informação têm gerado preocupações significativas sobre a proteção dos dados pessoais dos cidadãos. Isto posto, diante do intenso compartilhamento de informações via internet, é crucial discutir a privacidade de dados, visto que o uso inadequado dessas informações pode levar a danos físicos, materiais ou imateriais para os indivíduos.

Neste cenário, o uso inapropriado de dados pessoais pode resultar em danos físicos, como o risco de assaltos ou invasões de domicílio, e danos materiais, como fraudes financeiras e roubo de identidade. No aspecto imaterial, os indivíduos podem sofrer com a perda de controle sobre suas informações, o que pode levar à manipulação de suas percepções e à limitação de seus direitos, como o direito à liberdade de expressão e à privacidade.

Ademais, a coleta e uso de dados por meio de cookies, por exemplo, têm sido uma questão preocupante. Essas ferramentas rastreiam a navegação e pesquisas dos usuários, permitindo a segmentação e direcionamento de anúncios de marketing e publicidade. Isso resulta em uma vigilância constante do usuário, com suas informações pessoais sendo coletadas e usadas para fins comerciais sem que ele tenha total conhecimento disso. Diante dessa situação, a ausência de regulamentação pode levar à invasão da privacidade dos indivíduos e à violação de direitos relacionados aos seus dados pessoais. Assim, é fundamental pensar na segurança e no resguardo dos dados pessoais para preservar a privacidade e evitar potenciais violações e abusos.

Importa salientar que a proteção de dados pessoais é considerada um direito fundamental do ser humano, e, portanto, é crucial que a legislação e a tutela estejam em constante atualização e aperfeiçoamento para acompanhar o desenvolvimento tecnológico e informacional. Para lidar com essa questão, a existência de legislações específicas que tratem da proteção de dados é essencial, dado o valor estratégico que a informação possui no mercado atual.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018, desempenha um papel importante no contexto social brasileiro.

Essa lei tem como objetivo fazer com que empresas e o Poder Público se adequem às políticas de tratamento e compartilhamento de dados, protegendo, assim, a privacidade dos cidadãos. Por ser uma lei relativamente nova, é fundamental que alguns aspectos sejam estudados com profundidade para garantir sua efetividade e aplicação adequada.

Ainda, importa salientar que muitas pessoas não têm plena consciência dos riscos associados à exposição de informações pessoais nas redes sociais, sendo papel da sociedade, das empresas e das autoridades conscientizarem tais cidadãos sobre a importância da proteção de dados e da privacidade online.

Nesse sentido, a legislação desempenha um papel crucial para garantir a proteção dos dados pessoais dos cidadãos, sendo fundamental que os indivíduos conheçam seus direitos e saibam como exercê-los, e que as empresas e organizações respeitem essas normas para evitar abusos e garantir a privacidade dos usuários.

As normas gerais contidas na LGPD são de interesse nacional, devendo ser observadas pela União, Estados, Distrito Federal e Municípios, prezando-se, assim, pela aplicação da Lei de maneira harmônica em todos os entes da federação brasileira.

Em suma, a discussão sobre a privacidade de dados é de extrema importância no ambiente de alta tecnologia da informação e do compartilhamento constante de informações via internet. A proteção de dados pessoais é um direito fundamental dos indivíduos, e a legislação deve acompanhar as evoluções tecnológicas para garantir a segurança e a privacidade dos cidadãos no mundo digital. Assim, a Lei Geral de Proteção de Dados é uma peça fundamental nesse contexto, mas é essencial que haja uma constante reflexão e aprimoramento das abordagens para enfrentar os desafios e ameaças à proteção de dados, além de entender como a legislação aborda as soluções para este óbice.

As fontes bibliográficas serão a coleta em legislação, livros, artigos e revistas jurídicas, com o estudo do tema de forma mais elucidativa. O trabalho divide-se em cinco capítulos. O primeiro capítulo é a introdução, que traz uma breve análise do tema, atrelada à importância de sua tratativa. O segundo capítulo tratará sobre o avanço tecnológico dos meios de comunicação na era da Globalização, atrelado ao

surgimento das redes sociais e construção de novas identidades pessoais, além de citar os princípios e principais fundamentos da Lei Geral de Proteção de Dados.

O terceiro capítulo abordará como é, efetivamente, aplicada a Lei Geral de Proteção de Dados nas operações de tratamento realizadas por pessoa natural ou por pessoa jurídica de direito público ou privado, dentro do país de sua sede ou do país onde estejam localizados os dados, além de trazer as hipóteses de tratativa dos dados pessoais, dos dados pessoais sensíveis, dos dados anonimizados e dos dados pessoais de crianças e adolescentes.

O quarto capítulo tratará da efetiva proteção a tais dados pessoais pelo Poder Público, a responsabilidade e segurança no sigilo de dados e as devidas formas de fiscalização e sanções administrativas pelo incorreta divulgação e mau uso de tais dados pessoais.

Por fim, o quinto e último capítulo traz, como abordagem, os impactos da Lei Geral de Proteção de Dados nas relações trabalhistas, com o enquadramento de tais proteções abarcadas pela LGPD nas relações de trabalho.

2 A GLOBALIZAÇÃO E PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

2.1 A Construção da Identidade na era da Globalização face o tratamento dos dados pessoais no mundo globalizado

Para Manuel Castells “A construção da identidade vale-se da matéria-prima fornecida pela história, geografia, biologia, por instituições produtivas e reprodutivas, pela memória coletiva e por fantasias pessoais, pelos aparatos de poder e revelações de cunho religioso.” (CASTELLS, 2018).

Dito isto, parte da identidade do indivíduo é captada em face do meio em que ele se encontra, com a Internet sendo vista como a maior revolução da comunicação e conectividade da história da humanidade. Isto posto, se, antes, os indivíduos eram moldados por uma comunidade fechada e historicamente limitada, com o contato com outras comunidades sendo visto como algo injustificado e, muitas vezes, hostil, com o salto temporal atual a tecnologia da comunicação revolucionou o modo de interação dos indivíduos com a comunidade que eles nasceram, ainda mais se pensarmos no quão jovens as pessoas são introduzidas nestas tecnologias.

Ademais, o avanço tecnológico tem sido rápido e abrangente, tornando dispositivos como telefones celulares e computadores pessoais mais acessíveis e integrados à vida das pessoas. A internet também se popularizou e se tornou essencial em diversas atividades cotidianas, como aprendizado, lazer e comércio. Cada vez mais as interações sociais, negócios e registros são realizados digitalmente, tornando a tecnologia uma parte integral de nossas vidas.

Isto posto, com o aumento de internautas e o surgimento das redes sociais, a construção das identidades passou a ser influenciada por um mundo cada vez mais interconectado, resultando em uma nova dimensão de existência, a existência virtual. Assim, as redes sociais e a interação online têm impacto significativo na maneira como as pessoas constroem e expressam suas identidades no ambiente digital.

Por isso, se pode afirmar que a identidade é formada pelas percepções que o indivíduo tem sobre si mesmo, baseadas em suas características biológicas e sociais. Nesse contexto, os dados pessoais tornam-se o componente essencial para a identificação do indivíduo, tanto para si mesmo quanto para terceiros.

Ademais, conforme já salientado, a proteção dos dados pessoais está intrinsecamente relacionada ao direito à privacidade, que é um direito fundamental assegurado em diversos ordenamentos jurídicos, incluindo a Constituição da República Federativa do Brasil, de 1988. Contudo, diante da abrangência do domínio sobre os dados das pessoas, a partir da criação e produção em massa de informações nas redes de computadores, surge uma preocupação acerca de como esses dados são utilizados.

Sendo assim, importa salientar que, no ordenamento jurídico brasileiro, o direito à privacidade é assegurado pelo artigo 5°, inciso X, da Constituição Federal, e pelo artigo 21 do Código Civil, garantindo a proteção do âmbito privado do cidadão, seja em sua vida pública ou particular.

Ocorre que o grande avanço da era tecnológica, de acordo com Carvalho e Pedrini (2019), trouxe mudanças significativas na sociedade em razão das constantes modernizações trazidas pelo momento tecnológico vivenciado. Assim, os celulares, notebook, computadores, dentre tantos outros objetos eletrônicos com acesso à internet, possibilitam o processamento, armazenamento e compartilhamento em massa de informações, chegando a um número inimaginável de pessoas, e, em alguns casos, até de forma criptografada.

Com isso, constata-se que os avanços tecnológicos permitem a formação e disseminação de conhecimento em uma escala sem precedentes. A internet e seus produtos possibilitam a superação de obstáculos de tempo e espaço, alcançando imediatamente um grande número de usuários, facilitando a propagação de informações de forma rápida e abrangente. Neste sentido, Silva e Silva constatam que:

> O crescente uso das tecnologias da informação e da comunicação, em especial da Internet, imprimiu maior dinamicidade às relações econômicas, à participação política e às interações sociais, redesenhando as formas de ser e estar no mundo. Em nenhum outro momento histórico foi tão fácil e rápido acessar informações, produzir e compartilhar conteúdos, comunicar e interagir em sites de redes sociais, blogs e microblogs, tudo de maneira instantânea. O intenso desenvolvimento capitaneado pelo segmento de Tecnologias da Informação (TI) acelera ainda mais esse processo, pois a cada dia são lançados no mercado novos equipamentos, aplicativos, plataformas e ferramentas que maximizam a experiência de navegação na web, o que faz com que um número crescente de pessoas almeje a inclusão digital (2013, p. 2)

Isto posto, Carvalho e Pedrini (2019) chegam à conclusão de que o usuário da internet não é somente destinatário da informação, mas também veiculador da mesma. Entretanto, o ambiente digital, que possibilita a expressão democrática de opiniões, também é palco de violações aos direitos constitucionais, especialmente no que se refere à privacidade. A Constituição Federal, no art. 5°, inciso X, assegura o direito à intimidade, vida privada, honra e imagem das pessoas como invioláveis, garantindo o direito à indenização por danos morais ou materiais decorrentes de violações. A proteção desses direitos constitucionais é essencial no contexto digital para resguardar a privacidade dos indivíduos e prevenir possíveis danos.

Em contrapartida, a proteção dos dados pessoais tem sua origem no direito à privacidade, resultado da sociedade da informação. Diante do domínio abrangente sobre os dados das pessoas, surge a preocupação sobre o uso adequado dessas informações.

No Brasil, o direito à privacidade foi progressivamente positivado, com leis como o Código de Defesa do Consumidor em 1990 e o Marco Civil da Internet em 2014. Ainda, para preencher lacunas decorrentes da globalização contemporânea, foi criada a Lei Geral de Proteção de Dados (Lei n° 13.709/2018), inspirada nas normas europeias, que entrou em vigor em 2020, trazendo proteção especial aos dados pessoais e às informações que identificam ou tornam reconhecível a pessoa natural e visando garantir a segurança e privacidade das informações dos cidadãos.

2.2 A Lei Geral de Proteção de Dados e seus principais aspectos

Segundo Pinheiro (2018), a nova Lei Geral de Proteção de Dados – LGPD vem como uma garantia à liberdade de expressão, à segurança e à dignidade dos seres humanos. Vejamos:

> Destaque-se que a proteção das pessoas físicas relativamente ao tratamento dos seus dados pessoais é um direito fundamental, garantido por diversas legislações em muitos países. Na Europa, já estava previsto na Carta dos Direitos Fundamentais da União Europeia e no Tratado sobre o Funcionamento da União Europeia; no Brasil, já tinha previsão no Marco Civil da Internet e na Lei do Cadastro Positivo, mas a questão ainda era, muitas vezes, observada de forma difusa e sem objetividade no tocante aos critérios que serão considerados adequados para determinar se houve ou não guarda, manuseio e descarte dentro dos padrões mínimos de segurança condizentes (PINHEIRO, 2018, p. 18).

Ou seja, a Lei Geral de Proteção de Dados (LGPD) terá amplos efeitos no âmbito do direito digital. Essa legislação não se limita apenas às redes sociais, mas abrange qualquer empresa ou organização que colete e armazene dados de seus clientes em seus bancos de informações. É oportuno atentar para o que diz o artigo 1° da Lei Geral de Proteção de Dados:

> 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).

O artigo 2º da LGPD também traz alguns fundamentos que disciplinam a proteção de dados pessoais, conforme abaixo exemplificado:

> Art. 2º A disciplina da proteção de dados pessoais 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).

Nesse ínterim, a Lei Geral de Proteção de Dados (LGPD) busca regularizar a questão dos dados pessoais e sua administração por meio de diversos dispositivos jurídicos. O objetivo central é garantir o respeito aos direitos individuais, tratando os dados de forma transparente e responsável, protegendo a privacidade dos cidadãos e estabelecendo diretrizes para o tratamento adequado e seguro dos dados pessoais, assegurando a transparência e a responsabilidade no uso de tais informações.

Entretanto, importa salientar que a Lei Geral de Proteção de Dados (LGPD) não se restringe, apenas, ao meio virtual, mas a todos os meios em que se pode coletar e utilizar dados pessoais de maneira facilitada, sendo certo de que é no meio virtual onde se encontram os maiores desafios de proteção a tais dados.

Neste ínterim, em seu artigo 23, a LGPD, também, autoriza que os órgãos e entidades da administração pública realizem o tratamento dos dados pessoais unicamente com a finalidade de persecução do interesse público, e desde que tais hipóteses de levantamento de dados seja devidamente informada ao usuário, além do dever de indicar um encarregado que realize as operações de tratamento de tais

dados pessoais (BRASIL, 2018).

Ainda, se levarmos em consideração os requisitos para o tratamento de dados pessoais, o artigo 7º da Lei nº 13.709/2018 argumenta que o tratamento de tais dados somente poderá ser realizado nas seguintes hipóteses: mediante o fornecimento de consentimento pelo titular; ou para o cumprimento de obrigação legal ou regulatória pelo controlador; ou então pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; para a proteção da vida ou da incolumidade física do titular ou de terceiros; para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2018).

2.3 Princípios e Fundamentos da Lei Geral de Proteção de Dados

Nos termos do art. 5º, X, da Constituição Federal de 1988, “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

Conforme já exposto anteriormente, ante artigo 2º da Lei Geral de Proteção de Dados (LGPD), a proteção dos dados pessoais tem como fundamentos: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre

desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Ainda, de acordo com o artigo 6º da LGPD, os princípios que deverão ser observados na tratativa de tais dados pessoais são os seguintes: Princípio da Finalidade; Princípio da Adequação; Princípio da Necessidade; Princípio do Livre Acesso; Princípio da Qualidade de Dados; Princípio da Transparência; Princípio da Segurança; Princípio da Prevenção; Princípio da Não Discriminação; e Princípio da Responsabilização e Prestação de Contas. Vejamos cada um detalhadamente (BRASIL, 2018).

De início, importa salientar que o Princípio da Finalidade, previsto no inciso I do artigo 6ª da Lei Geral de Proteção de Dados, prevê que a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018). Ou seja, na hora da coleta, os dados deverão ter indicação clara e completa, devidamente fundamentada, ante a realização do tratamento para propósitos legítimos, explícitos, específicos, e sem possibilidade de futuro tratamento incompatível com tal finalidade. Ademais, por meio de tal princípio, chega-se à conclusão de que é garantido ao titular a devida legalidade no tratamento de seus dados, utilizando-os de maneira lícita.

O Princípio da Adequação, previsto no inciso II do artigo 6ª da Lei Geral de Proteção de Dados, prevê a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (BRASIL, 2018). Dito isto, os dados devem ser devidamente tratados de acordo com a sua destinação, com tais coletas de dados devendo ser compatíveis com a atividade fim almejada.

Em contrapartida, o Princípio da Finalidade, previsto no inciso III do artigo 6ª da Lei Geral de Proteção de Dados, prevê 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" (BRASIL, 2018). Ou seja, a coleta dos dados pessoais deve ocorrer de forma cuidadosa e restritiva à finalidade pretendida.

Ainda, conforme Zeferino:

> O princípio visa fazer com que a coleta de dados pessoais seja restrita ao que realmente é necessário para a realização da finalidade pretendida. Isso faz com que dados pessoais não pertinentes à ocasião de tratamento sejam mantidos fora do processo, de certa forma, zelando pelo sigilo dessas informações. Ou seja, dados pessoais que não são necessários não serão coletados, fazendo com que o indivíduo não seja exposto sem necessidade. Dessa forma, a coleta de dados pessoais se torna restritiva. Por exemplo, podemos citar o caso de exigir dados como laudos e diagnósticos cardíacos de um candidato à vaga administrativa. Não há necessidade disso, visto que um profissional da área administrativa não trabalha realizando esforços físicos. Assim sendo, o princípio da necessidade LGPD funciona como uma diretriz da legislação, garantindo que somente dados pessoais pertinentes sejam coletados. Para empresas que trabalham realizando coletas de dados pessoais, como o caso de consultorias em RH, agências de créditos, entre outras, pode parecer inicialmente que trabalhar respeitando o princípio da necessidade seja um fator dificultante. Entretanto, uma coleta mais efetiva de dados pessoais, se adequando à estrita necessidade, poderá fazer com que a empresa trabalhe de forma rápida e direta em seus cadastros. Isso porque não se perderá tempo e memória arquivando dados desnecessários. (ZEFERINO, 2020).

Nao obstante, o Princípio do Livre Acesso, previsto no inciso IV do artigo 6ª da Lei Geral de Proteção de Dados, prevê a “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” (BRASIL, 2018). Ou seja, o titular tem o direito de controlar o uso de seus próprios dados pessoais, garantindo-se a ele o livre acesso aos mesmos de forma facilitada, transparente e gratuita.

Previsto no inciso V do artigo 6ª da Lei Geral de Proteção de Dados, o Princípio da Qualidade de Dados prevê a “garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento” (BRASIL, 2018), sendo indispensável, por isso, que o cidadão mantenha constantemente atualizada suas informações nos sistemas de tecnologia da informação das empresas.

Afirma o inciso VI do artigo 6ª da Lei Geral de Proteção de Dados, que exemplifica o Princípio da Transparência, que deverá se observar a “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” (BRASIL, 2018). Ou seja, o legislador, com tal princípio, buscou garantir a não utilização dos dados pessoais com finalidades negativas.

Previsto no inciso VII do artigo 6ª da Lei Geral de Proteção de Dados, o Princípio da Segurança afirma que se deve garantir 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" (BRASIL, 2018). Neste ínterim, os sistemas de informação devem garantir, por meio de medidas técnicas e administrativas, a proteção a eventuais violações dos dados pessoais dos cidadãos.

O Princípio da Prevenção, previsto no inciso VIII do artigo 6ª da Lei Geral de Proteção de Dados, prevê a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (BRASIL, 2018). Na prática, tal inciso visa garantir que os dados pessoais sejam coletados de forma mais segura e cautelosa, sem a formação de posterior prejuízo ao indivíduo.

Previsto no inciso IX do artigo 6ª da Lei Geral de Proteção de Dados, o Princípio da Não Discriminação prevê a "não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (BRASIL, 2018). Tal princípio em destaque proíbe o tratamento discriminatório de dados quando realizado de forma ilícita ou abusiva. Isso significa que a discriminação no tratamento de dados, mesmo que sejam informações sensíveis, é vedada, desde que não esteja em conformidade com as bases legais estabelecidas. Em outras palavras, a manipulação de dados deve ser realizada de maneira justa e legal, evitando qualquer forma de discriminação.

Por fim, o Princípio da Responsabilização e Prestação de Contas, previsto no inciso X do artigo 6ª da Lei Geral de Proteção de Dados, prevê a "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). Isto posto, os responsáveis pelo tratamento de dados devem constantemente analisar a conformidade legal e aplicar medidas de proteção aos dados pessoais em todas as etapas do processo. Eles devem avaliar os riscos envolvidos e tomar decisões ponderadas para garantir a segurança e o cumprimento das regulamentações ao longo de todo o ciclo de vida dos dados sob sua responsabilidade.

3 A EFETIVA APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

3.1 A lei Geral de Proteção de Dados: conceitos e aplicabilidade

Conforme exposto no art. 3º da LGPD, os fundamentos da Lei Geral de Proteção de Dados são aplicados a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que (BRASIL, 2018):

> **I - a operação de tratamento seja realizada no território nacional (BRASIL, 2018);**

Excetuando-se, por isso, deste inciso I, o tratamento de dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o dê proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na Lei nº 13.709/2018.

> **II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (BRASIL, 2018)**
> **III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional (BRASIL, 2018).**

Já o artigo 4º da Lei 13.709/2018 informa que a mesma não se aplica ao tratamento de dados pessoais:

> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (BRASIL, 2018).

Neste ponto, importa esclarecer os conceitos de pessoas físicas e jurídicas

previstos no ordenamento jurídico brasileiro. As pessoas jurídicas encontram-se regulamentadas nos artigos 40 a 52 do Código Civil de 2002. Assim, pessoas físicas e jurídicas possuem direitos e obrigações previstos no ordenamento jurídico, e, quanto as pessoas jurídicas, a legislação, ainda, estabelece os diferentes tipos e formas de constituição.

Ademais, o artigo 5º da Lei Geral de Proteção de Dados traz alguns conceitos importantes para o entendimento da matéria relativa à proteção de dados, com o inciso I definindo como dados pessoais todas as informações relacionadas a pessoa natural identificada ou identificável; o inciso II afirmando que dado pessoal sensível é o 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; o inciso III trazendo o conceito de dado anonimizado como dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, e o inciso IV definindo banco de dados como conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico (BRASIL, 2018).

Alem disso, face artigo 5º da Lei Geral de Proteção de Dados, titular é pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (inciso V), sendo o controlador pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (inciso VI); o operador pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (inciso VII); o 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), face inciso VIII; e o agente de tratamento, no inciso IX, o controlador e o operador (BRASIL, 2018).

O inciso X, do artigo 5º da LGPD traz o conceito de tratamento como “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”, com a

anonimização sendo a 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 (inciso XI); o consentimento sendo a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais (inciso XII); o bloqueio se caracterizando como a suspensão temporária da operação de tratamento mediante guarda de dado pessoal ou de banco de dados (inciso XIII); e a eliminação caracterizando-se como a exclusão de dados ou de conjunto de dados armazenados em bancos de dados (inciso XIV) (BRASIL, 2018).

Por fim, o artigo 5º da Lei Geral de Proteção de Dados, ainda, define a transferência internacional de dados como o deslocamento de dados pessoais para países estrangeiros ou organismos internacionais (inciso XV); com o uso compartilhado de dados exemplificado no inciso XVI sendo definido como a própria 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; além do relatório de impacto à proteção de dados pessoais ser caracterizado, no inciso XVII, como a 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. Isto posto, o inciso XVIII argumenta que órgão de pesquisa é a 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 o objetivo de pesquisa em caráter histórico, cientifico, estatístico, ou, até mesmo, tecnológico, sendo a autoridade nacional o órgão da administração pública responsável por zelar pelo cumprimento da Lei 13.709/2018 em todo o território nacional (BRASIL, 2018).

3.2 Tratamento dos dados pessoais

Conforme artigo 7º da Lei Geral de Proteção de Dados, o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular (BRASIL,

> **2018);**

Neste caso, o controlador que obteve o consentimento do titular, caso necessite compartilhar tais dados pessoais com outros controladores, deverá, primeiramente, obter o consentimento específico do titular visando este fim, ressalvadas as hipóteses previstas de dispensa do consentimento.

Tal pedido de consentimento deve ser de forma inteligível e de fácil acesso, e o consentimento deve ser claro, objetivo e distinguível de outros assuntos.

> **II - para o cumprimento de obrigação legal ou regulatória pelo controlador (BRASIL, 2018);**

Diante de tal hipótese, o cumprimento de uma obrigação legal ou regulatória consiste no controlador poder tratar dados pessoais, mesmo sem o consentimento de seu titular, quando tiver que cumprir alguma determinação legal ou regulamentação.

> **III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei (BRASIL, 2018);**

Tal inciso III traz a possibilidade de a Administração Pública fazer o tratamento de dados pessoais, desde que delimitada a utilização dos mesmos para a consecução de políticas públicas previstas em lei ou regulamentos.

> **IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (BRASIL, 2018);**

Conforme inciso IV, uma empresa poderá se utilizar do tratamento de dados pessoais de seus clientes, por exemplo, para consultar o CEP do mesmo visando o cálculo do frete a ser utilizado.

> **V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;**
> **VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;**
> **VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro (BRASIL, 2018)**

Tal inciso VII flexibiliza o princípio da privacidade face ao princípio da preservação da vida.

> **VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (BRASIL, 2018);**

Tal inciso VIII é utilizado em situações específicas de tutela de saúde ou titular de dados.

> **IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou**
> **X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2018)**

3.3 Consentimento e acesso aos dados pelo titular

Conforme artigo 8º da Lei Geral de Proteção de Dados, o fornecimento de consentimento pelo titular deverá ser viabilizado por escrito ou por outro meio que demonstre a manifestação de vontade do titular (BRASIL, 2018).

Todavia, de acordo com o § 1º, se o consentimento for fornecido por escrito, deverá constar de cláusula destacada das demais cláusulas contratuais. Além disso, conforme o § 2º, cabe ao controlador o ônus de provar que tal consentimento fora obtido em conformidade com as disposições da LGPD (BRASIL, 2018).

O tratamento de dados pessoais mediante vício de consentimento é vedado, conforme § 3º, com o consentimento devendo se referir a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais deverão ser vistas como nulas (§ 4º) (BRASIL, 2018).

O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação (§ 5º) (BRASIL, 2018).

Ainda, conforme § 6º, em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração (BRASIL, 2018).

Ademais, nos termos do artigo 9º da LGPD, o titular tem direito ao acesso

facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso (BRASIL, 2018):

> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei (BRASIL, 2018).

Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca (art. 9º, § 1º) (BRASIL, 2018).

Entretanto, na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações (art. 9º, § 2º) (BRASIL, 2018).

Ainda, de acordo com o § 3º, do artigo 9º da LGPD, quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei (BRASIL, 2018).

3.4 Interesse legítimo e tratamento dos dados pessoais sensíveis

O legítimo interesse do controlador, previsto no art. 10 da Lei Geral de Proteção de Dados, somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a (BRASIL, 2018):

> 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).

Isto posto, conforme § 1º do artigo 10, quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. Ainda, o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse, e a autoridade nacional poderá, ainda, solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (BRASIL, 2018).

Com isso, temos que a Lei Geral de Proteção de Dados (LGPD) introduziu o conceito de "legítimo interesse" como uma opção para o tratamento de dados no Brasil, com o intuito de equilibrar a necessidade de utilizar informações para fins comerciais e tecnológicos com a importância de respeitar a privacidade dos indivíduos.

Em contrapartida, conforme artigo 11 da Lei Geral de Proteção de Dados, o tratamento de dados pessoais somente poderá ocorrer nas seguintes hipóteses:

> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BRASIL, 2018)

Ou seja, aplicam-se as regras acima mencionadas a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica (artigo 11, § 1º) (BRASIL, 2018).

Ainda, nos casos de aplicação do disposto nas alíneas “a” e “b”, pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da LGPD, conforme inciso II, do artigo 11 da LGPD (BRASIL, 2018).

Isto posto, afirma o § 4º do artigo 11 da LGPD que é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir a portabilidade de dados quando solicitada pelo titular (inciso I) ou as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata tal § 5º, conforme inciso II do mesmo (BRASIL, 2018).

3.5 Tratamento dos dados anonimizados e dos dados pessoais de crianças e adolescentes

Conforme aponta o artigo 12º da LGPD, os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido (BRASIL, 2018).

Ainda, o § 1º deste artigo afirma que a determinação do que é ou não razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios (BRASIL, 2018).

Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (§ 2º), com a autoridade nacional podendo dispor sobre

padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais (§ 3º) (BRASIL, 2018).

Em relação ao tratamento dos dados pessoais de crianças e adolescentes, como é sabido, há, no Brasil, diversos dispositivos que protegem as crianças e os adolescentes, como, por exemplo, a própria Constituição Federal de 1988 e o Estatuto da Criança e do Adolescente. Isto posto, a LGPD, em seu artigo 14, também trouxe uma regulamentação referente ao correto tratamento dos dados pessoais nessa faixa etária, buscando, sempre, o melhor interesse de tais menores de idade (BRASIL, 2018).

Assim, conforme § 1º, o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Ainda, poderão ser coletados dados pessoais de crianças sem o consentimento de um dos seus pais quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento do responsável pela criança (§ 3º) (BRASIL, 2018).

Os controladores não deverão condicionar a participação de crianças e adolescentes em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade (§ 4º), com tal controlador, ainda, devendo realizar todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis (§ 5º) (BRASIL, 2018).

Por fim, conforme § 6º do artigo 14, as informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (BRASIL, 2018).

3.6 Término do tratamento de dados

O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses, conforme artigo 15 da Lei Geral de Proteção de Dados:

> 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)

Já nos termos do art. 16 da LGPD, 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).

4 A PROTEÇÃO AOS DADOS PESSOAIS NA LEI GERAL DE PROTEÇÃO DE DADOS

4.1 Os direitos dos titulares dos dados pessoais

Nos termos do art. 17 da LGPD, toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade (BRASIL, 2018). Ou seja, independente do local em que se encontram os dados e da forma que seu tratamento é realizado, a pessoa natural é titular de suas informações, visto o direito de personalidade incidente.

Isto posto, o artigo 18 da Lei Geral de Proteção de Dados, ainda, afirma 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 (BRASIL, 2018):

> 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, 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)

Ainda, conforme § 1º do artigo 18 da LGPD, o titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional, com tal titular podendo se opor ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD (§ 2º, artigo 18) (BRASIL, 2018).

Tais direitos expostos no artigo 18 da LGPD serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento (§ 3º, artigo 18) (BRASIL, 2018).

Ainda, em caso de impossibilidade adoção imediata da providência de que trata

o § 3º do art. 18 da LGPD, o controlador enviará ao titular resposta em que poderá (§ 4º, artigo 18):

> I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
> II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência (BRASIL, 2018).

O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional (§ 6º, artigo 18) (BRASIL, 2018).

Ademais, conforme artigo 19 da LGPD, a confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular (BRASIL, 2018):

> I - em formato simplificado, imediatamente; ou
> II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular (BRASIL, 2018)

Conforme § 3º do artigo 19 da LGPD, quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento (BRASIL, 2018).

A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do artigo 19 da LGPD para os setores específicos (BRASIL, 2018).

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, conforme artigo 20 da LGPD. Ainda, o § 1º do artigo 20 afirma que o controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos

comercial e industrial (BRASIL, 2018).

Assim, em caso de não oferecimento de informações de que trata o § 1º do art. 20 da LGPD baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais (BRASIL, 2018).

Por fim, o artigo 21 da LGPD afirma que os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo. E, nos termos do artigo 22 da mesma Lei, a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva (BRASIL, 2018).

4.2 O tratamento dos dados pessoais pelo Poder Público

O artigo 23 da LGPD argumenta que o tratamento dos dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei (BRASIL, 2018);

Conforme § 1º do artigo 23, a autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento. Entretanto, o disposto nesta LGPD não dispensa as pessoas jurídicas mencionadas no caput do art. 23 de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) (§ 2º, artigo 23) (BRASIL, 2018).

O § 3º informa que os prazos e procedimentos para exercício dos direitos do

titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), com os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta LGPD (§ 4º) (BRASIL, 2018).

Ainda, importa salientar que os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo, com o artigo 24 da LGPD trazendo a ideia de que as empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares.

Ainda, os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral (artigo 25), e, conforme o artigo 26, o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da LGPD (BRASIL, 2018).

Neste ponto, importa, também, salientar que a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto (BRASIL, 2018):

> I - nas hipóteses de dispensa de consentimento previstas nesta Lei;
> II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou
> III - nas exceções constantes do § 1º do art. 26 desta Lei.
> Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação (BRASIL, 2018).

Por fim, importa ressaltar que a autoridade nacional, conforme já exemplificado,

poderá solicitar, a qualquer momento, que os órgãos e entidades do Poder Público realizem operações de tratamento de dados pessoais, buscando informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento da LGPD, ao estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais (artigos 29 e 30) (BRASIL, 2018).

4.3 A responsabilidade e segurança do sigilo de dados

Neste ponto, importa salinetar que, quando houver infração à Lei Geral de Proteção de Dados em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação (artigo 31 da LGPD), com tal autoridade nacional, ainda, podendo solicitar a 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 (artigo 32 da LGPD) (BRASIL, 2018).

Outrossim, conforme artigo 46 da LGPD, os agentes de tratamento de dados devem adotar todas as medidas de segurança capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Ainda, ante § 1º, a autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei, com tais medidas devendo ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (§ 2º) (BRASIL, 2018).

Ainda, face artigo 47 da LGPD, os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento, está obrigada a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término, e o controlador deverá comunicar à autoridade nacional e ao

titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (artigo 48), com a comunicação devendo ser feita em prazo razoável e conforme definido pela autoridade nacional, devendo, no mínimo, informar (§ 1º, artigo 48) (BRASIL, 2018):

> I - a descrição da natureza dos dados pessoais afetados;
> II - as informações sobre os titulares envolvidos;
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - os riscos relacionados ao incidente;
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (BRASIL, 2018).

Imprescindível salientar que a autoridade nacional verificará a gravidade do incidente, podendo determinar ao controlador a adoção das seguintes providências (§ 2º, artigo 48):

> I - ampla divulgação do fato em meios de comunicação; e
> II - medidas para reverter ou mitigar os efeitos do incidente (BRASIL, 2018).

Ainda, conforme § 3º do artigo 48 da LGPD, em caso de eventual juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los (BRASIL, 2018).

Sendo assim, conclui-se que os sistemas utilizados para o tratamento de dados pessoais devem ser devidamente estruturados, objetivando-se o atendimento dos requisitos de segurança, padrões de boas práticas e de governança, conforme artigo 49 da LGPD (BRASIL, 2018).

4.4 Da fiscalização e das sanções administrativas

Conforme previsão do artigo 52 da Lei Geral de Proteção de Dados, os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas em tal Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional (BRASIL, 2018):

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) 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$ 50.000.000,00 (cinquenta milhões de reais) 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 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019) (BRASIL, 2018)

Por isso, necessário observar, conforma § 1º do artigo 52 da LGPD, que as sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção (BRASIL, 2018).

Por conseguinte, a autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações à LGPD, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa (artigo 53, LGPD), face o fato de que, conforme § 1º, as metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias

para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei; além do regulamento de sanções e metodologias correspondentes estabelecer as devidas circunstâncias e/ou condições para a adoção de multa simples ou diária (§ 2º) (BRASIL, 2018).

Por fim, o artigo 54 da LGPD informa que o valor da sanção de multa diária aplicável às infrações a tal Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado, além de ser fundamentado pela autoridade nacional. Também, a intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento (BRASIL, 2018).

5 COMO A LEI GERAL DE PROTEÇÃO DE DADOS PODE IMPACTAR NAS RELAÇÕES TRABALHISTAS?

5.1 A Lei Geral de Proteção de Dados e seus principais impactos nas relações de trabalho

Conforme Pallotta e Moraes (2021), os dados pessoais dos cidadãos passam por um grande fluxo de tratamento ao longo da jornada de trabalho dos mesmos, podendo tais momentos serem divididos em quatro fases: fase anterior à celebração do contrato de trabalho; fase de celebração do contrato de trabalho; fase de execução do contrato de trabalho e fase do término do contrato de trabalho.

Portanto, nas relações de trabalho, ocorre um fluxo intenso de informações e dados pessoais, tanto entre empregadores e empregados como também no âmbito dos órgãos de controle interno das empresas e do governo. Esses dados são utilizados em várias situações, como para fins de fiscalização e outros procedimentos administrativos, incluindo convênios médicos, planos de saúde, vale-refeição, E-Social, consultorias contratadas, Serviços Especializados em Engenharia de Segurança e em Medicina do Trabalho (SESMT), Instituto Nacional do Seguro Social (INSS), Fundo de Garantia do Tempo de Serviço (FGTS), dentre outros. É importante ressaltar que o tratamento desses dados requer o cumprimento das leis de proteção de dados, visando garantir a privacidade e a segurança das informações pessoais dos indivíduos envolvidos.

Por isso, dentro das relações de trabalho, os dados pessoais e sensíveis dos trabalhadores – como, por exemplo, nome, endereço, CPF, RG, escolaridade, e-mail, estado civil, nome dos genitores, etc. - necessitam de adequação à Lei Geral de Proteção de Dados, devendo, por isso, ser observada cada fase da relação de trabalho e/ou emprego para o devido enquadramento de tais proteções abarcadas pela LGPD.

a) Da Fase Pré-Contratual

A fase pré-contratual é, por exemplo, o período de recrutamento de terceiros, a seleção de empregados para empresa, a análise de currículos, etc. Nesta fase de seleção de candidatos, é fundamental tomar alguns cuidados para garantir a proteção

e privacidade das informações dos candidatos.

Esses cuidados incluem: 1) Solicitar apenas as informações estritamente necessárias para avaliar e selecionar o candidato, considerando as atividades do cargo oferecido; 2) Restringir o manuseio e arquivo dos currículos, mesmo com o consentimento dos candidatos, mantendo a proteção das informações contidas neles; 3) Informar aos candidatos como suas informações serão tratadas e se serão mantidas em banco de dados, obtendo autorização expressa para tal; 4) Esclarecer que os dados fornecidos serão usados exclusivamente para a candidatura da vaga anunciada e não para outros fins, exceto para fins estatísticos, onde as informações são tratadas de forma anônima; 5) Assegurar o uso adequado e a não divulgação das informações obtidas durante as entrevistas, orientando os colaboradores da seleção sobre a responsabilidade na preservação das informações consideradas sensíveis; 6) Após a seleção de um candidato, destinar adequadamente as informações dos candidatos não selecionados, seguindo a opção escolhida (manter em banco de currículos ou eliminar os dados).

b) Da Fase Contratual

Aqui, há a admissão do empregado e/ou formalização de contrato, aumentando o fluxo de dados e documentos entre a empresa e o trabalhador, exigindo-se, por isso, maior cautela e cuidados na tratativa de tais informações.

Para cumprir as exigências legais de proteção de dados dos funcionários e colaboradores, as empresas precisam fazer uma análise de todos os departamentos que têm acesso a essas informações. Esse mapeamento ajudará a identificar riscos e necessidades de adequação à Lei, podendo envolver a revisão de cláusulas contratuais, políticas internas e a implementação de treinamentos específicos sobre o tratamento adequado dos dados, sendo, assim, imprescindível tal garantia.

Neste ponto, importa, ainda, salientar que o tratamento de dados pessoais sensíveis, como informações sobre saúde, raça, biometria, dados de menores de idade, dentre outros, requer atenção especial das empresas. Embora a coleta de alguns desses dados possa estar respaldada por leis específicas, eles exigem uma proteção ainda maior por parte do responsável pelo controle dessas informações (controlador), a fim de garantir a privacidade e a segurança dos dados sensíveis dos

indivíduos envolvidos. Por isso, é essencial seguir as diretrizes e regulamentações pertinentes para assegurar o tratamento adequado dessas informações sensíveis.

c) Da fase de Efetiva Execução do contrato de trabalho

A fase de execução do contrato de trabalho refere-se ao período em que o empregado já está atuando na empresa, desempenhando suas funções conforme as condições estabelecidas.

No contexto de tratamento de dados pessoais no ambiente de trabalho, é importante existir cláusulas nos contratos de trabalho que mencionem o tratamento de dados. Essas cláusulas podem conceder ao empregador o direito de tratar os dados do empregado, bem como estabelecer a obrigação de sigilo e responsabilização em caso de violação das informações. Assim, é aconselhável que tais disposições estejam presentes no contrato de trabalho, podendo fazer referência a documentos de compliance que devem ser observados pelo empregado titular dos dados. Essas medidas visam garantir a conformidade com as leis de proteção de dados, assegurando a privacidade e segurança das informações pessoais dos empregados.

Ainda, com a vigência da Lei Geral de Proteção de Dados, valoriza-se a transparência entre empregador e empregados, visando a relação harmônica entre ambos.

Conforme já exposto anteriormente, o artigo 11 da Lei Geral de Proteção de Dados trata dos dados sensíveis, relacionados à raça, etnia, convicção religiosa, filiação sindical, saúde, vida sexual, dados genéticos ou biométricos, dentre outros, devendo, por isso, tais dados sensíveis abarcarem uma proteção ainda maior por parte do empregador, apenas sendo coletados para finalidades definidas e realmente necessárias para o bom funcionamento da empresa.

Por fim, a ficha de registro empregado, assim como suas informações biométricas de impressão digital, íris, rosto, são considerados dados sensíveis. Por isso, caso o empregador precise tratar esses dados, é fundamental que, antes, haja a garantia de que o empregado tenha dado seu consentimento.

d) Da Fase Pós-Contratual

Tal fase é caracterizada pelo desligamento do funcionário/colaborador dos quadros efetivos da empresa, havendo a necessidade de se informar a devida finalização do uso dos dados de tais colaboradores.

Contudo, no contexto das relações trabalhistas, existem obrigações legais para a guarda de documentos, o que pode impedir o atendimento imediato de solicitações do titular dos dados em relação ao uso futuro dessas informações. Cada caso deve ser analisado individualmente, considerando as exigências legais de guarda e a possibilidade de fornecer ao titular informações sobre o uso futuro de seus dados. A legislação pode estabelecer, ainda, prazos específicos para a manutenção de certos documentos, o que pode limitar a disponibilidade imediata de atendimento às solicitações do titular. Nesse cenário, é fundamental agir em conformidade com as regulamentações vigentes e buscar a melhor solução para proteger os direitos do titular dos dados enquanto se cumpre as obrigações legais de guarda.

Além disso, o prazo prescricional para que o empregado possa exigir seus créditos e direitos trabalhistas provenientes da relação de trabalho é de cinco anos, limitado a dois anos após o término do contrato de trabalho, e, durante todo esse tempo, deve se observar as diretrizes da Lei Geral de Proteção de Dados.

5.2 A efetiva aplicação da Lei Geral de Proteção de Dados nas relações trabalhistas

Como visto, a Lei Geral de Proteção de Dados é aplicada na seara trabalhista, com o empregador devendo adotar precauções no armazenamento e retenção de documentos pessoais, tanto de candidatos a vagas de emprego quanto de empregados durante o contrato de trabalho.

Isto posto, a aplicação da LGPD nas relações de trabalho implica que o titular dos dados, que pode ser, por exemplo, o empregado ou o prestador de serviços, forneça as informações ao empregador, que deve tomar as corretas decisões relacionadas ao tratamento de tais materiais.

Conforme já exposto no artigo 7º da LGPD, o consentimento para guarda e armazenamento de dados/documentos pessoais de candidatos a vagas empregatícias pode ser dispensado, todavia, ao final do processo seletivo, a não contratação do funcionário implica em incompatibilidade de armazenamento desses

dados.

Portanto, se a empresa pretende manter os dados dos candidatos para uma futura necessidade de contratação, é necessário elaborar um termo de consentimento, devendo o mesmo ser apresentado aos candidatos, informando-os sobre a intenção da empresa em armazenar seus currículos e documentos por um período específico. O consentimento dos candidatos é fundamental para que a empresa possa, legalmente, manter esses dados em seus registros, garantindo a conformidade com as disposições da LGPD.

Ainda, se partirmos para uma análise mais detalhada da CLT, o empregador tem até cinco dias úteis para anotar as informações referentes à admissão do empregado na Carteira de Trabalho e Previdência Social (CTPS). Por esse motivo, é recomendado que a empresa retenha apenas cópias dos documentos essenciais para a contratação do funcionário, evitando qualquer problema relacionado à retenção dos documentos originais.

Ainda, quanto a transmissão, à terceiros, de dados pessoais e/ou dados pessoais sensíveis do empregado, o empregador deve adequar tal fato com o mesmo. Isto posto, com a implementação da LGPD e as mudanças relacionadas à proteção de dados no contexto trabalhista, é necessária a adoção de novas formas de armazenamento, com a definição de práticas que auxiliem na preservação de tais dados pessoais, garantindo, assim, a proteção dessas informações durante toda a permanência do empregado na empresa e mesmo após o período de guarda de documentos exigido pela legislação.

6 CONCLUSÕES

O presente trabalho teve como ponto central apresentar a temática referente à interpretação da LGPD, dos princípios que a orientam e de sua efetiva aplicação na seara trabalhista. Nessa esteira, é crucial compreender como a noção de privacidade evoluiu na sociedade da informação, capacitando os indivíduos com o controle sobre a coleta e o tratamento de seus dados pessoais, pois tal constatação é fundamental para entender a lei em profundidade.

Neste contexto, a má utilização de informações pessoais pode acarretar consequências prejudiciais tanto no âmbito físico, como a exposição a roubos, invasões de residências e empresas, furto de dados pessoais sensíveis, quanto no plano material, incluindo atividades fraudulentas, apropiação indébita, apropriação de identidade, dentre outros exemplos. No que tange ao aspecto não material, os indivíduos podem enfrentar a perda de domínio sobre seus dados, resultando na manipulação de suas percepções e na restrição de seus direitos fundamentais, como a liberdade de expressão e a salvaguarda da privacidade.

Isto posto, conforme visto, a Lei Geral de Proteção de Dados na seara trabalhista busca regulamentar a tratativa dos dados pessoais e/ou dados pessoais sensíveis, inclusive flexibilizando as possibilidades de tratamento adequado nessas situações. Portanto, além de entender a finalidade de suas tratativas, o empregador precisa estar ciente da legitimidade do processo de adequação.

Em contrapartida, a aplicação das exigências da LGPD traz, ainda, dúvidas e insegurança para muitos dos envolvidos nas relações trabalhistas, face empregados e empregadores. Contudo, as vantagens na aplicação de tal lei devem ser analisadas, tendo em vista que tais vantagens se sobrepõe as desvantagens na aplicação da mesma.

Como exemplo, dentre as desvantagens, pode-se citar a desinformação por parte das empresas; o custo despendido pelas empresas para colocar os dados em ordem e em conformidade com os parâmetros da LGPD, pois, enquanto as pequenas empresas tendem a ter menos dados e, com isso, não ser tão cara a adaptação, as empresas maiores precisam despender de um custo mais elevado na implementação da proteção de tais dados, nomeando, inclusive, um responsável pela proteção

desses dados pessoais em nome da empresa, sendo este, também, responsabilizado junto à empresa em caso de mau uso dos dados pessoais ou vazamento dos mesmos por qualquer motivo; ainda, há empresas que não implementam tais regulamentações da LGPD por medo do trato burocrático que poderia ser gerado *a posteriori*, ou por receio das multas que podem afetar tais empresas caso essa não seja compatível com a legislação em análise que, conforme artigo 52 da LGPD, perfaz o montante equivalente de até 2% (dois) por cento 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$ 50.000.000,00 (cinquenta milhões de reais) por infração.

Dentre as vantagens, pode-se citar a extrema segurança na tratativa dos dados pessoais dos empregados e clientes, gerando uma cyber-segurança para a empresa ao evitar que criminosos possam causar estragos e roubo de dados e informações dos clientes/empregados, pois, com a sofisticação de tais ataques crescendo a cada dia, ter, na empresa, uma estrutura compatível com a LGPD ajuda na segurança dos sistemas e garante o aumento da segurança cibernética, gerando, inclusive, ampliação dos negócios; além disso, a adequação à LGPD permite o gerenciamento eficiente dos dados, oferencendo aos usuários finais produtos e serviços mais céleres e seguros, garantindo o afastamento de qualquer violação dos dados e sigilo das informações; ainda, a LGPD estabelece o direito de intervenção humana em processos de decisão automatizada, reduzindo decisões arbitrárias e fazendo com que os dados fiquem mais organizados, facilitando o uso e aumentando a compreensão do valor dos dados subjacentes, além de fazer com que as organizações aprendam mais profundamente sobre seus clientes e identifiquem, por exemplo, áreas em que as suas necessidades não são atendidas. Ademais, ao aderir à LGPD, as empresas promovem a cultura de segurança de dados entre os funcionários e fomentam a responsabilidade social nos negócios, trazendo a visão de sucesso e liderança na adoção de uma nova cultura empresarial que valoriza a privacidade humana.

Outrossim, mais uma vez, importa salientar que a proteção de dados pessoais é um direito humano fundamental, sendo de vital importância que as leis estejam sempre atualizadas para acompanhar o avanço tecnológico. Isto posto, a existência

de legislações específicas, como a Lei Geral de Proteção de Dados, é crucial, dada a importância estratégica da informação no mercado atual, pois esta garante a proteção necessária para os dados em um contexto de constantes mudanças.

Em suma, é imprescindível que os empregadores entendam todo o fluxo de dados pessoais dentro da organização de sua empresa, em todas as etapas, desde o processo seletivo até a demissão de seus empregados, pois a clareza no fluxo de dados garante segurança e conformidade com a Lei Geral de Proteção de Dados, permitindo, com isso, que, durante todo o ciclo empregatício, sejam tomadas medidas adequadas para proteger a privacidade dos empregados e clientes.

Com isso, é imprescindível que haja a realização de um mapeamento do fluxo de dados pessoais dos empregados e clientes ao longo de suas trajetórias dentro da empresa, e, com base nessa análise, a empresa pode preparar políticas internas, códigos de conduta, canais de comunicação e ajustes contratuais necessários para garantir a proteção e privacidade dos dados pessoais dos clientes e empregados.

Não restam dúvidas, portanto, que é notória a capacidade da Lei Geral de Proteção de Dados (LGPD) respeitar a privacidade dos dados pessoais de acordo com os novo paradigmas da privacidade. Entretanto, para que tal lei seja eficaz, é necessário criar defesas e mecanismos que abordem o tratamento de dados com cautela, considerando o contexto moderno atual. Caso não sejam estabelecidas medidas adequadas, a lei pode não produzir os efeitos desejados, colocando em risco os direitos fundamentais dos cidadãos que ela busca proteger. Por isso, na seara do Direito do Trabalho, a implementação bem-sucedida da LGPD é imprescindível para a garantia da privacidade dos dados pessoais e da preservação da segurança e da integridade das informações dos indivíduos.

REFERÊNCIAS

ANPD. **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte.** Disponível em: https://www.gov.br/anpd/pt-br/documentos-epublicacoes/guia-vf.pdf. Acesso em: 22 jun. 2023.

BARROS, Leonardo. **Relaçao de Trabalho: Entendendo os Principais Tipos.** Disponível em: https://blog.tangerino.com.br/rh/relacao-de-trabalho/. Acesso em: 20 jun. 2023.

BOMFIM, Vólia Cassar. **Direito do Trabalho**. 15ª ed. Rio de Janeiro: Forense, 2018.

BRASIL. **Consolidação das leis do trabalho.** 50ª. ed. São Paulo: LTr, 2019.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Código de defesa do consumidor. Diário Oficial da União, Brasília, 11 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 20 jun. 2023.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Diário Oficial da União, Brasília, 10 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 05 jun. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei geral de proteção de dados. Diário Oficial da União, Brasília, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 jul. 2023.

CASTELLS, M. (2018). **O poder da identidade**: a era da informação, volume 2. São Paulo: Paz & Terra.

CASSAR, Vólia Bomfim. **Resumo de direito do trabalho.** 6. ed. Rio de Janeiro: Forense; São Paulo: Método, 2018.

CECCHETTINI, Eliane El Badouy. Vantagens e Desvantagens da Lei Geral de Proteção de Dados. **BREAK.** Disponível em: https://negocios.empresaspioneiras.com.br/break/noticias/NOT,0,0,1462074,vantagens+e+desvantagens+da+lei+geral+de+protecao+de+dados.aspx. Acesso em: 20 jun. 2023.

DELGADO, Maurício Godinho. **Curso de Direito do Trabalho**. 18ª. Ed. São Paulo: LTr, 2019.

DONEDA, Danilo. **Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro:** da emergência de uma revisão conceitual e da tutela de dados pessoais. 2008. Disponível em: https://ambitojuridico.com.br/cadernos/direitocivil/privacidade-vida-privada-e-intimidade-no-ordenamento-juridico-brasileiro-daemergencia-de-uma-revisao-conceitual-e-da-tutela-de-dados-pessoais/#_ftn27. Acesso em: 07 dez. 2022.

KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do Brasil:** lei nº 13.709/18. 2019. 83 f. TCC (Graduação) - Curso de Direito, Universidade Federal de Santa Catarina, Florianópolis, 2019. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf?sequence=1&isAllowed=y. Acesso em: 28 jan. 2023.

LIMA, Lindamaria. Os 10 Princípios para tratamento de dados da LGPD. **Triplait.** Disponível em: https://triplait.com/principios-para-tratamento-de-dados-da-lgpd/. Acesso em: 20 jul. 2023.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18).** 1. ed. Goiânia: RM Digital Education, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de dados Pessoais comentada.** 3. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2021.

MENDES, Thomas. **LGPD:** entenda sobre anonimização de dados. Disponível em: https://w3lcome.com/pt/lgpd-dados-anonimizados/. Acesso em: 06 jun. 2023.

NASCIMENTO, Amauri Mascaro. **Curso de direito do trabalho**. 21ª ed. São Paulo: Saraiva, 2006.

PALLOTTA, Maurício; MORAES, Beatriz. **LGPD nas relações de trabalho.** São Paulo, 2021.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais comentários à lei n. 13.709/2018:** LGPD**.** São Paulo: Saraiva, 2018. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553608324/cfi/0!/4/2@100:0.00. Acesso em: 14 jul. 2023.

RAPÔSO, Cláudio F L et al. **LGPD-LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO**: Revisão Sistemática. RACERevista da Administração, v. 4, 2019.

RIBEIRO, L. **Proteção de dados pessoais: Estudo comparado do regulamento 2016/679 do parlamento europeu e conselho e o projeto de lei brasileiro n. 5.276/2016.** Brasília, 2016.

SANDER, Guilherme. **Principais conceitos da LGPD**. 2019. Disponível em: https://sisqualis.com.br/conceitos-lgpd/. Acesso em: 06 maio 2023.

SILVA, Rosane Leal; SILVA, Letícia Brum. **A proteção jurídica de dados pessoais na internet:** análise comparada do tratamento jurídico do tema na União Europeia e no Brasil. Direito e novas tecnologias. Florianópolis: FUNJAB, 2013. Disponível em: http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65. Acesso em: 18 abr. 2023.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais**: comentada artigo por artigo. 2. Ed., ver., atual., ampl. Salvador: Juspodivm, 2020.

TUMELERO, Thays. **Princípios da LGPD:** terminologia e aplicação prática. 2019. Disponível em: https://ostec.blog/geral/principios-da-lgpd. Acesso em: 05 maio 2023.

TUMELERO, Thays. **Vigência da LGPD e a insegurança jurídica**. 2020. Disponível em: https://www.nsctotal.com.br/noticias/vigencia-da-lgpd-e-a-inseguranca-juridica. Acesso em: 28 jun. 2023.