# LEI GERAL DE PROTEÇÃO DE DADOS: LGPD E SUA INFLUÊNCIA NAS RELAÇÕES DE EMPREGO

Ivana Brizzi Kunzler[1]

Nelci Lurdes Gayeski Meneguzzi [2]

Resumo: O presente artigo, baseado na metodologia de pesquisa bibliográfica qualitativa, com o objetivo de melhor compreender a Lei Geral de Proteção de Dados - LGPD, faz uma análise histórica identificando a evolução da legislação até a entrada em vigor da Lei nº 13.709/2018. Analisa a importância, hodiernamente, da proteção de dados, já que informações, atualmente, tem alto valor de mercado, e, em contraponto, a legislação em foco, aplicada no tratamento de dados, representa para o seu titular um instrumento de controle sobre as próprias informações e significativa garantia de direitos. Ademais, para além desta parte inicial, este trabalho aborda a influência da Lei Geral de Proteção de Dados – LGPD nas relações de trabalho, especificando, além disso, como afeta as relações de emprego, haja vista que impossível a manutenção de tal relação sem que se colete dados, inclusive dados sensíveis, e aí se vê outra dificuldade, pois se tratando de uma vinculação onde o empregado é dependente e parte fraca do elo, o consentimento para fornecimento e tratamento dos dados pessoais fica em um limiar de extrema

1Acadêmica do Curso de Direito da Universidade Regional do Noroeste do Estado do Rio Grande do Sul - UNIJUI.

2Doutoranda do Programa de Pós-Graduação Stricto Sensu em Direitos Humanos da Universidade Regional do Noroeste do Estado do Rio Grande do Sul - UNIJUI. Mestra em Direito pela Universidade de Caxias do Sul - UCS. Docente do Curso de Direito na Universidade Regional do Noroeste do Estado do Rio Grande do Sul - UNIJUÍ, nos campus de Ijuí, Santa Rosa e Três Passos e na Universidade Regional Integrada do Alto Uruguai e das Missões - URI - Campus de Santo Ângelo.

vulnerabilidade. Faz uma breve análise da implicabilidade desta legislação no cotidiano da empresa e indica o quão importante a sua adaptação, seja para não sofrer com as penalidades que podem ser aplicadas, seja para se manter e/ou se tornar competitivo no mercado mundial. Finaliza concluindo que já era hora de o Brasil ter a sua legislação para proteção de dados pessoais, bem como da necessidade da população, e principalmente, das empresas se conscientizarem de sua importância e aplicar seus princípios e regras nas rotinas de trabalho.

Palavras-Chave: Lei Geral de Proteção de Dados – LGPD; Importância da *data protection;* Impactos nas relações de trabalho e emprego; Aplicabilidade nas empresas. Direito do Trabalho.

## INTRODUÇÃO

O presente artigo apresenta um estudo acerca da Lei Geral de Proteção de Dados - LGPD, a fim de se conhecer esta legislação que entrou em vigor no Brasil há tão pouco tempo. Esse estudo se faz necessário pois afeta todas as pessoas nas mais diversas áreas da vida e, em especial, nas mais diversas áreas do direito, seja relacionadas ao direito público ou direito privado, será, no entanto, enfatizada a sua implicação nas relações de trabalho, com ênfase nas relações de emprego.

Para a realização deste trabalho foram efetuadas pesquisas bibliográficas, tanto em relação à Lei nº 13.709/2018 propriamente, como das legislações que foram aprovadas e vigoraram ou ainda vigoram relacionadas ao tema abordado, bem como de artigos, cursos, enfim, na doutrina disponível sobre o tema, a fim de enriquecer a coleta de informações e permitir um aprofundamento no estudo da matéria, e revelar a sua importância para o direito e para toda a sociedade.

Inicialmente, no primeiro capítulo, foi realizada a

abordagem do aspecto histórico, identificando que a discussão surgiu na Europa e, no Brasil, observa-se o primeiro indicativo na Constituição de 1988, sendo uma grande e longa caminhada até a publicação da Lei Geral de Proteção de Dados – LGPD, em 2018, também são analisadas situações que esclarecem quão importante é a matéria de *data protection* para toda a sociedade.

Já no segundo capítulo o estudo é direcionado e aprofundado se voltando a aplicação da Lei Geral de Proteção de Dados – LGPD, respeitando os direitos fundamentais do indivíduo, nas relações de trabalho, mas principalmente nas relações emprego, influenciadas pela nova lei em vigor, havendo urgência na identificação de possibilidades e alternativas, especialmente quando se tem explícito na Lei que um dos critérios para fornecimento e tratamento de dados é a autorização consentida, em especial ao considerar dados sensíveis fornecidos em alguma das fases da relação empregatícia, relação esta claramente assimétrica. Também são analisadas algumas mudanças necessárias a serem implementadas pelas organizações para adequação à nova legislação, objetivando tanto a não incidência de sanções como um grande diferencial no mercado de negócios.

## 1 A LEI GERAL DE PROTEÇÃO DE DADOS – LGPD: APONTAMENTOS GERAIS

A informação nunca foi tão disseminada, e de forma tão rápida como na contemporaneidade, segundo Viviane Nóbrega Maldonado (2019) nunca na história uma quantidade tão grande de informações foi processada de forma rápida e sem interrupção, fazendo com que a proteção de dados, para que seja respeitada a privacidade do indivíduo, se tornasse matéria de suma importância a ser tratada nos dias de hoje, em especial aos que contém características de dados pessoais.

De acordo com Maria Eugenia Finkelstein e Claudio Finkelstein (2019, p. 285):

> Com o desenvolvimento da tecnologia e intensificação dos

> fluxos de informação, surgem novas possibilidades de armazenamento, utilização e manipulação de informações pessoais, refletindo em mudanças no conceito de direito à privacidade, de modo que a informação que antes era dispersa, torna-se organizada. Riscos que envolvem a violação à privacidade e à personalidade dos cidadãos na sociedade da informação crescem exponencialmente, como a possibilidade de uso indevido dos dados pessoais, cadastro e classificação dos indivíduos, propagandas de *marketing* invasivas, publicidade comportamental, vigilância estatal, utilização indevida da *Big Data*, coleta de dados através da *Internet* das coisas, entre outros.

Ainda segundo Finkelstein e Finkelstein (2019, p. 290):

> […] a cada vez que o usuário trafega na Rede, para que possa usufruir de seus benefícios, deverá preencher formulários virtuais, nos quais informa seus dados pessoais, seus hábitos de consumo e, às vezes, seus dados patrimoniais e preferências. Dessa forma, os *sites* que se dedicam ao comércio eletrônico organizam verdadeiros bancos de dados acerca de seus usuários, cuja utilização encontra-se numa zona cinzenta, uma vez que nem o usuário nem o Poder Público sabem exatamente a forma da utilização destas informações.

Porém, esta discussão teve início há muito tempo, nesse sentido Raphael Miziara (2021) afirma que, no cenário internacional, já em 1973 o Conselho da Europa disciplinou juridicamente o tratamento de dados pessoais, onde as Resoluções 22/1973 e 29/1974 versavam sobre princípios que objetivavam a proteção de dados pessoais em bancos de dados automatizados. Em 1981, o Conselho da Europa institui a Convenção nº 108 (Convenção para a Proteção de Indivíduos com Relação ao Processamento Automático de Dados Pessoais) aberta inclusive para países não integrantes da União Europeia, sendo considerado o primeiro instrumento internacional que regulamenta o assunto com força legal. Já em 1995 foi editada a Diretiva nº 46, a qual foi substituída, em 25 de maio de 2018, pelo Regulamento Geral de Proteção de Dados (GDPR).

Conforme Ludimila Santos Derbli (2019, p. 183):

> Em linhas gerais, o GDPR regula o tratamento e a livre circulação dos dados pessoais de uma pessoa singular identificada

> ou identificável que consiste na coleta, armazenamento e utilização de informações que identifiquem ou permitam a identificação de indivíduos europeus, tais como, nome, número de identificação, dados de localização, identificadores por via eletrônica ou outros elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social da pessoa singular.

Consoante afirma Finkelstein e Finkelstein (2019) o Regulamento Geral de Proteção de Dados – GDPR, ou General Data Protection Regulation, foi promulgado objetivando reforçar e unificar a proteção de dados pessoais da União Europeia, sendo obrigatório em todos os seus elementos e aplicável a todos os Estados membros.

No Brasil, inicia-se a inclusão de proteção de dados na legislação com a Constituição Federal (1988), em seu artigo 5º, inciso X: "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).

O Código de Defesa do Consumidor (BRASIL, 1990) traz à baila, em seu art. 43: "O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes". Bem como do §3º do mesmo artigo se depreende que quando o consumidor encontrar dados e cadastros com informações inexatas, poderá exigir a correção imediatamente, bem como o eventual destinatário ser comunicado das correções efetuadas, no prazo de 05 dias úteis.

Na sequência, a Lei nº 9.507/1997 que regula o acesso a informações e disciplina o rito processual do habeas data, o qual será concedido com o fim de assegurar o conhecimento de informações que dizem respeito ao requerente e que constam em banco de dados de entidades governamentais ou que sejam de caráter público, para retificar dados quando não for a preferência em fazer por meio de processo sigiloso, administrativo ou

judicial, e para que seja possível a anotação no cadastro do requerente de explicação ou contestação de dado verdadeiro mas justificável e que esteja sub judice ou em pendência amigável.

Já a Lei nº 12.414/2011 que disciplina a formação e a consulta a banco de dados com informação de adimplemento para formação de histórico de crédito, conhecida popularmente como "lei do cadastro positivo", prevê em seu art. 3º, §1º: "Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado" (BRASIL, 2011), já o §3º do mesmo artigo indica que há proibição de anotações com excesso de informações, assim consideradas as que não estiverem diretamente vinculadas à análise de risco de crédito, bem como anotações de informações sensíveis do consumidor, qualificando como sendo "aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas" (BRASIL, 2011). A mesma lei prevê ser direito do cadastrado, dentre outros, o cancelamento e reabertura do cadastro quando assim o solicitar, acessar, independentemente de justificativa, as informações sobre ele cadastradas, e ter os seus dados pessoais utilizados exclusivamente, de acordo e com a finalidade para qual foram coletados.

Segundo Lys Nunes Lugati e Juliana Evangelista de Almeida (2020) na Lei nº 12.414/2011 se constata a consolidação e a evolução do conceito de autodeterminação informativa no ordenamento jurídico, ao colocar o consentimento do titular das informações como condição para que o compartilhamento de dados seja lícito.

No mesmo ano entra em vigor a Lei nº 12.527/2011 que regula o acesso a informações e dispõe sobre os procedimentos a serem observados para garantir o acesso à informação, com observância aos princípios básicos da administração pública, e mediante procedimentos ágeis e objetivos, de forma clara,

transparente e em linguagem de fácil compreensão. O art. 31 desta lei dispõe que: "O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais" (BRASIL, 2011).

Em 2014 é aprovada a Lei nº 12.965/2014, o Marco Civil da Internet, que estabelece os princípios, as garantias, os direitos e os deveres para a utilização da Internet, além de estabelecer diretrizes para a atuação da União, Estados, distrito Federal e Municípios sobre a matéria, tendo como fundamento o respeito à liberdade de expressão, e dentre seus princípios trás a proteção da privacidade (ensejando indenização pelo dano moral e material causado pela violação da intimidade e da vida privada) e a proteção dos dados pessoais dos usuários(com determinação para não fornecimento a terceiros de dados pessoais, e para fornecimento de informações claras e completas quanto a coleta, uso, tratamento, armazenamento e proteção de dados pessoais).

No entanto, segundo Lugati e Almeida (2020, p. 02): "não existia regulamentação que abordasse especificamente a problemática da proteção de dados, o que colocou em destaque a importância de se ter uma legislação específica sobre isso." E, para fins de preencher esta lacuna, o Brasil sanciona, em 2018 a Lei Geral de Proteção de Dados - LGPD, sendo que esta, conforme Lugati e Almeida (2020) já estava em desenvolvimento desde 2010, e inclui o nosso país dentre os que tem legislação completa de proteção de dados.

De acordo com Finkelstein e Finkelstein (2019) a Lei nº 13.709/2018 foi aprovada com vetos do então Presidente da República Michel Temer, dentre eles quanto a supressão da criação da Autoridade Nacional de Proteção de Dados – ANPD, que foi posteriormente estabelecida como o órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, assim como a responsabilidade pela edição de normas sobre o tema, e a interpretação da Lei Geral de Proteção de Dados.

Como Derbli (2019) defende, a Lei nº 13.709/2018 (LGPD) foi eminentemente inspirada da General Data Protection Regulation (GDPR) em vigor na Europa desde 2018, sendo possível observar a presença em ambos, por exemplo, da abrangência na tutela de dados pessoais e dados sensíveis, na obrigatoriedade de se obter consentimento dos indivíduos para tratamento de seus dados pessoais, do direito ao esquecimento e da aplicação de sanções para quem descumprir as regras previstas na lei ou no regulamento. Mas a produção legislativa brasileira inova ao tratar, por exemplo, da utilização de dados necessários à execução de políticas públicas pela administração pública.

Conforme Felipe Palhares, Luis Fernando Prado e Paulo Vidigal (2021, n.p.):

> A LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, de direito público ou privado, e tem por fim máximo a proteção dos direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural. Não obstante, a lei fundamentala-se em valores como garantia do desenvolvimento econômico e tecnológico e a inovação (art. 2º, V), funcionando como desejável vetor de segurança jurídica, principalmente a entes que realizam o tratamento de dados pessoais de forma habitual e sistemática.

Este novo sistema, trazido pela Lei Geral de Proteção de Dados – LGPD implica no cotidiano de praticamente toda população, com maior ou menor intensidade, e levando em conta que informações e, em especial, dados pessoais, são hoje um dos principais insumos para o enfrentamento do mercado globalizado e baseado em tecnologia, há a necessidade inadiável de se ter um marco regulatório na proteção de dados.

E para se falar na importância da proteção de dados é imprescindível trazer alguns exemplos, os quais por si só, trazem consigo fundamentos suficientes para expor o mérito na aplicação da Lei Geral de Proteção de Dados – LGPD nos mais diversos setores e contextos, para que se possa manter direitos sociais dos indivíduos, como a liberdade e a intimidade.

Iniciando com o exemplo do caso Cambridge Analytica, trazido por Miziara (2020), concernente à defesa da democracia, onde o vazamento de dados de Facebook para uma companhia que trabalhou na campanha que elegeu Donald Trump, sendo que tal material foi utilizado em conjunto com algoritmos, criando um conjunto de ações para influenciar eleitores nos Estados Unidos da América e em vários outros países, com destaque para o pleito norte americano de 2016 e no plebiscito sobre o Brexit.

Já o caso Target, também fomentado por Miziara (2020), é visto como impactante no que concerne aso aspectos concorrenciais, havendo o monitoramento dos padrões de comportamento para enviesamento de consumo, então, desta forma, a Target sabe que, se uma mulher americana de 23 anos comprar uma loção de manteiga de coco, uma bolsa grande o suficiente para guardar fraldas, suplementos como zinco e magnésio e um tapete azul, há 87% de chances de ela estar grávida há 03 meses.

Coleta e manipulação de dados impactam, ainda, segundo Miziara (2020), na tomada de decisões empresarias, alterando a relação comercial entre empresas e consumidores, como quando se utiliza a localização geográfica do consumidor, tanto para oferecer produtos e publicar campanhas de marketing adequados àquela localidade ou região, como para praticar precificação geográfica, que consiste na possibilidade de aplicação de preços diferentes para um mesmo produto, dependendo da origem de acesso.

No tocante à proteção de direitos fundamentais, em especial no contexto laboral, Miziara (2020) traz como exemplo dois casos da empresa Amazon, sendo um deles quanto a utilização de algoritmo para rastrear a produtividade dos trabalhadores e demitir funcionários que não atendem as expectativas, baseando-se exclusivamente nos dados; já o outro é sobre ferramenta que a Amazon desistiu de utilizar para recrutamento de funcionários, automatizando a busca de talentos, pois tal sistema

apresentava viés contrário às mulheres.

Em especial no que concerne a este último exemplo, a Lei Geral de Proteção de Dados – LGPD, em seu art. 20, já demonstra sua importância ao assegurar direito à explicação em caso de despedida automatizada, sendo que o titular dos dados poderá solicitar a revisão das decisões tomadas unicamente baseadas em tratamento automatizado de dados pessoais (BRASIL, 2018).

Segundo Eugênio Facchini Neto e Karine Silva Demoliner (2019) com o surgimento das redes sociais, as pessoas criam contas, conectam-se umas às outras, e nestas plataformas revelam as atividades que realizam, suas imagens, gostos e predileções, e expõe cada vez mais sua vida privada, entretanto, em contraponto está um sistema altamente complexo e sofisticado que busca o maior número de informações do maior número possível de pessoas, as catalogam, traçando seus perfis.

Facchini Neto e Demoliner (2019) apontam que tudo o que se faz com a utilização da Internet é convertido em algoritmo, das tarefas mais simples como pesquisar algo no *googl*e às mais complexas, como transações financeiras, ou mesmo a realização de compras eletrônicas, e utilização de aplicativos em geral. Com base no perfil traçado, sabendo do que o indivíduo gosta, é, faz e acredita, há o direcionamento de publicidade e conteúdos específicos, a fim de induzir a prática de determinada ação.

No que se refere aos aplicativos de serviços públicos, ainda segundo Facchini Neto e Demoliner (2019), há a preocupação na possibilidade de controle, intromissão e manipulação pelo Estado, na esfera privada dos indivíduos. No Brasil vários estudos vem sendo realizados nos principais aplicativos disponibilizados pelo Governo Federal e suas autarquias, como no Sefaz, Meu INSS, Anatel, e pelos Governos Estaduais, como o Notas Fiscais Eletrônicas e CNH Digital, com a finalidade de analisar qual o grau de coleta de dados pessoais dos usuários e,

especialmente, se estão ou não sendo utilizados para a finalidade específica para a qual foram coletados ou se estão sendo utilizados para fins diversos e qual o grau de proteção que o aplicativo oferece contra vazamentos.

Conforme ensina Gustavo Rocha (2019), a maioria das pessoas ignora, ainda, que existe um conjunto de normas, normativas e regras que orientam o mundo digital, além a lei de proteção de dados, que traz uma regra clara: deverá haver interesse legítimo para a coleta e processamento de dados bem como que o detentor do dado permita o uso e o processamento deste.

Rocha (2019) afirma, outrossim, que, talvez baseados nesta ignorância, os indivíduos concordam com quaisquer regras que os softwares imponham sem pensar nos riscos envolvidos. Importante considerar, no entanto, que desta forma qualquer uma coleta dados sem mesmo informar a finalidade de uso e onde serão armazenados. E não se trata exclusivamente de dados coletados de forma digital, mas, por exemplo, na portaria de um prédio, quando se solicita documento de identificação, com foto e CPF, endereço, biometria, ao invés de somente informar o local onde se está indo. É e preciso saber onde ficam estes dados, e se estes dados vazarem, de quem era a responsabilidade de coleta, guarda e uso dos mesmos?

É indiscutível, segundo Rocha (2019) que para adaptar à Lei Geral de Proteção de Dados - LGPD as empresas e demais organizações deverão contar com equipes multidisciplinares, contando com advogados, engenheiros, pessoal de TI, e que todos da equipe pensem mais do que apenas cumprir com a letra da legislação, haja vista que há consequências diretas ou indiretas a toda a empresa, muito além das multas da lei, pois, além dos sistemas, existem pessoas, permissões de acesso, rastreabilidade das informações, entre outros, e para que quando se pensar em dados, se tenha ideias claras e objetivas sobre como agir com a coleta, como pegar o consentimento expresso e como guardar estas informações.

Insta evocar o art. 2º da Lei Geral de Proteção de Dados – LGPD, para entender a importância da *data protection*, tendo em mente que traz os fundamentos que disciplinam a proteção dos dados pessoais, sejam eles o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviabilidade 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).

Ademais, Chiara Spadaccini de Teffé e Mário Viola (2020, p. 05) ao falarem sobre a *data protection*, afirmam que: "O sistema legal desenvolvido para o tratamento de dados representa para o titular instrumento de controle sobre as suas informações pessoais e de garantia de direitos." Afirmam, além disso, que a Lei Geral de Proteção de Dados - LGPD indica uma nova cultura de tutela da privacidade e dos dados pessoais, com a instituição de norma baseada na ideia de que todo dado pessoal é relevante e possui valor, considerando representar projeção do indivíduo, além do fato de que mesmo informações que pareçam inicialmente irrelevantes, ou que não façam referência direta a alguém, uma vez transferido, cruzado ou organizado, pode resultar em dados específicos sobre determinada pessoa, trazendo informações inclusive de caráter sensível sobre ela.

Portanto, a Lei Geral de Proteção de Dados – LGPD facilita o controle dos dados tratados, tem como pilares centrais o amplo conceito de dado pessoal, a necessidade de que praticamente qualquer tratamento de dados tenha uma base legal, um rol taxativo de hipóteses legais para o tratamento de dados, a caracterização detalhada do consentimento do titular, assim como a preocupação com sua manifestação, o legítimo interesse como uma das hipóteses autorizativas, amplo rol de direitos do titular, e densa carga principiológica.

Apresenta, inclusive, deveres e responsabilidades aos agentes de tratamento, proporcionando segurança para que as informações circulem e antecipando os riscos de violação à privacidade, assim como evitando tratamentos abusivos de informações, além de vazamentos de dados.

## 2 A LEI GERAL DE PROTEÇÃO DE DADOS - LGPD E AS RELAÇÕES DE EMPREGO

As relações de trabalho, pelas características próprias do vínculo, ensejam a existência de coleta de informações entre contratante e contratado, no entanto, tal situação não autoriza que contratante viole direitos fundamentais do contratado.

A própria Lei nº 13.709/2018 traz em seu artigo 14 que "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei." (BRASIL, 2018).

Insta observar o que Flávia Acassa dos Santos (2020, pg. 145) enfatiza que é absolutamente aplicável às relações de trabalho:

> A proteção de dados é um direito humano que nasce vinculado à Declaração Universal dos Direitos Humanos (DUDH), aprovada pela Assembleia Geral das Nações Unidas em 1948, com o objetivo de garantir a dignidade do ser humano e como instrumento de combate à opressão, impunidade e insultos à dignidade humana.
>
> O objetivo deste direito é preservar a dignidade humana contra a invasão de privacidade que envolve a coleta e o tratamento excessivo de dados pessoais. Seu objetivo é estabelecer uma estrutura de garanti as que permita exercer os direitos e liberdades fundamentais dos seres humanos e impedir que o uso de informações pessoais seja usado indiscriminadamente contra os direitos e liberdades inerentes ao ser humano.

Conforme nos ensina Andrey Oliveira Lamberty e Marcelo Barroso Kümmel (2018), os direitos fundamentais hoje previstos no texto constitucional, relaciona-se de forma direta ao

desenvolvimento do Estado, adotando um caráter protecionista diante das possíveis violações que dele decorrem. No entanto, na esfera particular também ocorrem ameaças a esses direitos, como no âmbito trabalhista, em que se verifica uma grande diferença de condições entre empregado e empregador, e a tutela desses direitos se torna ainda mais necessária, já que a relação de desigualdade existente equipara o poder diretivo do empregador ao poder estatal, legitimando a aplicação dos direitos fundamentais a essa relação privada. Porém, diferentemente das relações entre Estado e indivíduo, a relação ocorre entre duas pessoas portadoras de direitos e deveres, que devem buscar a conciliação de seus interesses sem, para tanto, agredir direitos fundamentais da parte oposta.

Ainda segundo Lamberty e Kümmel (2018) a evolução da tecnologia aumentou a possibilidade de controle por parte do empregador, que dispõe de ampla gama de recursos de monitoramento, de forma que a intimidade e a vida privada do empregado fiquem ainda mais vulneráveis. Considerando, ademais, que o acesso e divulgação dos dados pessoais do contratado, com a possibilidade de manipulação desses, amplia a velocidade e a facilidade com que a informação se propaga, de forma que o conhecimento e a divulgação dessas informações pessoais podem gerar grave violação à intimidade e à privacidade das pessoas.

Para Clara Lacerda Accioly (2019) a proteção dos direitos do trabalhador deve, sem sombra de dúvidas, estar pautada pelos direitos fundamentais estabelecidos pela Constituição, em especial a dignidade da pessoa humana, e é essencial que a proteção de dados seja pautada no que diz respeito à tutela da privacidade do empregado, porém, deverão ser desenvolvidos parâmetros de proteção que se ajustem tanto aos imperativos de proteção do trabalhador quanto às necessidades dos agentes econômicos, já que o mercado, e a própria legislação, exigem, em alguma medida, a coleta e processamento de dados, ao menos para que se verifique a aptidão e adequação de um dado

trabalhador a um determinado ambiente laboral, com vistas a buscar as eficiências desejadas pelo empresário. A Lei Geral de Proteção de Dados - LGPD apresenta conceitos e institutos jurídicos para a tutela da privacidade das pessoas naturais e, por conseguinte, dos trabalhadores. Contudo, é imperativo que tais definições sejam interpretadas sob o prisma do Direito do Trabalho para que tenham real efetividade nessa seara, e na proteção efetiva do trabalhador.

Para proteger os direitos fundamentais dos indivíduos, inclusive nas relações de trabalho, a Lei Geral de Proteção de Dados - LGPD dispõe em seu artigo segundo que os fundamentos para a disciplina da proteção dos dados pessoas são: o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, informação, comunicação e opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico, tecnológico e a inovação, a livre iniciativa, livre concorrência, defesa do consumidor, bem como os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Vê-se como fundamento, portanto, além dos direitos fundamentais já expressos na Constituição Federal, a autodeterminação informativa, que consiste, segundo Miziara (2021) no poder que o indivíduo possui de controlar seus próprios dados, decidindo quando e como os revela, direito entendido por alguns, como o Tribunal Constitucional Alemão, como direito autônomo, e por outros, como no Tribunal Constitucional Português, como compreendido no direito à reserva da intimidade da vida privada.

Com certeza, como afirma Accioly (2019), haverá a necessidade de se buscar soluções estruturais que, partindo de procedimentos claros e transparentes, autorizem e legitimem a coleta e tratamento de dados dos empregados de forma consentida, no entanto, precipuamente, deverão ser estabelecidos parâmetros claros para a aferição da legitimidade do tratamento desses

dados, sob pena de ser fundamentalmente ferida a dignidade do trabalhador.

Até porque a violação dos direitos dos titulares dos dados pessoais causa consequências na esfera extrapatrimonial destes, e como destaca Pamplona Filho e Coni Junior (2020, p. 35):

> De fato, diante de tudo quanto exposto fica clarividente que a privacidade e intimidade dos titulares de dados pessoais (inclusive os empregados) estão protegidas pelo regramento da LGPD (notadamente no artigo 18), obrigando a todas as pessoas jurídicas de direito público e privado (inclusive as empresas empregadoras) a promover o tratamento adequado de tais informações intimas e privadas, podendo, portanto ser responsabilizadas, caso ofendam/lesem tais garantias (de natureza não patrimonial), amparadas por lei específica. Afinal, a legislação substantiva civil estabelece o dever geral de indenização para quem, por ato ilícito, cause danos a outrem, na forma do art. 927 do Código Civil. Portanto, diante de ofensas de fundo extrapatrimonial, deve ser aplicado o regramento respectivo nos termos específicos da CLT nos artigos 223 – A ao 223 - G.

Segundo Renato Caovilla, Rodrigo Dufloth e Letícia Pazine (2019) a Lei Geral de Proteção de Dados - LGPD tem por escopo assegurar aos titulares de dados pessoais que o tratamento de seus dados se dê de forma apta a garantir que os direitos fundamentais fundamentados na liberdade, intimidade e privacidade_sejam sempre observados, como acessar seus dados pessoais, requerer e obter cópias, eliminar os dados que foram previamente consentidos para tratamento, solicitar a exclusão de seus dados, salvo se existir alguma hipótese legal para sua manutenção, retificação de seus dados pessoais quando identificar que algum deles esteja incorreto e, caso haja descumprimento ao disposto pela LGPD, cabe ao titular se opor ao tratamento realizado. Ainda, do mesmo modo, a LGPD garante que os titulares tenham direito a anonimizar, bloquear ou eliminar dados que sejam desnecessários, excessivos ou tratados de maneira contrária às disposições da lei, realizar a portabilidade de seus dados, à informação das entidades públicas ou privadas com as quais o controlador tenha realizado um uso compartilhado de dados e ser

informado sobre a possibilidade de não consentir com o tratamento de dados, assim como revogar posteriormente o consentimento que foi anteriormente dado.

Constata-se, pois, que as relações de trabalho demandam coleta, utilização, classificação, utilização e transferência de uma série de informações, inclusive dos trabalhadores contratados, devendo, portanto, ser dever do empregador fazer uso correto das informações que detém, inclusive para proteção dos direitos fundamentais de seus colaboradores.

E se as relações de trabalho são e serão diretamente impactadas pela LGPD, ainda mais impactadas são as relações de emprego, fontes de incomensurável quantidade de fornecimento, utilização, transferência e armazenamento de dados pessoais, já que fica realmente difícil imaginar alguma relação de emprego na qual não exista tráfego de dados pessoais.

Assim, segundo Pamplona Filho e Coni Junior (2020) a política de privacidade da empresa e formulários de contratação de pessoal devem ser revistos, a fim de proteger e limitar a quantidade de dados que são fornecidos e expostos às empresas, e presentes em documentos como fichas de registro, contendo informações pessoais do trabalhador, tais como seu cadastro no registro geral, na receita federal, comprovantes de residência, estado civil, dados sobre filiação sindical, opção por vale transporte, quantidade, identidade e cartões de vacinação dos filhos para percepção de salário-família, tipo sanguíneo para eventuais emergências médicas, dentre outros dados utilizados com frequência durante a relação empregatícia, nos mais diversos momentos da relação empregatícia. Deve-se atentar, também, para que façam constar nos formulários e demais instrumentos informações claras, objetivas, inteligíveis, de fácil acesso e expressas acerca dos dados que estão sendo coletados e para quais motivos e finalidades, bem como explicitar quais deles serão armazenados e quais serão descartados, o tempo e forma de armazenamento e, principalmente se serão compartilhados e com quem.

Consoante afirmam Andrea Gardano Bucharles Giroldo e Daniela Cunha Machado (2020), nas relações de emprego a coleta e o tratamento dos dados pessoais dos empregados pelo empregador deverão estar justificados por alguma das bases legais e respeitar os princípios da finalidade, adequação, necessidade, livre acesso, transparência, segurança, prevenção e não discriminação. Deve-se ponderar se todas as informações que são transmitidas pelos empregadores, são efetivamente necessárias para a efetivação de uma contratação, assim como o empregador deverá garantir ao empregado que seus dados pessoais tão somente sejam utilizados para o fim a que se deu a coleta, ou seja, se coletar dados pessoais do empregado para o fim de efetivar sua contratação, este não poderá, a princípio, utilizá-los para outros fins, como a venda destes dados pessoais para terceiros.

Pamplona Filho e Coni Junior (2020. p. 25 e p. 26) alertam que, não obstante se voltar atenção majoritariamente para a fase contratual, a relação de emprego pode se dividir em quatro períodos, quais sejam: Pré-contratual, de formalização do contrato, contratual e pós-contratual.

Na mesma senda Giroldo e Machado (2020) constatam que a coleta e o armazenamento de dados de candidatos a certa vaga de emprego é hipótese de tratamento de dados pessoais e, por conseguinte, sujeita-se à incidência da Lei Geral de Proteção de Dados - LGPD, havendo necessidade de se ater à finalidade da coleta e armazenamento de dados pessoais do candidato, apenas naquilo que seja necessário para subsidiar a avaliação da capacidade técnica do indivíduo para ocupar a vaga de emprego ofertada e o atendimento ou não aos requisitos exigidos para determinado cargo ou função. Tendo em vista que a fase pré-contratual de seleção, tem por finalidade otimizar o processo de recrutamento e já se equipara a subordinação intrínseca às relações de emprego, a LGPD adota uma postura protetiva em relação aos titulares de dados, assim como a legislação trabalhista se

relaciona com a figura do empregado, garantindo a este o direito de obter informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. Concluída a fase de processo seletivo, por atingida a finalidade que justificou a coleta inicial dos dados, novas finalidades podem surgir, como a formalização do contrato de trabalho, ou interesse no armazenamento dos dados para possíveis contratações futuras, do contrário, não há motivos para guarda ou tratamento dos dados pessoais dos candidatos.

Quanto à fase contratual, Giroldo e Machado (2020) indicam que é atribuição legal do empregador, para fins de registro dos empregados, obter dados como nome do empregado, data de nascimento, filiação, nacionalidade, naturalidade, número de registro na Carteira de Trabalho e número de inscrição do empregado no NIS/NIT (seguridade social), no entanto, é imperioso que o tratamento de tais dados se dê em estrita observância à finalidade da coleta, ou seja, o estabelecimento da relação de emprego. Outros dados pessoais poderão ser necessários no momento da contratação, como o número de seus documentos pessoais, para fins de cadastro de admissões no E-Social, o endereço de seu domicílio, telefone e *e-mail*, para eventuais comunicações com o empregado, ou informações sobre características físicas do empregado para fins de fornecimento de equipamentos de proteção individual ou uniformes. Nessa fase, ainda, são realizados exames médicos admissionais, também por exigência legal, e os resultados se constituem de dados sensíveis, segundo a própria Lei nº 13.709/2018. Torna-se imprescindível ao empregador manter a transparência com o empregado acerca de quais dados serão coletados, assim como coletar tão somente os dados necessários para o fim pretendido, sendo vedada a utilização para outros fins, inclusive discriminatórios.

Já quanto ao término da relação de emprego, em conformidade com Giroldo e Machado (2020), o tratamento dos dados do trabalhador se fundamenta nas obrigações legais de guarda e

manutenção das informações pela empresa, pelo prazo previsto na legislação, ou para o exercício de direito em processo judicial, administrativo e arbitral, dentre os dados a serem mantidos estão os relacionados ao contrato de trabalho, como datas de início e término da relação contratual, funções exercidas, salários e alterações, jornadas de trabalho realizadas ao longo dos anos, períodos de férias, ocorrência de acidentes e outras informações que sejam de interesse à proteção do trabalhador.

Para Lamberty e Kümmel (2018), diante de possível conflito com direitos fundamentais do empregado, o empregador, especialmente na fase pré-contratual, deve tomar alguns cuidados objetivando não incorrer na violação de tais direitos, portanto, o empregador, no momento de tomar as informações do candidato à vaga, relacionando-se diretamente aos dados sensíveis do empregado deve, por exemplo, abster-se de fazer perguntas relativas às questões raciais, políticas, religiosas, atividades sindicais, ou qualquer questão que possa gerar discriminação, com exceção daquelas que sejam extremamente necessários para a prestação do serviço. Já o candidato à vaga poderá ocultar circunstâncias que não sejam relacionadas à causa contratual, e que lhe sejam impostas pelo empregador na entrevista de emprego.

Pamplona Filho e Coni Junior (2020) trazem, ainda, que mesmo quando a relação de emprego não for fonte direta de recepção de informações, será subsidiariamente responsável, em muitos casos, por originar tráfego de dados pessoais, visto que os empregadores acabam atuando indiretamente com fornecedores de serviços. Isso é possível evidenciar com a Contabilidade, que não necessariamente se faz internamente na empresa, e para quem serão enviados todos os dados pessoais e financeiros dos empregados, incluindo contas bancárias e informes de rendimento.

Isto também se vê, igualmente conforme Pamplona Filho e Coni Junior (2020), na relação com empresas de planos de

saúde ou convênios médicos, que recebem e tratam dados sensíveis dos empregados e geram outros, empresas de seguro de vida, de previdência privada, quando tais vantagens são ofertadas aos funcionários, empresas de Vale Refeição/Alimentação e/ou Vale transporte, que necessitam das informações pessoais do empregado e acabam de também de certa forma, tomando conhecimento do padrão de consumo e locais de uso de tais benefícios, e empresas de consultorias que atuam, por exemplo, buscando melhorias gerenciais, necessitando para tanto de informações pessoais das mais variadas espécies, ou consultorias necessárias a atender regramentos dos órgãos públicos, contratadas para elaboração de documentos como PPRA (programa de prevenção de riscos ambientais), PCMSO (Programa de Controle Médico de Saúde Ocupacional), LTCAT (Laudo Técnico das Condições do Ambiente de Trabalho), e SESMT (Serviços Especializados em Engenharia de Segurança e em Medicina do Trabalho).

Há ainda a possibilidade, segundo Pamplona Filho e Coni Junior (2020), de troca de informações encaminhadas pela empregadora para órgãos púbicos, tal como ocorre com as disponibilizadas para "E-Social", ou para a Relação Anual de Informações Sociais (RAIS) e Cadastro Geral de Empregados e Desempregados (CAGED) ou até mesmo para Declaração do Imposto sobre a Renda Retido na Fonte (DIRF) e Informações à Previdência Social (SEFIP).

Para Pamplona Filho e Coni Junior (2020) cabe inclusive ao empregador os deveres de prevenção e de não discriminação, impossibilitando a utilização dos dados para fins ilícitos e discriminatórios em todas as suas formas e áreas tais como de saúde, racial, ideológica, política, orientação sexual, introduzindo ainda a adoção de medidas para prevenir que ocorram danos advindos do tratamento de dados pessoais.

Dentre os requisitos trazidos pela Lei nº 13.709/2018, para tratamento de dados pessoais, está explícito no art. 7º a

hipótese o tratamento destes dados mediante o fornecimento de consentimento pelo titular, assim como também é possível para o cumprimento de obrigação legal ou regulatória pelo controlador. Já quanto aos dados sensíveis, estes somente poderão ser tratados quando o titular consentir, de forma específica e destacada e para finalidade específica, ou, sem tal consentimento, quando, dentre outras hipóteses, for indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador e para o exercício regular de direitos, como em contratos e processos judiciais. (BRASIL, 2018)

Segundo Lugati e Almeida (2020) não obstante o consentimento não ser a única base em que pode ser fundamentado o tratamento de dados, e não ser um princípio hierarquicamente superior aos demais, este assume uma importante posição na lei, sendo relevante analisar sua natureza, bem assim entender que o consentimento deve ser livre (além do já descrito na LGPD, não deverá conter nenhum vício, como erra, dolo, lesão, estado de perigo, ou vícios de consentimento, assim como, se há relação de subordinação entre as partes na hora da emissão da manifestação da vontade, o que poderia retirar a voluntariedade do consentimento), informado (dando-se ciência ao titular dos dados sobre todas as informações a respeito do tratamento destes, de forma detalhada, verdadeira e transparente, bem como informar as possíveis consequências no caso de não consentir, assegurando garantia de autonomia na decisão), e inequívoco (o titular deve agir de forma que indique de forma clara a sua anuência, de modo escrito ou por outro meio que demonstre sua vontade, devendo fazer referência a fins determinados, não podendo ser genérica, bem como não deveria ser apenas uma caixa de diálogo para marcar a opção "aceito" após um longo texto).

Neste sentido, após explanar sobre o assunto, Lugati e Almeida (2020, p. 19) afirmam que:

> […] conclui-se que é um grande passo o indivíduo estar no controle de suas informações, mas é necessário analisar que implementar o consentimento é uma atividade complexa,

> repleta de desafios e dificuldades. Ainda há um longo caminho para se efetivar o princípio da autodeterminação informativa e conferir uma efetiva segurança ao titular de dados.

Outro aspecto que merece destaque, especialmente nas relações de emprego, é o tratamento de dados sensíveis, que invariavelmente serão conhecidos durante o pacto laboral. De acordo com Teffé e Viola (2020), já que os dados pessoais qualificados como sensíveis se encontram presentes em todos os conjuntos informacionais do ser humano, a melhor forma de os proteger seria trazendo exemplos claros de dados assim considerados, explicitando que se tratam de dados referentes a origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político, além daqueles referentes à saúde ou à vida sexual e dados genéticos ou biométricos. Muitos destes dados poderiam, se expostos, ocasionar a discriminação de seu titular, devendo, por conseguinte, ser protegidos de forma mais rígida, assim como se verificar o contexto de sua utilização, além das relações que podem ser estabelecidas com as demais informações disponíveis e a potencialidade de seu tratamento servir como instrumento de estigmatização ou discriminação.

Fica evidente, portanto, que os dados sensíveis necessitam de uma tutela diferenciada e especial, contudo, a proibição do tratamento destes dados é inviável, em especial se relacionados às relações de trabalho ou emprego, pois, em alguns momentos, o uso de tais dados será legítimo e necessário, por conseguinte, entende-se que o tratamento de dados sensíveis é possível e pode ser necessário em determinadas circunstâncias, porém, deverá ser pautado estritamente nos ditames legais, pela relevância dos valores em questão, e legitimado apenas quando este tratamento não proporcionar realização de discriminações ilícitas ou abusivas.

Consoante afirmam Giroldo e Machado (2020), quando da contratação de um empregado, o legítimo interesse, a necessidade do tratamento de dados para execução do contrato ou o

consentimento do titular se apresentam como as principais bases legais que poderão fundamentar o tratamento dos dados pessoais por parte do empregador. E se for efetuada análise relativa ao tratamento de dados pessoais na vigência do contrato de trabalho, se constata uma maior dificuldade em se justificar atividades de tratamento através da obtenção de consentimento do empregado, haja vista que, em razão da subordinação jurídica, característica inerente à relação empregatícia, a obtenção do consentimento livre, inequívoco e informado, como prevê a legislação, converte-se em um desafio para o empregador, ao passo que o controlador poderá buscar a legitimação da atividade de tratamento de dados pessoais nas demais bases legais elencadas no artigo 7º da LGPD, dentre as quais aquelas que tratam de cumprimento de obrigação legal ou regulatória; para execução de contrato, como porventura se faz necessário para viabilizar fornecimento de benefícios corporativos, como plano de saúde, vale refeição e vale transporte.

Para Santos (2020), nas relações de trabalho o empregado é o titular dos dados e o empregador ocupa a figura de controlador de dados, e, por mais que o consentimento seja dispensado nas hipóteses de execução de contrato ou de procedimentos relacionados a contrato do qual seja parte o titular dos dados do empregado, seu tratamento merece cautela, objetivando não ferir a privacidade do trabalhador, ocasionando danos à imagem, danos de natureza moral, além de prejuízos de ordem material ao empregador.

De acordo com Pamplona Filho e Coni Junior (2020), importa destacar a necessidade da empresa de obter o consentimento dos empregados para cada dado colhido, levando sempre em consideração ser o empregado parte hipossuficiente da relação, e se limitar o uso dos dados para a sua respectiva finalidade, tempo de tratamento e guarda, devendo o funcionário ser informado do destino das suas informações pessoais, acima de tudo diante do heliocêntrico do contrato de emprego, que funciona

como agente de diversos outros contratos, como bancários, convênios médicos, e contábeis, para os quais se torna necessário transferir dados, o empregado deverá conceder seu consentimento para tráfego de seus dados para cada uma dessas relações jurídicas acessórias. A empresa deve, outrossim, estar capacitada para garantir ao empregado o direito ao acesso aos dados e, respectiva confirmação da existência do devido tratamento, a correção de dados ou ainda requerimento da anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados – LGPD, portabilidade dos dados, mediante requisição expressa, o conhecimento das informações que foram compartilhadas para os entes públicos e demais empresas com as quais o empregador mantém vínculo jurídico e tenham tido acesso por algum motivo as informações pessoais dos colaboradores, além do direito à eliminação dos dados pessoais fornecidos, bem como, à revogação do consentimento anteriormente concedido.

Ainda conforme Pamplona Filho e Coni Junior (2020), quanto aos direitos à revogação do consentimento e à eliminação dos dados, estes sofrem limitações, levando em consideração que a empresa está autorizada por lei a se recusar a efetivá-los, ao menos imediatamente, quando esta recusa decorrer de estrito cumprimento de obrigações legais, como no período em que a legislação exigir a guarda pertinente da documentação, e quando decorrentes das imposições legislativas, as empresas poderão manter o arquivamento de documentação dos ex-empregados, durante o prazo prescricional, para apresentação de eventuais defesas em futuros passivos trabalhistas, além da obrigação de guarda de informações para compartilhamento com convênios de saúde em caso de aposentadoria ou desligamento sem justa causa, dentre outras, como demandas de natureza declaratória, imprescritíveis pela própria natureza, como fornecimento de dados para fins previdenciários ou PPP (Perfil Profissiográfico

Previdenciário).

Importa destacar ainda, como bem anotado por Pamplona Filho e Coni Junior (2020), que cabe à empresa o ônus da prova de que o consentimento do empregado foi obtido em conformidade com o disposto na Lei, até porque, geralmente, os contratos de trabalho funcionam como avenças de adesão, onde as condições contratuais são ofertadas ao candidato ao emprego, a quem cabe a decisão livre de optar por as aceitar ou não, todavia, a avaliação da legitimidade de validade do consentimento do empregado se torna imprescindível, uma vez que o atinge na maioria das vezes em momento de maior fragilidade, no qual se encontra desempregado, se adotando, a priori, uma interpretação mais favorável ao aderente.

Não se pode esquecer que, diferentemente do que ocorre em outras relações, como em contratos celebrados na esfera cível, a relação de trabalho está fundada no princípio da proteção e na restrição da autonomia da vontade, o art. 444 da CLT dispõe que:

> As relações contratuais de trabalho podem ser objeto de livre estipulação das partes interessadas em tudo quanto não contravenha às disposições de proteção ao trabalho, aos contratos coletivos que lhes sejam aplicáveis e às decisões das autoridades competentes. (BRASIL, 1943)

Diante disso, Miziara (2021) alerta que tal artigo da Consolidação das Leis do Trabalho – CLT, baseado no princípio da proteção, vai ao encontro do disposto na Lei Geral de Proteção de Dados – LGPD, a fim de salvaguardar os direitos do trabalhador diante da relação assimétrica frente ao empregador, impondo limites e contornos à autonomia privada, estabelecendo lugares que são impenetráveis ao empregador, mesmo que a realidade laboral deseje e admita o controle do empregador a determinados aspectos da rotina laboral, no intuito de aumento da saúde, segurança e produtividade da equipe, deve se impôr limite às entradas abusivas, preservando-se direitos fundamentais como a intimidade e a vida privada, além de proporcionar a

autodeterminação informativa.

Pamplona Filho e Coni Junior (2020) observam que uma das formas de se obter um consentimento válido com maior segurança jurídica seria a regulamentação do tratamento de dados por meio de normas coletivas, tanto mediante realização de acordos diretamente com as empresas, quanto entre os sindicatos, na forma de convenção coletiva de toda a categoria, dado que não há restrição constitucional nem legal neste sentido, e tais instrumentos normativos podem estabelecer critérios e regras que confiram maior segurança aos empregados, pretendendo tutelar o momento da efetivação do consentimento relacionado ao tráfego de dados pessoais ou dos procedimentos a serem seguidos pelas empresas e entidades sindicais para fornecimento de dados dos sindicalizados, conferindo maior eficiência sem abdicar das cautelas inerentes aos direitos da personalidade.

De acordo com Pamplona Filho e Coni Junior (2020) a proteção da LGPD aos empregados se faz presente tanto nas chamadas empresas B2B (Business to Business ou venda entre empresas) como nas B2C (Business to Consumer ou venda para o consumo) as quais terão de se adaptar, especialmente no setor de recursos humanos, já que terá forte impacto no direito do trabalho, e considerando que em muitas empresas os principais destinatários da proteção do banco de dados serão os empregados, portanto, o tratamento de dados no contexto laboral é usualmente feito em favor do empregado, e na defesa dos seus interesses, dessa maneira, uma obrigação do empregador.

Segundo Giroldo e Machado (2020) sendo diversas as informações coletadas ao longo da relação de emprego no Brasil, independentemente da fase contratual, e o tratamento dos dados justificado de formas diversas, inclusive no tocante ao fornecimento de informações a terceiros e à manutenção de informações mesmo após o encerramento do contrato de trabalho, urge a adoção pelos empregadores de regras internas relacionadas à coleta, tratamento e descarte dos dados pessoais e sensíveis que

venham a ser disponibilizados, assim como implantação de medidas de proteção da informação por meio de acessos restritos ou configurações que demandem dupla validação, a fim de evitar o uso inadequado dos dados por operadores buscando desvirtuar a finalidade das informações para benefício próprio.

Em caso de descumprimento do previsto na LGPD, ainda conforme Giroldo e Machado (2020), severas multas poderão ser aplicadas às empresas, podendo, inclusive, inviabilizar o prosseguimento das atividades de empresas no mercado. Observa-se, pois, ser inadiável a implantação de mecanismos que promovam a segurança do ambiente onde os dados coletados estejam armazenados, a adoção de regras que possam assegurar o cumprimento da lei e mitigar riscos relacionados ao tratamento dos dados pessoais, e, ainda que a LGPD não obrigue as empresas a adotarem políticas internas de boas práticas e governança, pode ser uma ótima alternativa para regrar a coleta de dados pela empresa, sendo medida que auxilia a evitar a solicitação de informações que não são necessárias para a formação da relação de emprego, reduzindo as chances de exposição ao risco de questionamento em caso de fiscalização ou de denúncia de trabalhadores aos órgãos de fiscalização. Outra medida está na escolha dos parceiros comerciais, devendo-se exigir destes, políticas internas relacionadas às boas práticas sugeridas na LGPD, idoneidade e comprometido com o cumprimento da legislação. Quanto aos operadores de dados, a fiscalização de suas atividades por meio de monitoramento do uso de ferramentas disponibilizadas para o trabalho e a aplicação de medidas disciplinares em caso de descumprimento das normas internas também são medidas necessárias não só para inibir, mas também para comprovar o compromisso da empresa com a observância dos dispositivos legais.

Conforme disposto na Lei Geral de Proteção de Dados – LGPD, quando o controlador ou o operador, contratados pela organização para execução de tais funções, e no exercício de

atividade de tratamento de dados pessoais, causar a outra pessoa dano patrimonial, moral, individual ou coletivo, violando a legislação de proteção de dados pessoais, é obrigado a reparar o dano, ainda, o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações legais ou quando não tiver seguido as instruções lícitas do controlador, assim como os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados. No entanto, os agentes de tratamento não serão responsabilizados quando provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído, ou que embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados, ou ainda que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (BRASIL, 2018)

Ainda segundo a Lei Geral de Proteção de Dados – LGPD cabe à empresa, por meio dos agentes de tratamento adotar medidas de segurança, técnicas e administrativas a fim 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, devendo o controlador comunicar à autoridade nacional e ao titular a ocorrência de qualquer incidente de segurança que possa acarretar risco ou dano relevante aos seus titulares. Os controladores e operadores poderão, também, formular regras de boas práticas e de governança que estabeleçam as condições de organização, regime de funcionamento, procedimentos, inclusive reclamações e petições de titulares, normas de segurança, padrões técnicos, obrigações específicas para os envolvidos no tratamento, além de ações educativas, mecanismos internos de supervisão e mitigação de riscos. (BRASIL, 2018)

Para Caovilla, Dufloth e Pazine (2019), um dos principais desafios encontrados para a implementação de uma política interna de proteção de dados nas empresas consiste na

dificuldade de conscientização não só do seu corpo diretivo, como também da disseminação da cultura da proteção de dados entre seus colaboradores, clientes, fornecedores e consumidores, sendo, pois, importante que os contratos contenham cláusulas específicas abordando o uso de dados pessoais, destacando sua finalidade, os dados que serão coletados, quem terá acesso a estes, como serão armazenados e, se possível o período de retenção. Deve-se, ainda, fazer uma avaliação periódica dos impactos e dos riscos envolvendo o tratamento de dados pessoais, para que a organização possa estabelecer políticas de ação adequadas para mitigação de riscos e danos ensejados pelo eventual vazamento de dados.

A Lei n 13.709/2018 apresenta, outrossim, sansões administrativas a serem aplicadas em caso de infrações cometidas, jáPamplona Filho e Coni Junior (2020) pontuam que a fiscalização será ostensiva e as sanções administrativas são austeras, portanto, não compensa se aceitar os riscos de se manter à margem do regramento legal, sobretudo diante da possibilidade de massificação de demandas trabalhistas perante Justiça do Trabalho. Deve-se trabalhar, no entanto, na efetivação de um minucioso mapeamento de dados para identificar os riscos que cada empresa está submetida, elaborar termos de uso de serviços, políticas de privacidade, revisão de contratos de trabalho ou prestação de serviços e instrumentos jurídicos utilizados, definir forma de tratar os dados já existentes na organização, elaborar regulamento de *compliance* de dados para garantir a conformidade de procedimentos a serem adotados se observando a nova legislação, definir e contratar, se for o caso, quem desenvolverá atividades de operador e de encarregado, assim como reforçar a cautela no tratamento dos dados em tempos excepcionais, tal como os ora vivenciados por conta da pandemia do *COVID-19*, quando há expressivo trafego de dados e informações inclusive pelos meios digitais, com aumentando da capacidade de vigilância e controle sobre os empregados, colocando-os em situação

de maior fragilidade, notadamente no que diz respeito a dados sensíveis como os ligados à saúde, da mesma forma há de se ter atenção quanto ao trabalho remoto de casa, que demanda maior preocupação ainda com a proteção de dados, segurança no uso de programas, e-mails e aplicativos.

Vencidos os desafios de se implantar uma política para efetivamente aplicar a Lei Geral de Proteção de Dados - LGPD nas empresas, além de cumprimento de dever legal, desonerando-se de incidência de pesadíssimas multas, riscos de responsabilidade civil, e bloqueio ou eliminação dos dados relacionados a uma infração, pode-se aumentar a lucratividade das organizações, já que, conforme Miziara (2021) a organização estará seguindo uma tendência do mercado, agregando valor à marca e à empresa, sendo vista no mercado com maior transparência e detentora de controle de informações. Ainda, como a Lei Geral de Proteção de Dados – LGPD se aplica a todas as empresas que tratam dados pessoais de indivíduos que se encontram em território europeu no momento da coleta ou que ofereçam serviços à sua população, assim como empresas europeias ficam praticamente impedidas de contratar com empresas situadas em países e empresas que não dispõe do nível de proteção adequado, com o cumprimento da exigência mercadológica de se adequar aos ditames da LGPD, há o aumento da competitividade das empresas no cenário internacional, inclusive com maior ingresso de investimentos de capital estrangeiro.

## CONCLUSÃO

Diante do estudo realizado sobre a Lei Geral de Proteção de Dados – LGPD, ficou claro que já não era sem tempo de o Brasil ter uma legislação específica sobre o assunto, sendo inclusive critério para não exclusão do contexto mercadológico mundial, com ênfase no Europeu, mas principalmente para proteger os dados pessoais em toda e qualquer relação.

Insta salientar que entender um pouco mais da referida Lei é fundamental para toda a sociedade, já que impacta a todos indistintamente. Nesse contexto, onde a tutela de proteção de dados tem levantado importantes discussões, não poderia ser diferente com o Direito do Trabalho, já que a proteção dos direitos do trabalhador deve, indubitavelmente, estar pautada pelos direitos fundamentais assentados na Constituição, notadamente na dignidade da pessoa humana, sendo essencial que a proteção de dados se torne tema relevante no que diz respeito à tutela da privacidade do empregado.

Sendo inevitável, principalmente nas relações de emprego, que, em alguma medida, ocorra a coleta e o processamento de dados, ao menos para que se verifique a necessidade, aptidão e adequação, visando buscar a eficiência desejada pelo empresário em implementar programas de *compliance*, sem ferir o direito do trabalhador. Contudo, é preciso que essas definições sejam efetivas, mesmo quando esbarrarem na necessidade de se obter consentimento, que deve ser lido considerando a assimetria que é natural à relação de emprego, para que tutele adequadamente os dados sujeitos a tratamento em diferentes situações.

Desta forma, levando em conta o estudo e análise da Lei nº 13.709/2018, mormente no que pertine às atividades a serem exercidas por todas as organizações, especialmente na seara trabalhista, considerando os direitos tutelados aos titulares de dados pessoais, as obrigações das empresas destinatárias de dados pessoais, especialmente de empregados, e que a fiscalização deverá ser vigorosa, tanto por parte dos titulares dos dados, como por órgãos de proteção aos cidadãos e pela Autoridade Nacional de Proteção de Dados (ANPD), com possibilidade, caso não se respeite os ditames legais, de aplicação de sanções e responsabilização civil, bem como de ingresso de reclamatórias trabalhistas na Justiça do Trabalho, é medida urgente e extremamente necessária, a todas as empresas, a imediata implantação de um sistema de proteção de dados pessoais de acordo com os regramentos da

Lei Geral de Proteção de Dados - LGPD.

Além dos riscos de sanções, urge às empresas a adaptação às novas regras, já que a proteção de dados pessoais passou a ser uma exigência mercadológica, de modo que as empresas que não se adequarem perderão espaço concorrencial, principalmente no mercado internacional.

Portando, há a incontestável necessidade de mudança de cultura e adaptação legal, diante da realidade que se apresenta, em especial para as empresas, ainda, mais especificamente quando diz respeito a dados de seus empregados, para que se evite prejuízos de ordem material e moral. Ademais, em futuros estudos correlatos, com o passar dos anos, pode-se analisar, na prática, se a vigência da Lei Geral de Proteção de Dados – LGPD, realmente teve efetividade.

## REFERÊNCIAS

ACCIOLY, Clara Lacerda. A proteção de dados do trabalhador: O direito do trabalho constitucionalizado e seu diálogo com o direito à privacidade. *Revista Dos Estudantes De Direito Da Universidade De Brasília*. Disponível em: https://periodicos.unb.br/index.php/redunb/article/view/22429/20410. Acesso em 31 jan. 2022.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 07 set. 2021.

BRASIL. *Consolidação das Leis do Trabalho.* Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del5452compilado.htm. Acesso em: 17 out. 2021.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Dispõe sobre

a proteção do consumidor e dá outras providências. Disponível em: . Acesso em: 07 set. 2021.

BRASIL. *Lei nº 9.507, de 12 de novembro de 1997.* Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Disponível em: . Acesso em: 07 set. 2021.

BRASIL. *Lei nº 12.414, de 09 de junho de 2011.* Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: . Acesso em: 07 set. 2021.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011 Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.* Disponível em: . Acesso em: 07 set. 2021.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014.* Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 set. 2021.

BRASIL. *Lei n° 13.709, de 14 de agosto de 2018.* Aprova a 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: 28 jul. 2021.

CAOVILLA, Renato; DUFLOTH, Rodrigo; PAZINE, Letícia. Proteção de dados pessoais: Desafios e impactos práticos para as organizações. *Revista de Direito Recuperacional e Empresa.* Disponível em: https://www.revistadostribunais.com.br/maf/app/favdoc/document?docguid=I52eee2a08f2511e9a59f010000000000. Acesso

em: 03 abr. 2022

DERBLI, Ludimila Santos. O transplante jurídico do Regulamento Geral de Proteção de Dados da União Europeia ("GDPR") para o Direito brasileiro. *Revista Eletrônica do Programa de Pós-graduação da Câmara dos Deputados*, Brasília, v. 12, n. 30, p.181- 193, set./dez. 2019. Disponível em: https://bd.camara.leg.br/bd/handle/bdcamara/39401. Acesso em: 31 jul. 2021.

FACCHINI NETO, Eugênio; DEMOLINER, Karine Silva. *Direito à privacidade na era digital – Uma releitura do art. XII da Declaração Universal dos Direitos Humanos (DUDH) na sociedade do espetáculo.* Disponível em: https://revistaconsinter.com/wp-content/uploads/2020/01/ano-v-numero-ix-direito-a-privacidade-na-era-digital-uma-releitura-do-art-xii-da-declaracao-universal-dos-direitos-humanos-dudh-na-sociedade-do-espetaculo.pdf. Acesso em: 06 nov. 2021.

FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Claudio. Privacidade e Lei Geral de Proteção de Dados Pessoais. *Revista de Direito Brasileira.* Florianópolis, SC. v. 23, n. 9, p. 284-301. Mai./Ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 07 set. 2021.

GIROLDO, Andrea Gardano Bucharles; MACHADO, Daniela Cunha. A proteção da informação no âmbito das relações de emprego e os impactos da aplicação da LGPD aos contratos de trabalho no Brasil. *Revista de Direito e as Novas Tecnologias*. Disponível em: https://www.revistadostribunais.com.br/maf/app/favdoc/document?docguid=Id085fa7048a011eaa7e1dff08190eba6. Acesso em: 03 abr. 2022.

LAMBERTY, Andrey Oliveira; KÜMELL, Marcelo Barroso. A eficácia dos direitos fundamentais nas relações trabalhistas da sociedade informacional: A proteção dos dados

pessoas do empregado na fase pré-contratual. *Revista de Direito Constitucional e Internacional.* Disponível em: https://www.revistadostribunais.com.br/maf/app/favdoc/document?docguid=I97695a2028d111e8b883010000000000. Acesso em: 31 jan. 2022.

LUGATI, L. N.; ALMEIDA, J. E. de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. *Revista de Direito*,*[S. l.]*, v. 12, n. 02, p. 01-33, 2020. DOI: 10.32361/2020120210597. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 6 set. 2021.

MALDONADO, Viviane Nóbrega. A Lei Geral de Proteção de Dados: objeto, âmbito de aplicação, requisito, segurança e a necessidade de sua correta implementação. *Revista dos Tribunais, LGPD Lei Geral de Proteção de Dados Pessoais: Manual de implementação.* Disponível em: https://proview.thomsonreuters.com/title.html?redirect=true&titleKey=rt%2Fmonografias%2F206179087%2Fv1.11&titleStage=F&titleAcct=ia744d7790000015f9191364d13e0e92f#sl=0&eid=71ccc6f93f470c053a79d93244009920&eat=%5Bereid%3D%2271ccc6f93f470c053a79d93244009920%22%5D&pg=RB-1.1&psl=p&nvgS=false. Acesso em: 07 set. 2021.

MIZIARA, Raphael. *Teoria e prática no contexto laboral.* Curso LGPD – Lei Geral de Proteção de Dados. Porto Alegre/RS, mai. 2021. Disponível em: https://ead.trt4.jus.br/course/view.php?id=2400&section=8. Acesso em: 31 maio 2021.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. *Compliance Digital e LGPD*. Volume V 1ª

Edição. 2021. Disponível em : https://proview.thomsonreuters.com/title.html?redirect=true&titleKey=rt%2Fmonografias%2F262297688%2Fv1.3&titleStage=F&titleAcct=ia744d7790000015f9191364d13e0e92f#sl=p&eid=8217aa6461842b0dda8c87fe0d450d0a&eat=%5Bereid%3D%228217aa6461842b0dda8c87fe0d450d0a%22%5D&pg=RB-5.1&psl=&nvgS=false. Acesso em: 07 set. 2021.

PAMPLONA FILHO, Rodolfo; CONI JUNIOR, Vicente Vasconcelos. A Lei Geral de Proteção de Dados Pessoais e seus impactos no Direito do Trabalho. *Direito Unifacs: debate virtual*, Salvador, n. 239, p. 1-42, maio 2020. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/6744/4066. Acesso em: 07 set. 2021.

REQUIÃO, Maurício. *Covid-19 e proteção de dados pessoais: o antes, o agora e o depois.* Disponível em: https://www.conjur.com.br/2020-abr-05/direito-civil-atual-covid-19-protecao-dados-pessoais-antes-agora-depois. Acesso em: 17 out. 2021.

ROCHA, Gustavo. *Compliance Digital e a Lei Geral de Proteção de Dados – LGPD.* Disponível em: https://jus.com.br/artigos/72807/compliance-digital-e-a-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 06 nov. 2021.

SUPERIOR TRIBUNAL DE JUSTIÇA. *Um marco na regulamentação sobre dados pessoais no Brasil.* Disponível em: https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dados-pessoais-lgpd, Acesso em: 25 out. 2021

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *civilistica.com*, v. 9, n. 1, p. 1-38, 9 maio 2020.

Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510/384. Acesso em: 17 out. 2021.