VICTÓRIA TEREZA LARA ROSA

PROTEÇÃO DE DADOS NO CONTEXTO DA RELAÇÃO ENTRE EMPREGADO E EMPREGADOR: ANÁLISE DA APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PELOS TRIBUNAIS REGIONAIS TRABALHISTAS

LAVRAS-MG
2022

VICTÓRIA TEREZA LARA ROSA

PROTEÇÃO DE DADOS NO CONTEXTO DA RELAÇÃO ENTRE EMPREGADO E EMPREGADOR: ANÁLISE DA APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PELOS TRIBUNAIS REGIONAIS TRABALHISTAS

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Lavras – UFLA, como parte das exigências do Curso de Direito para a obtenção do título de Bacharel.

Profa. Dra. Stefania Becattini Vaccaro
Orientadora

LAVRAS-MG
2022

VICTÓRIA TEREZA LARA ROSA

PROTEÇÃO DE DADOS NO CONTEXTO DA RELAÇÃO ENTRE EMPREGADO E EMPREGADOR: ANÁLISE DA APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PELOS TRIBUNAIS REGIONAIS TRABALHISTAS

DATA PROTECTION IN THE CONTEXT OF THE RELATIONSHIP BETWEEN EMPLOYEE AND EMPLOYER: ANALYSIS OF THE APPLICATION OF THE GENERAL DATA PROTECTION LAW BY REGIONAL LABOR COURTS

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Lavras – UFLA, como parte das exigências do Curso de Direito para a obtenção do título de Bacharel.

APROVADO EM: ___ de _____ de 2022.
Profa. Dra. Stefania Becattini Vaccaro – UFLA
Prof. Dr. XX – XX

Profa. Dra. Stefania Becattini Vaccaro
Orientadora

LAVRAS-MG
2022

RESUMO

A Lei Geral de Proteção de Dados, que regulamenta o tratamento de dados pessoais, inaugurou o marco regulatório das informações capazes de identificar pessoas naturais. Porém, a lei não traz nenhum dispositivo específico acerca do tratamento de dados no contexto das relações entre empregado e empregador, o que gera margem para discricionariedade e interpretações divergentes. Por isso, o presente trabalho tem como objetivo analisar as decisões proferidas pelos Tribunais Regionais do Trabalho da Segunda e Terceira Região, discutindo os pontos semelhantes e divergentes. Nesse sentido, foram analisadas 46 decisões do Tribunal Regional do Trabalho da Segunda Região, dentre despachos, sentenças e acórdãos, selecionados através de busca jurisprudencial pela expressão "proteção de dados" realizada no site do respectivo tribunal. Em relação ao Tribunal Regional do Trabalho da Terceira Região, foram analisados 5 acórdãos, uma vez que a ferramenta de busca jurisprudencial do site do tribunal limita a busca a tais decisões. A expressão utilizada também foi "proteção de dados". A partir da análise das decisões, foi possível constatar que a aplicação da LGPD pelos Tribunais Regionais do Trabalho da Segunda e da Terceira Região às controvérsias envolvendo proteção de dados tem sido bastante adequada e ponderosa, alinhada aos princípios do Direito do Trabalho e visando o equilíbrio da relação, sem, contudo, deixar de responsabilizar o empregado pelo tratamento indevido de dados.

Palavras-chave: Proteção de Dados. Privacidade. Empregado. Direito do Trabalho. Decisões.

ABSTRACT

The General Data Protection Law, which regulates the processing of personal data, inaugurated the regulatory framework for information capable of identifying natural persons. However, the law does not contain any specific provision on data processing in the context of employee-employer relations, which creates room for discretion and divergent interpretations. Therefore, the present work aims to analyze the decisions handed down by the Regional Labor Courts of the Second and Third Region, discussing similar and divergent points. In this sense, 46 decisions of the Regional Labor Court of the Second Region were analyzed, among orders, sentences and judgments, selected through a jurisprudential search for the expression "data protection" carried out on the website of the respective court. Regarding the Regional Labor Court of the Third Region, 5 judgments were analyzed, since the jurisprudential search tool on the court's website limits the search to such decisions. The expression used was also “data protection”. From the analysis of the decisions, it was possible to verify that the application of the LGPD by the Regional Labor Courts of the Second and Third Region to disputes involving data protection has been quite adequate and powerful, in line with the principles of Labor Law and aiming at the balance of the relationship, without, however, failing to hold the employee responsible for the improper treatment of data.

Keywords: Data Protection. Privacy. Employee. Labor Law. decisions.

SUMÁRIO

1 INTRODUÇÃO

Com o passar do tempo, o avanço tecnológico acelerado ocasionou grandes mudanças na sociedade e na forma com que as atividades econômicas se organizam. Atualmente, a circulação em massa de informações assume papel crucial na ordem mercadológica, de forma que os dados se tornaram ativos de grande valor. De posse de informações específicas sobre a população, empresas e governos podem mudar completamente o curso de suas ações para que sejam mais assertivas e atinjam determinados objetivos com mais facilidade.

Diante da importância que os dados pessoais assumiram na sociedade, foi preciso regular o tratamento destes, de modo a garantir a devida privacidade aos seus titulares. Nesse contexto, o Brasil promulgou, em 2018, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13079 de 14 de agosto de 2018, que regulamenta o tratamento de dados de pessoas físicas, inclusive no meio digital, realizado por pessoas físicas ou jurídicas de direito público ou privado para fins econômicos e não particulares.

Neste ponto, insta esclarecer que o termo tratamento é aqui entendido como toda e qualquer operação que envolva dados pessoais, os quais, por sua vez, são entendidos como informação relacionada a pessoa natural identificada ou identificável.

Verifica-se que desde a promulgação da LGPD, o tema vem ganhando bastante relevância no mudo jurídico e renova o debate sobre os limites jurídicos de proteção de dados pessoais consagrados, no art. 5º, XI, da Constituição Federal de 1988 como direito fundamental. Dentre os questionamentos que surgiram neste cenário, destacam-se: a possível violação de dados de clientes pelo empregador e a utilização de dados sensíveis do empregado pelo empregador, os quais serão objeto de análise neste artigo.

A elevação a status constitucional do direito à proteção de dados e a relevância do tema, por si só, elevam as exigências por um tratamento adequado às violações de tal direito. A inclusão da proteção de dados como um direito expresso no rol do artigo 5º da Constituição garante visibilidade ao tema e traz reflexos na análise e aplicabilidade do Código de Defesa do Consumidor, da Lei do Cadastro Positivo, da Lei de Acesso à Informação, do Marco Civil da Internet e, não menos importante, da Consolidação das Leis do Trabalho (CLT). Nas palavras de Pietro Perlingiere (2002):

> A normativa constitucional não deve ser considerada sempre e somente como mera regra hermenêutica, mas também como norma de comportamento, idônea a incidir sobre o conteúdo das relações entre situações objetivas, funcionalizando-as aos novos valores. (PERLINGIERE, 2002, p. 12).

Na seara do trabalho esse debate ganha cores ainda mais intensas porque a relação entre empregado e empregador envolve e exige o tratamento de uma enorme quantidade de dados pessoais desde a fase pré-contratual até a pós-contratual. Com efeito, todas essas fases precisam estar de acordo com os dispositivos da LGPD para assegurar a proteção aos direitos da personalidade do empregado e, também, para resguardar o empregador de possíveis responsabilizações.

Ocorre, porém, que o regramento de dados brasileiro se caracteriza pela sua generalidade e não há, no texto da lei, nenhuma menção expressa aos dados dos trabalhadores, o que gera certa discricionariedade na sua aplicação. Nesse sentido, afirma Vólia Bonfim (2020):

> [...] a lei brasileira não contempla expressa disposição sobre o direito do trabalho, mas sua incidência a ele é irrefutável, pois a relação de trabalho sequer teria como se iniciar e desenvolver sem a coleta, recepção, armazenamento e retenção de dados pessoais dos empregados ou candidatos a empregos. Importante destacar que o elevado fluxo de dados nas relações de trabalho assume grandes proporções e atrai especial atenção sobre a questão, uma vez que o empregador, desde a fase pré-contratual (processos seletivos e admissão), passando pela fase contratual e chegando até a fase pós-contratual, tem acesso e se torna responsável pelo armazenamento e guarda de dados pessoais dos trabalhadores. (BONFIM, 2020, p. 2).

Assim, buscou-se realizar uma pesquisa no âmbito dos Tribunais Regionais do Trabalho da Segunda e da Terceira região, que representam os estados de São Paulo e Minas Gerais, respectivamente, para verificar como essas instâncias vêm decidindo as controvérsias envolvendo a proteção de dados dos sujeitos envolvidos na atividade do empregador, sejam eles clientes ou funcionários, com o intuito de verificar a existência de certo padrão de argumentação e tendência de posicionamento.

A escolha de tais tribunais leva em consideração o elevado desenvolvimento econômico dos estados de São Paulo e Minas Gerais e o polo empresarial localizado no Sudeste do Brasil. Como a região concentra população e renda, depreende-se que o volume e a complexidade das relações de emprego objetos de controvérsias no judiciário é maior. Portanto, o estudo das decisões proferidas pelos Tribunais Regionais do Trabalho da Segunda e Terceira Região envolvendo a proteção de dados de trabalhadores se fez mais relevante se comparado aos demais tribunais, tanto pelo volume de decisões a serem analisadas, quanto pela complexidade das controvérsias nelas presentes.

Neste sentido, foram analisadas 46 decisões do Tribunal Regional do Trabalho da Segunda Região, dentre despachos, sentenças e acórdãos, selecionados através de busca jurisprudencial pela expressão “proteção de dados” realizada no site do respectivo tribunal.

Em relação ao Tribunal Regional do Trabalho da Terceira Região, foram analisados 5 acórdãos, uma vez que a ferramenta de busca jurisprudencial do site do tribunal limita a busca a tais decisões. A expressão utilizada também foi “proteção de dados”.

A partir da análise das decisões, observou-se semelhanças nas temáticas envolvendo a relação trabalhista e proteção de dados: demissão por justa causa, dano moral e compartilhamento de geolocalização, as quais serão melhor analisadas no decorrer do trabalho.

Antes de passarmos à análise temáticas semelhantes abordadas nas decisões estudadas, mister se faz a apresentação da Lei Geral de Proteção de Dados e de seus fundamentos e principais conceitos, visando possibilitar a discussão da sua aplicação às relações de trabalho.

2 REFERENCIAL TEÓRICO

2.1 Limites normativos da lei geral de proteção de dados

Conforme já apresentado, a Lei n° 13.79/2018, conhecida como Lei Geral de Proteção de Dados (LGPD) regulamenta o tratamento de dados de pessoas físicas, inclusive no meio digital, realizado por pessoas físicas ou jurídicas de direito público ou privado para fins econômicos e não particulares. Sua promulgação representou um marco regulatório da utilização de dados, pois, além de delimitar as hipóteses legítimas de uso e estabelecer as sanções para seu descumprimento, esclarece conceitos que balizam, norteiam e organizam toda relação que envolve o tratamento de dados pessoais. Alguns desses conceitos, que são fundamentais para compreender a lógica da Lei Geral de Proteção de Dados e sua aplicação no contexto trabalhista, serão abordados a seguir:

2.2 Dado pessoal e seu titular

Nos termos do artigo 5°, inciso I da Lei Geral de Proteção de Dados, o dado pessoal compreende toda a informação relacionada a pessoa natural identificada ou identificável. Assim, a lei tem por objeto a proteção do dado capaz de identificar seu titular, ou seja, nem todo dado ou informação é considerado dado pessoal e, portanto, não estará no escopo de aplicação da LGPD.

Compreende-se que o dado pessoal carrega informações acerca do titular capazes de identificá-lo e distingui-lo entre outros pares. Nesse sentido, posiciona-se Doneda:

> Determinada informação pode possuir um vínculo objetivo com uma pessoa, revelando algo sobre ela. Este vínculo significa que a informação se refere às

> características ou ações desta pessoa, que podem ser atribuídas a ela em conformidade à lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como sobre opiniões que manifesta e tantas outras. É importante estabelecer esse vínculo é objetivo, pois ele afasta outras categorias de informações que, embora também possam ter alguma relação com uma pessoa, não seriam propriamente informações pessoais: as opiniões alheias sobre esta pessoa, por exemplo, a princípio não possuem esse vínculo objetivo; também a produção intelectual de uma pessoa, em si considerada, não é per se informação pessoal (embora o fato de sua autoria o seja). (DONEDA, 2011, p. 93).

Nessa seara, é indispensável definir, também, o conceito que a lei traz para titular. Segundo o inciso V do já citado artigo 5°, titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Portanto, dado pessoal e titular são conceitos interdependentes: se não houver um titular identificado ou identificável, o dado não é pessoal, ocasião em que não se aplica a LGPD.

Assumindo, então, que dado pessoal é toda e qualquer informação capaz de identificar uma pessoa natural, tem-se que o conceito legal é extremamente amplo. O mesmo tipo de informação pode ou não ser considerado um dado pessoal a depender do contexto em que é analisado, podendo assumir diferentes contornos de acordo com o caso concreto.

Um exemplo bastante citado por juristas especializados em proteção de dados é a situação em que a calota de um carro se caracterizou como dado pessoal quando foi possível identificar o dono do veículo através do reconhecimento da calota, que tinha aspectos bastante peculiares. Usualmente, não se imaginaria que a informação de um objeto tão inusitado poderia assumir tal papel. Porém, quando os satélites de geolocalização do “Google Earth” capturaram imagens do carro cujas calotas são inconfundíveis, a esposa do dono do veículo foi capaz de identificá-lo na casa de uma amante.

Assim, é necessário recorrer à análise contextual e circunstancial do caso concreto para definir, de fato e com precisão, se a informação se trata ou não de um dado pessoal.

2.3 Dado Pessoal Sensível

Diante da definição de dado pessoal delimitada acima, a LGPD estabelece uma categoria de dados pessoais que merece proteção especial por identificar aspectos específicos da personalidade do titular. Nos termos do artigo 5°, inciso II da lei, 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, genético ou biométrico, quando vinculado a uma pessoa natural.

Em razão da natureza particular do dado pessoal sensível, ele requer maior proteção legal, visto que o seu tratamento inadequado possui maior potencial de causar a discriminação e dano grave ao titular. Nesse sentido, deve-se observar pressupostos e regras diferentes definidas na LGPD para a sua utilização.

Assim, o tratamento adequado e legal dos dados pessoais sensíveis do titular é essencial para as garantias de seus direitos da personalidade. Conforme Mulholland,

> A tutela jurídica de dados pessoais como um corolário do direito à privacidade (ou do direito à identidade) nos leva a considerar que a autodeterminação informativa, ou o poder de controle sobre os próprios dados, deve ser a tônica quando buscamos a proteção específica dos dados sensíveis, especialmente se tais dados podem gerar tratamentos desiguais. O reconhecimento do direito fundamental à igualdade no artigo 5º, caput, da Constituição Federal tutela também o direito ao tratamento sem distinções de qualquer natureza. Ao mesmo tempo, dentre os objetivos fundamentais da República Federativa do Brasil, constantes do artigo 3º, da Constituição Federal, está o de "promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação". Soma-se ao reconhecimento constitucional da proteção da igualdade e da não discriminação, a previsão na LGPD da impossibilidade do tratamento para fins discriminatórios ilícitos ou abusivos. (MULHOLLAND 2018, p. 175).

2.4 Agentes de Tratamento de Dados Pessoais

A Lei Geral de Proteção de Dados estabelece, no inciso XI do artigo 5°, que são agentes de tratamento o controlador e o operador. O controlador, definido no inciso VI do mesmo artigo, é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O conceito possui elevada importância prática, uma vez que a LGPD atribui obrigações específicas ao controlador, além de imputar-lhe responsabilidades em relação à reparação por danos decorrentes de atos ilícitos, conforme o disposto nos arts. 42 a 45.

Já o conceito de operador está regulamentado no inciso VII do artigo 5° da lei como pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. A previsão implica dizer que o operador só poderá tratar os dados para a finalidade previamente estabelecida pelo controlador, o que demonstra a principal diferença entre os dois agentes: o poder de decisão. O operador só pode agir no limite das finalidades determinadas pelo controlador.

A Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal cujas atribuições, definidas no artigo 55-J da LGPD englobam a elaboração de estudos sobre as práticas proteção de dados pessoais e privacidade, publicou em 2021 um Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Esse estudo visa estabelecer diretrizes não-vinculantes aos agentes de tratamento e explicar quem pode exercer tais funções, bem como discutir as definições legais e os respectivos regimes de responsabilidade.

No Guia, a ANPD estabelece que os agentes de tratamento devem ser definidos a partir de seu caráter institucional. Não são considerados controladores ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento. No contexto de uma pessoa jurídica, a própria organização é o agente de tratamento para os fins da LGPD, já que é esta que estabelece as regras para o tratamento de dados pessoais, a serem executadas por seus representantes ou prepostos. Portanto, as três figuras não se confundem: o controlador agirá em seu interesse e determinará as diretrizes para tratamento dos dados pessoais pelo operador, que agirá nos interesses do controlador e deverá sempre ser uma pessoa externa, não subordinada a ele. Os funcionários, por outro lado, atuarão em subordinação às decisões do controlador e em seu nome, figurando apenas como um representante aos olhos da LGPD.

Como exemplo, o Guia traz a seguinte situação prática: uma empresa decide enviar propagandas aos seus clientes com a finalidade de alavancar as vendas de determinado produto. Para isso, contrata agência de publicidade, que elaborará a campanha de marketing com fotos de pessoas utilizando o produto. A empresa informa todos os critérios para a campanha, tais como o público-alvo e estabelece os critérios de como deve ser a aparência física dos modelos fotográficos. A agência de publicidade trata dados pessoais para prestar o serviço para a empresa, ao selecionar modelos fotográficos e armazenar as fotos desses titulares. Após a conclusão do serviço pela agência, o funcionário da empresa envia as propagandas aos clientes.

Neste exemplo a empresa atua como controlador, ao determinar o tratamento de dados e definir os seus elementos essenciais. A agência de publicidade atua como operadora ao tratar dados conforme a finalidade definida pelo controlador. E o funcionário, ao enviar os e-mails para os clientes, atua sob o poder diretivo da empresa e não se caracteriza como agente de tratamento.

Tal distinção é extremamente importante para o presente trabalho, uma vez que, no contexto abordado, o empregado será titular de dados ou representante do controlador no tratamento de dados, mas nunca agente de tratamento passível de responsabilização pela LGPD.

No que tange a responsabilidade dos agentes de tratamento, o Guia leciona que a responsabilidade solidária entre controlador e operador estabelecida pelo inciso I, § 1º do artigo 42 da LGPD, prevista para os casos de danos causados em razão do tratamento irregular realizado por operador (por descumprir as obrigações da legislação ou por não observar as instruções do controlador), é considerada como uma excepcionalidade, já que em regra a responsabilidade é do controlador.

2.5 Princípios

Assim como toda norma jurídica, a Lei Geral de Proteção de Dados é baseada em um conjunto de princípios, que dão sustentação, orientação e norte para aplicação dos seus dispositivos legais. Conforme o artigo 6° da lei:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL, 2018).

Dessa forma, toda a operação de tratamento de dados pessoais deve observar o disposto neste artigo, de forma a proporcionar ao titular dos dados a devida privacidade, segurança e proteção.

Dentre os princípios essenciais, destaca-se a finalidade, a adequação e a necessidade, os quais merecem ser analisados com mais atenção.

De acordo com o princípio da finalidade, toda atividade que envolva o tratamento de dados pessoais deve estar obrigatoriamente atrelada a um fim, sendo que a definição do propósito deve ser definida pelo responsável por tomar as decisões relacionadas ao tratamento, o controlador, nos termos da lei. Além disso, as finalidades definidas devem ser sempre legítimas e específicas, não podendo ser elencados propósitos que sejam genéricos ou que estejam em desconformidade com a legislação.

Já o princípio da adequação estabelece que o tratamento deve ser realizado de forma compatível com as finalidades definidas pelo controlador e informadas ao titular.

De forma correlata, o princípio da necessidade, também conhecido como princípio da minimização, proíbe que o tratamento de dados pessoais ultrapasse o estritamente necessário para que se atinjam as finalidades definidas, sendo ilícita, portanto, a utilização de mais dados pessoais que os necessários para os fins definidos pelo controlador.

A observação dos princípios na aplicação da lei, sobretudo os elencados acima, é fundamental para assegurar a proteção integral do titular dos dados e a segurança no tratamento, uma vez que é impossível prever taxativamente reações jurídicas para todas as controvérsias que eventualmente surgirem.

Especial é a aplicação dos princípios da LGPD no presente trabalho, pois, conforme já ressaltado, não há dispositivos específicos regulamentando o tratamento de dados pessoais na relação trabalhista, de forma que seus preceitos foram citados e utilizados como fundamento para várias das decisões analisadas.

2.6 Bases Legais de Tratamento

Na sistemática da LGPD, o tratamento de dados pessoais somente pode ser realizado se houver fundamento jurídico que o autorize. Este fundamento jurídico é comumente chamado pelos estudiosos do tema de base legal de tratamento.

Toda atividade de tratamento deve estar respaldada por uma base legal, sendo que a identificação do fundamento adequado a cada caso cabe sempre ao controlador. Além disso,

não se deve eleger mais de uma base legal para uma mesma atividade, sob pena de se caracterizar desconformidade em relação à sistemática legal.

Assim, a todo tratamento de dados realizado deve corresponder, além de uma finalidade específica, uma base legal correspondente que o legitime.

Os dados pessoais não sensíveis cujos titulares não sejam crianças ou adolescentes podem ser tratados com fundamento em dez bases legais distintas, cada uma delas elencadas em um dos incisos do art. 7º da LGPD. Já o art. 11 prevê as hipóteses de tratamento de dados pessoais sensíveis, que, conforme já explicitado, são mais restritas e rigorosas.

Tanto nos casos abrangidos pelo art. 7° quanto nos abrangidos pelo art. 11, não há hierarquia entre as diversas bases legais, sendo que, dentro do âmbito de aplicação de cada um dos artigos, o controlador poderá escolher a base legal que lhe for mais conveniente, desde que, é claro, seja efetivamente aplicável ao caso concreto.

3 ANÁLISE DAS DECISÕES DOS TRIBUNAIS

Diante dos conceitos e definições preliminares acima esclarecidos, passa-se à exposição e discussão das temáticas semelhantes encontradas nas decisões do Tribunal Regional do Trabalho da Segunda e Terceira Região envolvendo proteção de dados estudadas.

3.1 Demissão por Justa Causa

A primeira controvérsia que surge acerca da aplicação da Lei Geral de Proteção de Dados à relação trabalhista diz respeito ao dever de sigilo pelos empregados de dados do negócio em que está envolvido, especialmente relativos ao cliente. Os limites jurídicos a serem observados pelo empregado e pelo empregador na aplicação das sanções baseadas no poder diretivo têm sido objeto de análise dos Tribunais, especificamente no que tange a demissão por justa causa.

O Decreto Lei n° 5.452 de 1° de maio de 1943, conhecido como Consolidação das Leis do Trabalho (CLT) estabelece, em seu artigo 482, as condutas praticadas pelo empregado que podem ocasionar sua demissão por justa causa. São elas: a) ato de improbidade; b) incontinência de conduta ou mau procedimento; c) negociação habitual por conta própria ou alheia sem permissão do empregador, e quando constituir ato de concorrência à empresa para a qual trabalha o empregado, ou for prejudicial ao serviço; d) condenação criminal do empregado, passada em julgado, caso não tenha havido suspensão da execução da pena; e) desídia no

desempenho das respectivas funções; f) embriaguez habitual ou em serviço; g) violação de segredo da empresa; h) ato de indisciplina ou de insubordinação; i) abandono de emprego; j) ato lesivo da honra ou da boa fama praticado no serviço contra qualquer pessoa, ou ofensas físicas, nas mesmas condições, salvo em caso de legítima defesa, própria ou de outrem; k) ato lesivo da honra ou da boa fama ou ofensas físicas praticadas contra o empregador e superiores hierárquicos, salvo em caso de legítima defesa, própria ou de outrem; l) prática constante de jogos de azar; m) perda da habilitação ou dos requisitos estabelecidos em lei para o exercício da profissão, em decorrência de conduta dolosa do empregado; além da prática de atos atentatórios à seguridade nacional devidamente comprovada em inquérito administrativo, disposta no parágrafo único do referido artigo.

A justa causa, nas palavras de Maurício Godinho Delgado (2016):

> é o motivo relevante, previsto legalmente, que autoriza a resolução do contrato de trabalho por culpa do sujeito contratual comitente da infração. Trata-se, pois, da conduta tipificada em lei que autoriza a resolução do contrato de trabalho por culpa da parte comitente da infração – no caso, o empregado. Trata-se, pois, da conduta tipificada em lei que autoriza a resolução do contrato de trabalho por culpa do trabalhador. (DELGADO, 2016, p. 1.320).

A justa causa é um instituto altamente prejudicial ao empregado, não só no aspecto moral, mas, sobretudo, no aspecto patrimonial. Uma vez caracterizada, o empregado terá direito apenas a saldo de salários e férias vencidas, não recebendo indenização (se estável), aviso prévio e 13º salário. Além disso, o empregado não poderá levantar imediatamente o Fundo de Garantia do Tempo de Serviço – FGTS. Por isso, sua incidência deve ser precisa e robustamente comprovada pelo empregador, de forma a não causar prejuízos injustos ao trabalhador.

Das 46 decisões do Tribunal Regional do Trabalho da Segunda Região analisadas, 7 versavam sobre demissão por justa causa de empregados que, por ato de indisciplina e insubordinação, utilizaram dados pessoais dos sujeitos envolvidos na atividade do empregador de forma indevida, aumentando a possibilidade de violações do segredo da empresa. No Tribunal da Terceira Região, o caso se repetiu em um dos 5 acórdãos estudados.

Atos de insubordinação e de indisciplina são caracterizados pela desobediência de ordens gerais de serviço contidas em documentos de instrução da empresa, ou o descumprimento de ordens legais, pessoais e diretas feitas pelo empregador. A violação do segredo da empresa, que ocorreu em alguns processos analisados, diz respeito à prática de ato que implica divulgação pelo empregado de bem corpóreo ou incorpóreo de uso ou conhecimento exclusivo da empresa sem autorização desta. Assim, não é necessário que a

conduta do empregado enseje, necessariamente, prejuízo à organização, pois a mera inobservância de ordens legais já caracteriza a justa causa.

As decisões analisadas foram proferidas no contexto de reclamações trabalhistas que visavam a reversão da demissão por justa causa para dispensa imotivada, modalidade em que o contrato de trabalho é extinto sem culpa do empregado, e o recebimento das verbas devidas, as quais seriam excluídas na modalidade justa causa. O pedido do empregado reclamante foi julgado procedente em apenas uma sentença, de forma que todas as decisões proferidas em segundo grau de jurisdição (3 decisões) mantiveram a demissão por justa causa.

O envio de dados pessoais dos envolvidos nas atividades da empresa utilizando meio diverso ao e-mail corporativo foi conduta que se repetiu em 4 das 8 decisões, revelando uma tendência de comportamento indevido por parte dos trabalhadores que merece ser analisada.

Diferentemente da conta de e-mail de uso pessoal, o correio eletrônico corporativo é a conta de uso privativo de determinada pessoa jurídica, criada com a finalidade exclusiva de atender as necessidades da empresa. Logo, quem detém a titularidade da conta é a própria empresa, que é responsável pela manutenção dos dados veiculados através do meio de comunicação, tratando-se de um instrumento de trabalho posto à disposição do empregado para o exercício da atividade laboral em nome da empresa.

Ressalvadas divergências doutrinárias, a corrente majoritária entende que o e-mail corporativo, por ser de titularidade do empregador, está sujeito ao seu controle, vigilância e fiscalização. Assim, o uso dessa ferramenta no cotidiano da organização visa a possibilitar que o empregador acesse as informações que circulam, facilitando o exercício de seu poder diretivo, desde que previamente acordado e explicitado. Nesse sentido, Rúbia Zanotelli de Alvarenga (2010) afirma que:

> Quando o e-mail for corporativo, por se tratar de uma ferramenta de trabalho, porque destinado à realização do serviço, será possível ao empregador acessar o conteúdo material do mesmo por meio de rastreamento, desde que haja prévia comunicação ao empregado da fiscalização no regulamento da empresa e desde que não o faça de forma abusiva. (ALVARENGA, 2010).

Em contrapartida, o acesso pela empresa a dados veiculados através do correio eletrônico de uso particular do trabalhador poderia configurar abuso do poder diretivo do empregador, pois violaria o direito à privacidade do empregado. Portanto, a exigência de utilização de e-mail corporativo no ambiente de trabalho e para a circulação de informações da empresa e dos envolvidos em sua atividade se dá em razão da impossibilidade de controle do e-mail privado do empregado, de forma que seria possível a divulgação de dados pessoais de terceiros sem o conhecimento da empresa.

Em todas as decisões analisadas, o magistrado que as proferiu acusou a violação de princípios da Lei Geral de Proteção de Dados pelo trabalhador que enviou dados pessoais de envolvidos na atividade da empresa utilizando meio diverso ao e-mail corporativo. Tais princípios, dispostos no artigo 6° da lei, norteiam o tratamento de dados pessoais de acordo com a boa fé e a legítima expectativa dos titulares.

Os princípios da finalidade e da adequação, norteadores da aplicação dos dispositivos da LGPD e indispensáveis à segurança do titular, determinam que o tratamento de dados deve condizer com aquele informado ao titular e possuir propósitos legítimos, excluindo a possibilidade de utilização dos mesmos dados para outro fim sem consentimento do titular. De forma complementar, o princípio da necessidade determina que o tratamento de dados deve ser mínimo e se limitar ao necessário ao atingimento da finalidade elencada.

Os sujeitos envolvidos nas atividades da empresa, sejam eles colaboradores ou clientes, fornecem seus dados pessoais com finalidade específica que, certamente, não envolve o compartilhamento com outros empregados através de seus e-mails pessoais, meio não sujeito ao controle do empregador. Ainda, o uso de correio eletrônico ou outro meio de comunicação particular não é necessário ao atingimento dos objetivos da atividade. A conduta em questão coloca as informações em risco de exposição, as quais poderiam ser facilmente enviadas a terceiros sem o conhecimento da empresa. Portanto, houve, de fato, violação aos princípios da Lei Geral de Proteção de Dados, o que, mesmo que não cause prejuízos à empresa, é motivo legítimo para caracterização da demissão por justa causa.

Conforme já discutido anteriormente, os trabalhadores que agem em nome do controlador não podem ser responsabilizados nos termos da LGPD, visto que não são agentes de tratamento, mas apenas representantes subordinados. Porém, isso não significa que eventuais descumprimentos da lei por empregados do controlador, sendo devida e prudente a aplicação das sanções impostas na Consolidação das Leis Trabalhistas (CLT).

3.2 Dano Moral

Como já estudado, a Lei Geral de Proteção de Dados visa regular o tratamento de dados pessoais, de forma a estabelecer as diretrizes para proteção da privacidade do titular. Em razão da sua natureza, a relação de emprego exige que o empregador tenha acesso e armazene uma grande quantidade de dados do empregado, inclusive por determinação legal.

O artigo 7° da referida lei estabelece as hipóteses em que o controlador, pessoa a quem competem as decisões referentes ao tratamento de dados pessoais, é autorizado a tratar dados

dos titulares. São as chamadas bases legais, já abordadas previamente. Nas relações de emprego, nas quais o empregador figura como controlador, a grande maioria dos dados dos trabalhadores são tratados para cumprir determinações legais ou para possibilitar o cumprimento do contrato de trabalho.

Porém, o fato de o empregador estar autorizado a tratar dados do empregado não o desobriga de observar os deveres de cuidado estabelecidos pela LGPD. De acordo com o artigo 42 da Lei, o controlador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Tal dispositivo encontra respaldo em regras elementares de responsabilidade civil, particularmente o caput do art. 927 do Código Civil, e também vai de encontro ao estabelecido na CLT. A Lei nº 13.467/2017 (Reforma Trabalhista) trouxe um regramento específico ao dano moral sofrido pelo trabalhador, tratado em seu artigo 233-B como dano extrapatrimonial. Objeto de relevante discussão doutrinária, a reparação ao dano extrapatrimonial submete-se a regras que restringem os bens jurídicos protegidos e fixam limites ao valor das indenizações. As especificações do dano extrapatrimonial não serão objeto de estudo e crítica no presente artigo, especialmente porque não foram citadas nas decisões analisadas e fogem ao objetivo do trabalho.

Três das 51 decisões analisadas se tratavam de pedidos de indenização por dano moral sofrido pelo empregado em razão de tratamento indevido de seus dados pelo empregador. Nas três, o magistrado reconheceu a existência do dano e imputou ao empregador a obrigação de indenizar os prejuízos morais causados.

Das decisões citadas, duas foram proferidas por magistrados do Tribunal Regional do Trabalho da Segunda Região, das quais uma versava sobre divulgação de dados sensíveis do empregado, que ocasionou descriminação e desrespeito por parte dos dos demais trabalhadores. Como já visto, s dados sensíveis revelam aspectos específicos da personalidade do titular que, quando tratados indevidamente, geram maior probabilidade de exposição, discriminação e dano.

No processo em análise, o reclamante teve sua condição de portador do vírus HIV divulgada por superior e, após tal fato, passou a sofrer discriminação, constrangimento e humilhação. As ofensas não ficaram restritas ao estado de saúde do empregado, mas versavam também sobre especulações a respeito de sua orientação sexual.

De fato, o empregador tem legitimidade para tratar dados de saúde do empregado, uma vez que são necessários para cumprimento de obrigações legais e para o regular cumprimento

do contrato de trabalho, obedecendo ao disposto no inciso II do artigo 7° da Lei Geral de Proteção de Dados. Porém, a exposição de tais dados a terceiros extrapola a finalidade com as quais foram coletados e viola a privacidade de seu titular, ferindo diversos princípios da LGPD. A gravidade do tratamento indevido de dados pessoais sensíveis é evidente, uma vez que atinge os aspectos mais individuais da personalidade do indivíduo, que o caracterizam como seres humanos únicos e singular, ferindo sua honra e dignidade. Assim, a exposição pública de um dado sensível do trabalhador é ainda mais gravosa quando comparada à divulgação de um dado comum, visto que, além de a legislação atribuir-lhe proteção especial, sua própria natureza já demanda maiores cuidados em razão de sua delicadeza e particularidade.

Diante da gravidade da conduta do empregador, o magistrado considerou, na sentença condenatória, "presumíveis os constrangimentos sérios e juridicamente tutelados (aflição, ansiedade, sofrimento mental, angústia, desequilíbrio no bem-estar, autoaceitação e violação da autoestima) sofridos pelo reclamante em razão da divulgação de um dado sensível entre outros empregados" (processo n°1000203-67.2021.5.02.0473, TRT 2), situação que se repetiu nas outras duas decisões analisadas.

O dano moral presumido, também chamado de dano moral *in re ipsa*, assume que não é necessário provar a existência de prejuízos à moral da vítima do dano, de forma que a mera comprovação da existência de violação a direitos da personalidade já enseja o dever de indenizar. Assim, torna-se menos oneroso a sua caracterização, do ponto de vista probatório e processual. A vítima de um dano moral considerado pelos tribunais como "in re ipsa" tem certeza que terá pedido de indenização procedente, o que torna a responsabilização quase que imediata do agente causador.

Sobre isso, esclarece Carlos Roberto Gonçalves:

> O dano moral, salvo casos especiais, como o de inadimplemento contratual, por exemplo, em que se faz mister a prova da perturbação da esfera anímica do lesado, dispensa prova em concreto, pois se passa no interior da personalidade e existe in re ipsa. Trata-se de presunção absoluta. Desse modo, não precisa a mãe comprovar que sentiu a morte do filho; ou o agravado em sua honra demonstrar em juízo que sentiu a lesão; ou o autor provar que ficou vexado com a não inserção de seu nome no uso público da obra, e assim por diante. (GONÇALVES, 2012, p. 353).

A doutrina diverge bastante a respeito da caracterização do dano moral presumido. Há autores que defendem que toda e qualquer lesão a direitos da personalidade do indivíduo, que afetem a honra, a dignidade e a moralidade do indivíduo geram o dever de indenizar independentemente da comprovação do dano sofrido.

Adotando esse posicionamento, o dano moral advindo do tratamento inadequado de dados pessoais seria, de fato, *in re ipsa*, já que atinge a privacidade dos titulares, que é uma das espécies do gênero direitos da personalidade, previsto no artigo 21 do Código Civil Brasileiro, que trata da vida privada, bem como no artigo 5°, inciso X da Constituição Federal, que garante o direito à intimidade e à vida privada como direito fundamental (BRASIL, 1988).

Porém, o que se verifica, de fato, é que a dispensa de provas do efetivo prejuízo psíquico sofrido pela vítima de um dano para a concessão de indenização vem sendo definida de acordo com critérios jurisprudenciais. Da análise de decisões realizada por possível depreender que a existe tendência de formação de um padrão de entendimento nos tribunais regionais estudados que considera presumido o dano moral causado ao empregado em virtude da violação de seus dados pessoais por parte do empregador.

Tal entendimento verifica-se adequado, visto que contribui para efetivação dos direitos dos trabalhadores, uma vez que coíbe a prática de abusos por parte do empregador, além de reforçar ainda mais o dever de cuidado no tratamento de dados pessoais. É cediço que, na relação de emprego, o trabalhador ocupa posição inferior em relação ao empregador, o que deve ser sempre levado em consideração na análise de controvérsias judiciais e, nesse caso, a flexibilização probatória contribui bastante para o equilíbrio da relação e coibir abusos.

3.3 Compartilhamento de geolocalização

Em uma definição básica, geolocalização consiste na utilização de recursos tecnológicos para fazer o rastreamento de um dispositivo por meio de uma conexão remota. Essa conectividade varia entre três métodos: GPS (sistema de posicionamento geográfico), GSM (sistema global para comunicações móveis) e wireless (redes sem fio, como Wi-Fi).

Dentre esses métodos, tomamos como análise o mais popular deles, o GPS. Tal tecnologia tem como base de conexão satélites em órbita da Terra que permitem, através da triangulação de antenas, localizar qualquer ponto no planeta capaz de emitir e captar sinal. A tecnologia GPS é comumente utilizada em smartphones, computadores portáteis, automóveis e até mesmo em transportes públicos, com o fim de garantir a segurança dos usuários e a identificação do aparelho/veículo.

Em três das decisões analisadas, a instituição empregadora reclamada solicitou autorização judicial para acessar a geolocalização do aparelho celular do empregado reclamante com o fim de comprovar sua jornada de trabalho.

Porém, a utilização da geolocalização do usuário por meio de seu dispositivo eletrônico se concretiza como tratamento de um dado pessoal à luz da Lei Geral de Proteção de Dados.

Conforme já explicitado, a lei considera dado pessoal qualquer informação relacionada a pessoa natural identificada ou identificável, podendo assumir contornos distintos de acordo com o caso concreto.

Nas palavras de Teresa Coelho Moreira (2010),

> na medida em que a instalação (...) de dispositivos (de localização) permite conhecer a localização das pessoas e, no caso dos dispositivos de geolocalização transmitidos por um telemóvel, obter informação acerca de uma pessoa física que pode ser identificada, dado que os dispositivos móveis inteligentes estão indissociavelmente ligados a pessoas singulares, cai-se, então, no tratamento de dados pessoais. (MOREIRA, 2010, p. 53).

Há, inclusive, situações em que a geolocalização pode ser considerada um dado pessoal sensível, quando relevar, por exemplo, que o indivíduo se encontra em um estabelecimento religioso, requerendo ainda mais cuidado e atenção às especificidades da lei em seu tratamento. A LGPD disciplina esse tipo de situação do §1° do artigo 11, que determina a observação das regras específicas para tratamento de dados sensíveis quando houver a existência de "dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular".

Portanto, a localização de um indivíduo é considerada um dado pessoal tutelado pelas normas de proteção de dados pessoais e, caso seja utilizada em desacordo com as normas legais, o tratamento indevido da informação enseja a punição do agente de tratamento.

Nos casos em comento, o pedido de acesso à geolocalização do aparelho celular dos reclamados para comprovação da jornada de trabalho e afastamento do pagamento de horas extras foi negado.

A jornada de trabalho, disciplinada nos artigos 58 a 75-E da CLT, corresponde ao período de tempo em que o empregado se encontra à disposição do empregador estabelecido no contrato de trabalho. A duração normal do trabalho estabelecida por lei, e também a mais comum, é de oito horas diárias, e, caso se exceda, o empregador fica obrigado a indenizar o trabalhador pelas horas extraordinárias trabalhadas. A prova da jornada de trabalho incube ao empregado, ônus que se inverte nos casos em que o empregador conta com mais de 10 empregados, de acordo com a súmula 338 do Tribunal Superior do Trabalho. O cartão de ponto é o meio mais utilizado para comprovação da jornada, podendo ser aceitos também outros meios de prova.

Nas decisões, os magistrados consideraram que o acesso a tais dados pelas instituições empregadoras reclamadas violaria de forma desproporcional a privacidade dos empregados e

que a prova pretendida poderia ser produzida por outros meios, como a oitiva de testemunhas, por exemplo.

Ainda, considerou-se que houve violação dos princípios da adequação e da necessidade dispostos na Lei Geral de Proteção de Dados, uma vez que a mitigação ao direito à inviolabilidade da vida privada através do compartilhamento da geolocalização do indivíduo não é indispensável, nem tampouco inevitável nos casos em tela.

Ao proferir decisão em Mandado de Segurança analisado, que tramita no Tribunal Regional da Terceira Região, o desembargador Marco Antonio Paulinelli de Carvalho afirmou:

> Os dados de localização da autora são dados/informações pessoais, e não há razão suficiente para justificar a violação da intimidade e da privacidade da reclamante e não estão presentes circunstâncias que justifiquem tamanha violência às garantias fundamentais. (BRASIL. TRT 3ª REGIÃO. Mandado de Segurança n.º 0011155-59.2021.5.03.0000. Relator: Desembargador Marco Antônio Paulinelli de Carvalho. Belo Horizonte, Minas Gerais, 25 de outubro de 2021).

Portanto, o acesso à geolocalização dos empregados caracteriza tratamento indevido de dados pessoais pela violação aos princípios da Lei Geral de Proteção de Dados.

4 CONCLUSÃO

Tendo em vista a margem interpretativa trazida pela Lei Geral de Proteção de Dados em relação ao tratamento dos dados de trabalhadores e a crescente relevância do tema, a análise criteriosa do posicionamento dos magistrados acerca da aplicação de seus dispositivos se faz extremamente necessária.

No estudo das decisões dos Tribunais Regionais do Trabalho da Segunda e da Terceira região, constatou-se posicionamentos convergentes dos magistrados no tocante à demissão por justa causa e à indenização por dano moral em casos de tratamento de dados indevidos, bem como ao compartilhamento da geolocalização para fins de comprovação de jornada de trabalho.

Quanto à demissão por justa causa, verificou-se que os magistrados consideraram como ato de indisciplina e insubordinação e violação de segredo de empresa a conduta de empregados que utilizam meio diverso ao e-mail institucional para envio de dados pessoais dos envolvidos nas atividades do empregador.

Em relação à indenização por danos morais, em 100% dos casos analisados o magistrado condenou o empregador a indenizar o empregado pelo dano extrapatrimonial causado com a divulgação de seus dados pessoais e sensíveis sem a autorização e em desacordo com as diretrizes da Lei Geral de Proteção de Dados. Ainda, tais decisões consideraram presumido o

dano causado ao trabalhador, dispensando provas do abalo psicológico e emocional sofrido para a configuração do dever de indenizar.

Por fim, com relação à utilização da geolocalização do aparelho celular do empregado para fins de comprovação de jornada de trabalho, os tribunais a consideraram inadequada e desnecessária, contrariando os princípios da Lei Geral de Proteção de Dados. As decisões ainda preconizaram a utilização de outros meios de prova menos agressivos ao direito fundamental à privacidade.

Tendo em vista a análise realizada, percebe-se que o posicionamento dos tribunais escolhidos visa garantir o equilíbrio da relação entre empregado e empregador, priorizando a garantia aos direitos fundamentais da parte mais vulnerável, ou seja, o trabalhador. A LGPD tem como norteador de sua aplicação valores pautados na boa-fé e proteção do titular frente ao controlador, assegurando a segurança e transparência no tratamento de seus dados pessoais. Da mesma forma, a CLT se apoia em princípios garantidores da proteção do trabalhador e balizadores dos poderes do empregador. Portanto, ambas as legislações contribuem para efetivação da dignidade e dos demais direitos fundamentais do empregado, que também figura como titular de dados pessoais tratados pelo empregador.

Em contrapartida, o empregado também pode agir em nome do empregado no tratamento de dados, ocasião em que a legislação trabalhista e o entendimento dos tribunais estudados não o exclui da responsabilização por condutas que desrespeitem os princípios da LGPD. Além disso, a referida lei impõe à instituição empregadora a adequação de seus processos garantidores da privacidade dos envolvidos em suas atividades, como a criação de políticas de segurança e confidencialidade, bem como devidas orientações aos empregados.

Diante o exposto, conclui-se que os magistrados que atuam nos Tribunais Regionais do Trabalho da Segunda e da Terceira Região têm aplicado a Lei Geral de Proteção de Dados às controvérsias envolvendo a proteção de dados de forma adequada e ponderosa, alinhada aos princípios do Direito do Trabalho e visando o equilíbrio da relação, sem, contudo, deixar de responsabilizá-lo pelo tratamento indevido.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVARENGA. Rúbia Zanotelli de. **Os limites do poder fiscalizatório do empregador quanto ao monitoramento do correio eletrônico no ambiente de trabalho.** Âmbito Jurídico [online]. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-78/os-limites-do-poder-fiscalizatorio-do-empregador-quanto-ao-monitoramento-do-correio-eletronico-no-ambiente-de-trabalho/> Acesso: 01 de março de 2022.

AMORIM, Rubens Vieira; TAUCHERT, Maicon Rodrigo. O uso da política de segurança da informação no monitoramento do e-mail coporativo e o direito de privacidade do empregado. **Revista São Luís Orione** a. 14, v. 1, n. 8, Disponível em: <http://seer.catolicaorione.edu.br:81/index.php/revistaorione/article/view/66/52> Acesso em 13 de abril de 2022.

ANTUNES, Cristiane Ribeiro Seabra. O presente artigo tende abordar os limites do poder fiscalizatório do empregador quanto ao monitoramento dos e-mails, analisando os direitos e garantias fundamentais no ambiente laboral. **Revista Eletrônica de Direito do Centro Universitário Newton Paiva,** v. 2, n. 21, Belo Horizonte, 2013. Disponível em: <https://revistas.newtonpaiva.br/redcunp/wp-content/uploads/2020/05/D21-50.pdf>. Acesso em 13 de abril de 2022.

BEZERRA LEITE, Carlos Henrique. **Curso de Direito Processual do Trabalho.** São Paulo: LTr, 2021.

BRASIL. ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** 2021. Disponível: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf>. Acesso em 13 de abril de 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Diário Oficial da União, Brasília, DF, 1988.

BRASIL. **Lei 10.406 de 2002.** Código Civil. Diário Oficial da União, Brasília, DF, 2002.

BRASIL. **Lei 13.709 de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 2018.

BRASIL. TRT 3ª REGIÃO. **Mandado de Segurança n.º 0011155-59.2021.5.03.0000.** Relator: Desembargador Marco Antônio Paulinelli de Carvalho. Belo Horizonte, Minas Gerais, 25 de outubro de 2021.

CRONAPP. **Geolocalização em aplicativos:** o que é e como funciona? [online]. Redação Cronapp, 2020. Disponível em: <https://blog.cronapp.io/geolocalizacao-em-aplicativos/#:~:text=Em%20uma%20defini%C3%A7%C3%A3o%20b%C3%A1sica%2C%20a,%2DFi%2C%20por%20exemplo> Acesso em 13 de abril de 2022.

DELGADO, Maurício Godinho. **Curso de direito do trabalho**. 15.ed. São Paulo: LTr, 2016.

DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. **Espaço Jurídico.** Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em:

<https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em: 07 abr. 2022.

GONÇALVES, Carlos Roberto. Direito civil brasileiro: responsabilidade civil. 7. ed. São Paulo: Saraiva, 2012. v. 4. p. 353

LOUREIRO, Silvana Crispim. **Segurança da Informação preservação das informações estratégicas com foco em sua segurança.** (Monografia). Pós-Graduação *Latu Sensu*. Universidade de Brasília – UNB, Brasília, 2008. Disponível em: < https://silo.tips/download/segurana-da-informaao-preservaao-das-informaoes-estrategicas-com-foco-em-sua-seg>. Acesso em 13 de abril de 2022.

MOREIRA, TERESA COELHO, A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo electrónico do empregador, Almedina, Coimbra, 2010, P. 53

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista De Direitos E Garantias Fundamentais**, 19(3), 159-180. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603>. Acesso em 02 nov. 2021.

PAIVA, Thairone de Sousa. **Colisão de direitos fundamentais:** a proteção dos dados pessoais e a proteção à saúde e bem-estar por aplicativos de monitoramento via geolocalização. Trabalho de Conclusão de Curso. Universidade Federal do Rio Grande do Norte – UFRN, 2022. Disponível em: <https://repositorio.ufrn.br/bitstream/123456789/46046/1/TCC%20Thairone%20Finalizado.pdf>. Acesso em 13 de abril de 2022.

PERLINGIERI, Pietro. **Perfis do Direito Civil:** Introdução ao direito civil constitucional. Tradução de Maria Cristina De Cicco. 3ª ed. Rio de Janeiro: Renovar. 2002, pág. 12.

PINHEIRO, Iuri; BONFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. Instituto Trabalho em Debate, 2020. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho>. Acesso em 13 de abril de 2022.

TOLEDO, Rita de Cássia Morais; NETO, Genésio Rodrigues de Queiroga; GODINHO, Adriano Marteleto. A Responsabilidade Civil pela Violação dos Dados Pessoais. **Revista IBERC,** v. 3, n. 1, p. 1-23, 2020. Disponível em: <https://revistaiberc.responsabilidadecivil.org/iberc/article/view/105/78>. Acesso em 13 de abril de 2022.