INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA

ESCOLA DE DIREITO E ADMINISTRAÇÃO PÚBLICA

PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONAL *STRICTO SENSU* EM DIREITO, JUSTIÇA E DESENVOLVIMENTO

MESTRADO PROFISSIONAL

REFLEXOS DA LEI GERAL DE PROTEÇÃO DE DADOS NAS RELAÇÕES DE TRABALHO:

Desligamento de empregados por justo motivo em decorrência de incidentes de segurança de dados sob o prisma da LGPD

Sérgio Eliezer Pelcerman

Orientadora: Profa. Dra. Beatriz Kira

São Paulo

2022

SÉRGIO ELIEZER PELCERMAN

REFLEXOS DA LEI GERAL DE PROTEÇÃO DE DADOS NAS RELAÇÕES DE TRABALHO:

Desligamento de empregados por justo motivo em decorrência de incidentes de segurança de dados sob o prisma da LGPD

Dissertação apresentada como requisito para obtenção do título de mestre em Direito, Desenvolvimento e Justiça pela Escola de Direito e Administração Pública do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP.

Orientadora: Profa. Dra. Beatriz Kira

São Paulo

2022

SÉRGIO ELIEZER PELCERMAN

REFLEXOS DA LEI GERAL DE PROTEÇÃO DE DADOS NAS RELAÇÕES DE TRABALHO:
Desligamento de empregados por justo motivo em decorrência de incidentes de segurança de dados sob o prisma da LGPD

Dissertação apresentada como requisito para obtenção do título de mestre em Direito, Desenvolvimento e Justiça pela Escola de Direito e Administração Pública do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP.

São Paulo, 12 de Dezembro de 2022.

BANCA EXAMINADORA:

_____
Profa. Dra. Beatriz Kira
Orientadora - IDP

_____
Prof. Dr. Thomas Victor Conti
Avaliador 1

_____
Prof. Dr. Carlos Marcelo Gouveia
Avaliador 2

AGRADECIMENTOS

Agradeço, em primeiro lugar, a Deus, soberanamente bom e justo, pela oportunidade de estudar em uma das maiores instituições de ensino jurídico do País e, assim, ter a oportunidade de ter estudado no local em que grandes acadêmicos do Direito estudaram e deixaram sua "marca" na história da Casa.

Não menos, agradeço aos brilhantes docentes que me lecionaram verdadeiras obras em forma de conteúdo, em especial, ao professor Danilo Doneda, que me fez entender a complexidade e a necessidade de discussão sobre o Tema desta dissertação.

Agradeço igualmente a Professora Beatriz Kira pela sensibilidade em fornecer uma orientação tão rica e com aspectos acadêmicos que me fizeram refletir praticamente sobre a íntegra da dissertação, visando, em todos os contatos realizados, me auxiliar para transmitir um estudo sólido, rico e acadêmico em tão pouco tempo de contato.

Agradeço, também, aos membros da minha família, que, com amor e carinho, me apoiaram no decorrer do mestrado e me incentivaram "nesta longa caminhada na busca pelo saber" e na reforma interior, bem como aos profissionais do Direito, com os quais tive a oportunidade de aperfeiçoar a prática jurídica.

Não poderia deixar de mencionar meus grandes amigos, que desde a tenra infância convivem ao meu lado, que sempre fizeram - e fazem - parte de minha história de vida. Não menos importante, aos meus Colegas de sala de aula, no regime virtual, que percorreram todos os caminhos comigo.

Por fim, agradeço aos profissionais e amigos do Escritório Almeida Prado & Hoffmann Advogados Associados, um a um, pela oportunidade, incentivo e apoio recebido ao longo de todos esses anos, exatamente desde 2011. Agradeço por fazer parte não só de um grupo, mas de um time, que aplica a ética e que me fez - e faz – crescer profissional, intelectual e moralmente, tornando-me, verdadeiramente, um cidadão que aplica e defende todas as questões de senso de justiça.

RESUMO

O objetivo desta dissertação consiste na realização de um estudo acerca da legalidade quanto à aplicação da justa causa em decorrência de vazamento de dados naturais e de terceiros durante o exercício da atividade laboral e com o descumprimento da norma que regula os dados. Embora a Lei nº 12.709/2018 – Lei Geral de Proteção de Dados (LGPD) preveja as hipóteses de violações ao tratamento, na prática, não é claro se a sua incidência na Justiça do Trabalho poderia refletir a legalidade ou eventual abuso de poder por parte do empregador, e se tais violações justificariam a incidência das hipóteses de aplicação da justa causa previstas no artigo 482 da CLT. Mormente, nas situações categóricas envolvendo justa causa, é de extrema particularidade e de tamanha dificuldade aliar os comandos de lei especial com os preceitos maiores da Lei Trabalhista (CLT). Neste contexto, a pesquisa aborda as seguintes questões: em casos de vazamentos de dados, qual a métrica adequada de se aplicar a justa causa em decorrência de violações ao artigo 482, da CLT, em conjunto a Lei n.º 13.709/2018? O artigo 482 se enquadrará na Lei n.º 13.709/2018 ou a Lei n.º 13.709/2018 se encaixará no artigo 482 da CLT? Para responder a estas questões, o estudo é estruturado da seguinte forma: (*i*) discussão acerca do conceito de dados pessoais; (*ii*) o enquadramento de dados na LGPD; (*iii*) da responsabilidade objetiva ao cometer violações à LGPD; (*iv*) das sanções no cometimento de violações à LGPD; (*v*) a aplicação ou não da LGPD na Justiça do Trabalho; (*vi*) o conceito de justa causa; (*vii*) da distinção entre dados privados e dados públicos; (*viii*) a aplicação ou não da justa causa em decorrência de vazamento de dados; (*ix*) as hipóteses particulares de aplicação de justa causa em razão do vazamento de dados, mormente pela ausência de fundamentação expressa na CLT e o respectivo enquadramento. Assim, a pesquisa busca entender em qual o texto o conceito de "dados", e especialmente o significado de "dados pessoais", pode ser relacionado ao ato comissivo e enquadrado no rol do artigo 482 da CLT, à luz dos princípios do direito do trabalho bem como dos princípios de proteção de dados. Tal investigação aponta para a possibilidade de harmonizar os institutos legais relevantes para determinar a legalidade do desligamento de empregados por justo motivo, em decorrência do vazamento de dados de terceiros, clientes, parceiros e colaboradores em geral, durante o exercício da atividade e que traduzam dados naturais. A determinação da justa causa, argumenta-se, depende de uma análise de cada caso em concreto.

Palavras-chave: Dado pessoal; Justa causa; Incidente de Segurança; Lei Geral de Proteção de Dados.

ABSTRACT

The objective of this masther thesis is to carry out a study about the legality regarding the application of just cause due to the data leak of natural and third party during the labour activity and with the non-compliance norm that regulates the data. Although Law nº 12.709/2018 – General Data Protection Law (LGPD) foresees the hypotheses of violations to the treatment, in practice, it is not clear whether its incidence could reflect in the Labour Court the legality or possible abuse of power by the employer, and whether such violations would justify the incidence of just cause hypotheses provided in article 482, of labour law, CLT. Especially, in categorical situations involving just cause, it is extremely particular and very difficult to connect the commands of special law with the greater precepts of the CLT. In this context, the research addresses the following questions: in cases of data leaks, what is the appropriate metric to apply just cause as a result from violations of Article 482, CLT, together with Law No. 13,709/2018? Will Article 482, CLT, fit into Law No. 13,709/2018 or will Law No. 13,709/2018 fit into Article 482, CLT? To answer these questions, the study is structured as follows: (i) discussion about the concept of personal data; (ii) the framework of data in the LGPD; (iii) strict liability when committing violations of LGPD; (iv) sanctions for committing LGPD's violations; (v) the application or not of the LGPD in the Labour Court; (vi) the concept of just cause; (vii) the distinction between private and public data; (viii) the application or otherwise by just cause as a result of data leak; (ix) the particular applications hypotheses of just cause due to data leak, mainly due to the lack of grounds expressed in the CLT and the respective framework. Thus, the research seeks to understand in which text the concept of "*data*", and especially the meaning of "*personal data*", can be related to the commissive act and framed in the list of CLT, article 482, in particular, the rights principles of the labour as well as data protection principles. This investigation points to the possibility of combine the relevants legal institutes to determine the dismissals legality of employees for just cause, as a result of datas leak from third party, customers, partners and employees in general, during the practice of the activity and that transforms natural data. The determination of just cause, it is argued, depends on an analysis of each specific case.

Keywords: Personal Data; Dismissal for fault; Security incidente; General Data Protection Law.

SUMÁRIO

1 INTRODUÇÃO

A Lei nº 13.709/2018, também chamada de Lei Geral de Proteção de Dados, ou simplesmente LGPD, tem como objeto o tratamento e a proteção de dados e informações pessoais/naturais, em toda e qualquer relação jurídica.

Preliminarmente, faz-se de extrema importância destacar o objetivo essencial da referida lei, o qual é apresentado no *caput* do seu artigo 1º, com a seguinte redação:

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

Do objetivo acima transcrito é possível extrair que se trata de lei destinada à proteção de dados e informações pessoais, inclusive digitais, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e de personalidade da pessoa natural.

O artigo 5º, I, da LGPD define dado pessoal como "informação relacionada a pessoa natural identificada ou identificável." Nesse aspecto, "dado pessoal" pode ser qualquer informação que possibilite, de forma direta ou indireta, a identificação de uma pessoa. A título de exemplos se pode citar o nome, CPF, e-mail e número de documentos de identificação. Os dados pessoais, referidos pelo artigo 1º da LGPD, portanto, não se restringem às informações básicas, como nome e número de documentos, mas abrange qualquer informação que possa ser associada à pessoa identificada ou identificável.

Em complemento, cabe dizer que a LGPD sofreu forte influência do Regulamento Geral de Dados Pessoais (*General Data Protection Regulation),* ou GDPR como é conhecido pela sigla em inglês, lei que trata da proteção de dados na União Europeia.[2]

No entanto, o GDPR estabelece regras mais específicas do que a lei brasileira para garantir a proteção dos direitos e liberdades no que diz respeito ao processamento dos dados pessoais dos empregados no contexto de trabalho. Por exemplo, em seu artigo 88 o GDPR regula o processamento de dados no contexto do emprego. Além disso, o item 5, do artigo 30 do GDPR preconiza que as micro, pequenas e médias empresas que possuírem menos de 250 (duzentos e cinquenta) trabalhadores, estarão dispensadas de manter o registro de suas

---

1 BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

2 PINHEIRO, Patricia Peck. **Proteção de dados pessoais comentários à Lei n. 13.709/2018 (LGPD)**. 3. ed. São Paulo: Saraiva Jur, 2021. p. 20.

atividades de tratamento de dados, relacionando-se especificamente a temática do controle dos dados e relações empregatícias entre empresas e empregados.

O mesmo vale para o artigo 13, do GDPR, ao prever que em caso de recolhimento de dados pessoais relativos a um titular de dados, o responsável pelo tratamento deve, no momento de obtenção dos dados pessoais, fornecer informações, como por exemplo, a identidade e os dados do contato do responsável pelo tratamento e dependendo, do seu representante.

Enaltece-se a situação específica, em seu caráter coletivo, dentro de um grupo de empresas envolvidas em uma atividade econômica conjunta e sistemas de monitoramento no local de trabalho. Insta salientar que o GDPR se aplica aos 27 países da União Europeia, abrangendo também os países que compõem o Espaço Econômico Europeu (Liechtenstein, Islândia e Noruega), e está vigente desde 25 de maio de 2018, após a consumação de *vacatio legis* de dois anos.

Um dos pontos mais relevantes para o presente estudo é o fato de a lei europeia ter previsto aplicações mais específicas quanto ao processamento de dados pessoais em relações laborais, destacando-se o artigo 88 do GDPR, que será abordado pormenorizadamente mais adiante. Por sua vez, a lei brasileira tem aplicação geral, destinada a todas as áreas, inclusive ao Direito do Trabalho. Nesse sentido, apesar de o legislador não ter elaborado a LGPD pensando nas relações de trabalho e emprego, sua aplicação é fundamental para a proteção de diversas informações que permeiam as Relações de Trabalho, desde a formalização do Contrato de Trabalho até a respectiva rescisão e posterior arquivamento de tais informações. Evidentemente, a LGPD poderá ser aplicada às relações de trabalho quando o caso concreto envolver dados pessoais.

Vale enfatizar que a Autoridade Nacional de Proteção de Dados (ANPD), órgão da Administração Pública que deve implementar, fiscalizar e zelar pela correta aplicação e observância da lei, prevista no artigo 55-A da LGPD, assume a importante função de editar atos preventivos para a correta aplicação da norma, assim como atos de conscientização. Por sua vez, cabe às empresas e à sociedade, como um todo, a função de conduzir discussões quanto ao conteúdo da LGPD e a forma de proceder a proteção de dados. Vale dizer que as infrações cometidas às normas previstas na Lei, além de penalizadas com o pagamento de multa (LGPD, art. 52, II[3]), também estão sujeitas a responsabilização por eventuais danos patrimoniais, morais, individuais ou coletivos.

---

[3] LGPD, "Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I -

Nesse contexto, fundamentalmente, se faz necessário analisar o significado de "tratamento de dados pessoais", bem como as operações inerentes a utilização de dados sob qualquer espécie que possam efetivamente causar um incidente de segurança, caso as normas da empresa não sejam corretamente seguidas. Por exemplo, em uma empresa que tem o cuidado de adotar códigos de conduta com o intuito de preservar os mais diversos dados (prevendo a proibição de compartilhamento de informações), caso algum funcionário transmita um documento para diversos e-mails de terceiros sem verificar para quem o está enviando, esse funcionário, além de violar o termo de consentimento firmado com o empregador (LGPD, art. 5º, XII), estaria violando a própria LGPD. Nessa situação, a depender da gravidade, o ato pode dar causa à rescisão do contrato de trabalho por incontinência de conduta ou mau procedimento do funcionário (CLT, art. 482, "b").

Em outras palavras, na relação entre empregador-funcionário, enquanto vigente as obrigações contratuais, ambos terão responsabilidades mútuas. Contudo, esse mesmo cenário não se aplica aos dados manuseados pelos empregados inerentes a clientes, terceiros e que sejam considerados sigilosos e sensíveis. Tais dados são o objeto da presente dissertação, que buscará examiná-los no que concerne às possibilidades previstas aos empregadores, multas e danos que possam ocasionar nesses atos. Enquanto o empregador terá o papel de proporcionar mecanismos (orientações) ao quadro de funcionários da empresa, caberá ao empregado respeitar as regras daquela microssociedade e não direcionar de forma indevida informações de clientes, terceiros e, até mesmo, de colaboradores em geral, ou seja, informações que contenham dados pessoais e que possam comprometer a vida individual de cada pessoa e não somente a empresa que seria empregadora.

Acarreta, que no momento em que ocorre a rescisão do contrato de trabalho de determinado funcionário, consequentemente termina o tratamento de dados pessoais entre empregador-funcionário, podendo enquadrar os incisos I e III, do artigo 15, da LGPD, uma vez que o empregado não terá mais acesso aos dados naturais constantes do Banco de Dados da empresa. Da interpretação do inciso I do referido dispositivo, é possível extrair que há uma finalidade específica para o tratamento de dados. No âmbito laboral, a finalidade específica

---

advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração;" (BRASIL. **Lei nº 13.709, 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

consiste na proteção de dados naturais de pessoas que o empregado possa ter contato enquanto praticante do exercício laboral, em todos os sentidos, sendo crucial o diálogo entre ambas as figuras. O dever de proteção caberá a cada funcionário que, a depender do ato particular e do dano causado à empresa, incorrerá nas hipóteses de justa causa, uma vez que terá acesso irrestrito a dados de pessoas naturais (ainda que jurídicas), cujo vazamento poderá causar danos irreversíveis. Por sua vez, a empresa é responsável pelo fornecimento de instruções sobre a política de tratamento de dados de forma geral, e os funcionários que não observarem a devida proteção de dados cometerão mau procedimento (CLT, art. 482, "b"). O mau procedimento se configura quando o empregado toma uma decisão equivocada, que resulta em ação irregular e incompatível com as obrigações funcionais acordadas.

Dessa forma, se o funcionário violar os bancos de dados e transmitir informações para terceiros, poder-se-á dizer que houve quebra de procedimentos de ordem patrimonial e até mesmo de confiança que acarretaria em uma análise dos procedimentos adotados e os eventuais danos causados à pessoas naturais titulares dos dados, ensejando, nesse momento, o entendimento sobre a responsabilidade trabalhista e as modalidades de punição que o empregador poderia utilizar em tal cenário.

Conota-se que a gravidade em si, ao se falar em transgressões à LGPD dentro de uma empresa por algum funcionário, pode remeter à justa causa, eis que, a justa causa se baseia em faltas graves que ensejam a ruptura da confiança na relação laboral, por isso, a transmissão de dados pode gerar indícios dessa irregularidade.

É possível verificar que a Lei Geral de Proteção de Dados, em seu artigo 5º, Inciso XIV, prevê a figura da "eliminação", significando a "exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado".

Além disso, é importante ressaltar que que no âmbito trabalhista, uma grande questão que aflige diversas empresas e funcionários é justamente o tempo de guarda de determinado documento. Na modalidade física, era difícil disponibilizar espaços físicos adequados aos grandes volumes de documentos que deveriam ser guardados e muitos documentos eram eliminados antes de findo o prazo legal de guarda. Com o espaço virtual, muitos dos problemas foram resolvidos, bastando, por exemplo, a existência de "nuvens", de redes e de servidores para o armazenamento correto e efetivo de documentos.

A questão se relaciona com a eliminação incorreta dos documentos com dados sensíveis, podendo se atribuir responsabilidade ao funcionário que praticou a ação de transmissão dos dados sensíveis de terceiros. Para cada definição que a LGPD traz, há uma aplicação específica no Direito do Trabalho, enfatizando-se mais uma vez o caráter geral da

norma analisada. Evidentemente, cada instituição (pública ou privada), possui ordenamentos e regramentos próprios, os quais tem por objetivo harmonizar as relações entre todas as áreas daquele pequeno círculo, cada qual com o seu papel dentro da incorporação, sendo relevante a área de atuação da empresa (instituição), por exemplo, que dependendo do caso, detém maior gravidade quanto ao teor das informações que possam ser vazadas e gerar danos e impactos perante terceiros, bem como, ao empregador.

Diante do caráter introdutório ora narrado, surge a questão objeto de estudo e análise da presente dissertação, qual seja, o vazamento de dados internos da empresa para o mundo externo ou o descumprimento dos preceitos da LGPD inerente ao incidente de segurança gera o desligamento por justo motivo? Esse é o questionamento que o presente trabalho visa abordar. Veja-se que inexiste, atualmente, qualquer previsão ou possibilidade de desligamento de empregados por justo motivo em decorrência de vazamento de dados, o que vai diretamente ao encontro das regras da LGPD. Tal tema deve ser analisado e estudado a fundo, eis que possui desdobramentos não apenas nas leis do trabalho, mas também na aplicação da LGPD e seus reflexos na vida das pessoas.

Para responder às perguntas de pesquisa, o estudo examina os seguintes termos: (*i*) as regras inerentes a LGPD sobre a presente temática; (*ii*) as regras da CLT, se existentes, sobre a presente temática e eventual confrontação com a LGPD; (*iii*) o vazamento dos dados e os impactos legais; (*iv*) o tratamento dos dados e a qualificação de dados sensíveis; (*v*) modalidades de rescisão de contrato de trabalho por justo motivo previstas na CLT; (*vi*) como a CLT trata os processos de desligamento por justo motivo; (*vii*) proteção dos dados entre empregador e empregado, visando apresentar argumentos e posicionamentos concretos sobre as espécies de vazamento de dados; e (*viii*) a consequente possibilidade do empregador de realizar os desligamentos por justo motivo de empregados responsáveis por vazamento de dados, ainda que não sejam encarregados pelo tratamento dos referidos dados, integrando as duas legislações para obtenção de um resultado final.

Daí decorre a multidisciplinariedade do Direito, com a interligação entre as diversas áreas, especificamente na presente dissertação envolvendo o Direito do Trabalho e a LGPD, voltada ao aspecto tecnológico que será abordado. Diante de toda a conjectura abordada até então, evidentemente, que se trata muito mais do que da proteção de dados, se trata, acima de tudo, de conscientização, educação, treinamento em segurança da informação, liberdade (vinculada à responsabilidade) de expressão e legitimidade, pois, a todo e qualquer momento, a pessoa estará diante de tomada de decisões.

Para tanto, utilizar-se-á a denominada metodologia dedutiva, destacando-se a análise de julgados da temática, aliada ao estudo de caso específico, e à discussão de doutrina (tratando-se de uma literatura recente, mas que norteia o crivo do jurista, em atenção à velocidade das transformações que vêm ocorrendo nos últimos tempos) sobre a Lei Geral de Proteção de Dados, em seu caráter geral e, especialmente, sua aplicação no Direito do Trabalho e no Direito do Processo do Trabalho. Realiza-se, assim, o exame da posição de diversos autores, a fim de compreender as regras específicas quanto à violação das normas inerentes ao processamento de dados nas relações de emprego.

2 LEI GERAL DE PROTEÇÃO DE DADOS: ESCOPO E OBJETIVOS

Conforme visto na Introdução, a LGPD possui o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, especificamente evitando-se que tais dados sejam utilizados em malefício do titular, aplicada à toda legislação em caráter generalizado, sem qualquer aplicação específica para as demandas inerentes à esfera laboral, diferentemente do quanto previsto na legislação de proteção de dados internacional.

Assim, quando condutas se relacionam com o Direito do Trabalho, além da aplicação da nova norma especial, deverá ser interpretada em conjunto com a Consolidação das Leis do Trabalho, ante à complementariedade de ambas as normas para resolução de casos concretos.

Considerando-se, ainda, o contexto da justa causa, há incidentes de segurança de dados em caso de vazamento, espécie que será devidamente analisada na presente dissertação

Diante do presente cenário, faz-se necessário elucidar a evolução da LGPD, haja vista que, anteriormente à criação da referida legislação, há constitucionalmente a proteção e inviolabilidade da pessoa humana, o que demandou, de acordo com a evolução tecnológica, a necessidade de criação de legislação específica para a proteção dos dados e o consequente aspecto protetivo junto as esferas sociais, econômicas, legais e de segurança aos titulares dos dados.

2.1 Evolução, definição e espécies de dados: pessoais, pessoais sensíveis, de uso público e de acesso público

Antes de adentrar ao objeto principal do presente estudo, importante se faz a análise do contexto histórico até a promulgação da LGPD, assim como dos seus principais pontos, como âmbito de aplicação, extraterritorialidade, definições e os princípios que norteiam o sistema de proteção de dados pessoais como um todo, espécies de dados.

É importante observar conceitos e a própria história inerente à proteção dos dados, para se compreender o atual cenário envolvendo incidentes de segurança, justamente para que, com a formalização conceitual, seja viável a análise das confrontações perante o Direito do Trabalho e se os institutos se relacionam no aspecto das penalidades, da responsabilidade e atuação dos agentes envolvidos no controle e transmissão de dados.

Desta forma, a subdivisão em tópicos tem o viés de apresentar minuciosamente todos os pontos inerentes à evolução da LGPD, bem como, as devidas características e definições dos

dados manuseados por empregados a fim de classificá-los com base na legislação aplicada e em decorrência disso, buscar introduzi-los no sistema de responsabilidade civil e consequentemente, penalidades aplicáveis pelo uso irregular, conforme ver-se-á adiante.

2.1.1 Evolução Histórica da Legislação

É indubitável que a LGPD trouxe ao mundo jurídico inovações quanto as formas de entendimento sobre as matérias inerentes aos dados pessoais e, consequentemente, quanto a forma de exposição, controle e, até mesmo, sobre os incidentes de segurança que envolvam vazamento dos dados.

Veja-se que a lei, aprovada em 14 de agosto de 2018 e em vigor desde 18 de setembro de 2020, regulamenta a forma como as organizações podem utilizar os dados pessoais no Brasil, estabelecendo regras detalhadas a respeito da coleta, uso, tratamento e armazenamento desses dados. A referida legislação impõe profunda transformação no sistema de proteção de dados brasileiro, em boa medida alinhada com a também nova legislação europeia, o General Data Protection Regulation (GDPR), afetando todos os setores da economia, tanto no âmbito digital quanto fora dele.

Dentre as regras trazidas pela nova legislação brasileira, considerando as hipóteses de vazamentos de dados e outros incidentes de segurança, chama a atenção no meio empresarial é o artigo 52 da LGPD. Esse dispositivo prevê que, no caso de infrações cometidas às normas previstas na Lei, aos agentes de tratamento de dados responsáveis serão aplicadas as sanções administrativas ali previstas, desde a mais branda, como a advertência, até a mais severa, como a proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.

O conceito de proteção de dados detém interligação com a sua aplicação nas mais diversas espécies de relações, que, segundo Pinheiro e Bomfim [4], ostentam autêntica transversalidade, ou seja, não há aplicação somente no ramo do Direito, como também se estende aos mais diversos setores gerais, como a Economia, Educação, Marketing ou órgãos que envolvam a transmissão e controle de dados.

Desde as últimas décadas do Século XX, a tecnologia se desenvolve a passos largos. Com o surgimento dos computadores e da informática, os seres humanos e, principalmente, as corporações empresariais passam, cada vez mais, a ter a necessidade de registrar, armazenar e manipular dados. A importância e a crescente utilização dos dados pessoais para as mais

---

[4] PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. *In:* MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (coord.). **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2021. p. 49.

variadas finalidades, sejam de identificação, classificação e/ou autorização, entre outras, os vem se transformando em um elemento para o mercado e, sobretudo, para que as pessoas, físicas ou jurídicas, tenham autonomia e liberdade para operar na atual sociedade da informação. Não obstante, os dados pessoais também se revelam como um dos grandes atrativos do mundo moderno, visto que a identificação dos indivíduos, de seus gostos, preferências, necessidades e desejos, passou a representar uma fonte lucrativa para os grandes negócios, conforme será abordado na sequência.

Em que pese ser esse fluxo de dados uma realidade dos novos tempos, concomitantemente, ele potencializa a possibilidade de infração a direitos fundamentais, como a vida privada, a privacidade e aos demais valores a eles relacionados. Assim, se o risco de violação e de divulgação de dados é uma constante, cabe ao Estado desenvolver uma proteção moderna, específica e eficiente sobre o tema. Nas palavras de Crespo e de Ribeiro Filho[5], "se por um lado, o avanço tecnológico é fator de dinamização da vida e evolução social, por outro, o Direito, como ciência, precisa dar uma resposta aos conflitos cotidianos, cada vez mais complexos". Logo, cresce a preocupação legislativo-regulatória em relação aos bancos de dados e seus desdobramentos correlatos, que se passa a expor.

Mesmo que o Brasil só tenha promulgado uma lei específica para proteção de dados pessoais em 2018, não se pode dizer que o ordenamento jurídico nacional, até então, era silente sobre o tema. Pelo contrário, à nível constitucional, verifica-se que todas as constituições Brasileiras trataram, à luz das especificidades de cada época, de questões relativas ao direito à privacidade. Percebe-se que, na esfera constitucional, a evolução se inicia com a inviolabilidade de domicílio e o sigilo das correspondências, passando à proteção da intimidade, privacidade, honra e à imagem, salvaguardando, igualmente, a confidencialidade dos dados, abrangendo qualquer tipo de informação, transmitida ou não.

Nesse sentido, visualiza-se ao longo da história que uma das grandes questões que preocupavam as pessoas, conforme histórico acima narrado, era a preservação da privacidade e da intimidade, sendo perceptível o alcance no âmbito civil. Como se refere aos aspectos da vida civil (vida privada), os efeitos dos aspectos particulares se estendem ao trabalho, especialmente porque há diariamente contato com diversos tipos de dados (raça, cor, gênero, interesses), os quais devem ser preservados pela ótica legal, especificamente nos termos do artigo 5º, incisos I e II da LGPD.

---

[5] CRESPO, Danilo Leme; RIBEIRO FILHO, Dalmo Ribeiro. A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da Lei Geral de Proteção de Dados Pessoais. **Revista de Direito Privado**, São Paulo, v. 20, n. 98, p. 161-186, mar./abr. 2019.

Por conseguinte, com a evolução da tecnologia, consequentemente as formas de trabalho também evoluíram, transformando também as formas de comunicação, o modo pelo qual há a interação entre os núcleos humanos. Logo, é relevante que empresas adotem meios preventivos, para que incidentes de segurança de dados não causem impactos drásticos aos seus resultados e à economia como um todo.

Com efeito, a história propriamente dita mostra que se trata de uma conquista, preservação da intimidade e a inviolabilidade da privacidade, evoluindo-se até a promulgação da LGPD para preservação de Direitos que também se relacionam com a necessidade de guarda e zelo das empresas e dos agentes que efetivamente são responsáveis por esse tratamento nas atividades empresariais, relacionando-se com o aspecto laboral ora apresentado.

Muito antes da LGPD, que foi criada com o fim de consolidar os entendimentos sobre a proteção de dados pessoais, ampliar o escopo de aplicação legal e garantir maior segurança jurídica, a Constituição Federal de 1988 (CF) abordou o tema de forma bastante assertiva, mesmo sendo contemporânea às Diretivas da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), de 1980 e à Convenção 108, de 1981. Ademais, ao longo de seus 114 artigos, a CF reflete os valores da Declaração Universal dos Direitos Humanos, em especial nos Título I e II, nos quais prevê os Princípios Fundamentais e os Direitos e Garantias Fundamentais.

No ano de 1990, foi editado o Código de Defesa do Consumidor (Lei 8.078/1990 - CDC), cujo artigo 43 dispõe sobre o direito dos consumidores de ter acesso aos seus dados pessoais que estejam arquivados em bancos de dados.

> 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.[6]

Ainda que não se trate, expressamente, de consentimento, os §1º e §2º, do artigo 43, do CDC exigem que a abertura de cadastros, fichas, registros de dados pessoais e de consumo seja comunicada ao consumidor por escrito, de forma clara, objetiva, verdadeira e em linguagem de fácil compreensão.

> §1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

---

6 BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 08 abr. 2022.

> §2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.[7]

Posteriormente, o Código Civil de 2002 detalhou, em seu Capítulo II, os direitos da personalidade. São aqueles inerentes à pessoa e à sua dignidade, quais sejam a vida, integridade física, honra, imagem, nome e intimidade. Nesse sentido, se tais dispositivos legais são aplicáveis a toda pessoa natural, em qualquer circunstância e em qualquer ambiente, seja real ou virtual, é evidente que o Código Civil já traz premissas fundamentais, inclusive bem diretas, para a garantia de direitos relacionados à privacidade e à proteção de dados pessoais, ainda que, neste último caso, de modo mais genérico.

Em 2011, foram promulgadas duas leis importantes sobre o tema. Primeiramente, tem-se a Lei 12.414/2011, conhecida como Lei do Cadastro Positivo, recentemente alterada pela Lei Complementar 166/2019, destinada à formação e consulta a banco de dados com informações de adimplemento, de pessoas físicas ou jurídicas, para formação de histórico de crédito, assim como permite a inscrição automática de dados dos usuários em bancos de dados, sendo assegurado o direito à exclusão. Entre os principais direitos, ressaltam-se: (*i*) utilização dos dados pessoais de acordo com a finalidade para qual houve a coleta; (*ii*) ciência e conhecimento sobre os elementos e critérios utilizados na análise de riscos; e (*iii*) compartilhamento de dados somente com a autorização do cadastrado, por meio de assinatura em termo específico.

Por segundo, a Lei 12.527/2011, designada como Lei de Acesso à Informação, atribuiu aos órgãos e entidades do Poder Público o dever de proteção da informação sigilosa e pessoal de cada indivíduo. Segundo a referida Lei, os dados pessoais deverão ser tratados de (*i*) forma transparente e com respeito à intimidade, à vida privada, à honra e à imagem da pessoa, e às liberdades e garantias individuais; e (*ii*) de acesso restrito, devendo a sua divulgação para terceiros ocorrer, tão somente, com o consentimento expresso do titular. Observa-se que a Lei de Acesso à Informação já defendia princípios e direitos que vão ao encontro do disposto pela Lei Geral de Proteção de Dados, promulgada em 2018, como será analisado em detalhes em tópico próprio.

No mesmo sentido de proteção de dados, em 15 de março de 2013, foi editado o Decreto 7.962/2013, que regulamenta o comércio eletrônico, impondo ao fornecedor o dever de fazer uso de mecanismos eficazes e seguros para tratar os dados dos consumidores. No ano

---

[7] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 08 abr. 2022.

seguinte, em 2014, foi aprovada e promulgada a Lei 12.965/2014, conhecida como o Marco Civil da Internet (MCI), que regulamenta o uso da internet e estabelece os princípios, garantias, direitos e os deveres relativos. Fruto de longas discussões, negociações e ponderação de interesses, além de sedimentar a proteção na internet, o Marco Civil da Internet dedicou capítulo exclusivo para a salvaguarda dos dados pessoais, cuja aplicação depende do uso da internet. Entretanto, embora o texto tenha abrangido os direitos garantidos no artigo 5º da Constituição Federal e alguns elementos do Código Civil, do Código de Defesa do Consumidor e de outros atos normativos, o seu objetivo não é regular a privacidade e a proteção de dados de forma abrangente e estruturada.

Quanto ao tema, a referida lei reafirma que qualquer operação de coleta, armazenamento, guarda e tratamento de registros por meio da internet, de dados pessoais ou de comunicações por provedores de conexão deverá respeitar os direitos à privacidade, à proteção de dados pessoais e ao sigilo das comunicações privadas dos registros. E, em eventual inobservância de tais preceitos, os provedores ficarão sujeitos às penalidades de advertência, multa, suspensão temporária e proibição do exercício da atividade. Ocorre que mesmo após a sua regulamentação através do Decreto 8.771/2016, que aborda o tratamento de dados que transitam pela internet apenas no modo *online*, sem ter ingerência sobre os dados offline, o MCI não era tão específico e abrangente. Aliás, o Decreto 8.771/16 também não foi capaz de esclarecer questões e lacunas relativas ao vazamento de dados e aos demais incidentes de segurança, de reiteradas e recentes ocorrências.

Assim, em razão da cobrança social e dos recorrentes vazamentos de dados, o Brasil demandou a necessidade de consolidação de uma lei que tratasse com maior amplitude sobre a proteção dos dados pessoais como um todo, especialmente no que tange à coleta, boas práticas, tratamento pelo Poder Público e por particulares, controle, segurança, governança, responsabilidade, entre outros assuntos. Nesse contexto, fruto do Projeto de Lei 4.060/12, de autoria do Deputado Federal Milton Monti, posteriormente aprovado pelo Senado Federal, através do PLS 58/18, em 14 de agosto de 2018 é promulgada a Lei 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), com vigência iniciada em 18 de setembro de 2020, que será detalhada a partir do próximo item.

Entretanto, é indispensável ponderar que a LGPD não se sobrepõe ao MCI, tampouco o revoga. Ao contrário, a LGPD, nas palavras de Crespo e Ribeiro[8], divide o palco com o Marco

[8] CRESPO, Danilo Leme; RIBEIRO FILHO, Dalmo Ribeiro. A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da Lei Geral de Proteção de Dados Pessoais. **Revista de Direito Privado**, São Paulo, v. 20, n. 98, p. 161-186, mar./abr. 2019.

Civil da Internet nas relações firmadas pela internet e, para as demais, atua como protagonista principal.

É notório que a evolução histórica tentou ditar o ritmo aos problemas referentes à intimidade, sobretudo os condizentes aos direitos da personalidade, surgidos nas sociedades, seja no passado, seja na atualidade. Diante dos complexos quadros envolvendo a privacidade das informações, é que a dinâmica acerca da valoração, do zelo e do prestígio dos dados, em especial, quanto a não divulgação a terceiros, ganhou e vem ganhando destaque no cenário atual das sociedades, o que acarretou na promulgação da LGPD.

Com a evolução histórica das leis, que repita-se, sempre buscavam trazer disposições para proteção dos titulares (vida, segurança, liberdade e inviolabilidade) para controle e privacidade de informações, a LGPD, incorporando-se todos os preceitos existentes, trouxe aos usuários e titulares de dados, ferramentas necessárias para a proteção, bem como, possibilidade de solução dos danos causados e consequentemente, nomear e atribuir responsabilidade aos agentes responsáveis pelo controle das informações, sejam de uso privado ou público.

Não obstante ao referido fato, trouxe também a necessidade dos agentes responsáveis por manusear as informações e dados recebidos não transmiti-las indevidamente, o que reflete o aumento de segurança em toda e qualquer operação de controle, guarda, transferência ou exclusão de dados, refletindo nos exatos termos necessários para analisar os impactos na esfera laboral, haja vista o acesso constante em informações de clientes ou terceiros, mediante a análise pormenorizada do institutos da referida legislação e como são aplicáveis no dia-a-dia.

2.1.2 Caráter geral e aplicabilidade da LGPD

A denominação Lei Geral de Proteção de Dados, destacando-se o uso do termo “Geral”, revela os efeitos da LGPD em diversas espécies de relações, inclusive, no âmbito trabalhista. Conforme prevê o artigo 1º, a lei se aplica às pessoas naturais ou jurídicas, seja de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural, como se depreende do texto legal:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou

> privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.[9]

Por sua vez, o artigo 3º[10] coloca sob escopo da norma, qualquer operação de tratamento realizada por pessoa natural ou pessoa jurídica, de direito público ou de direito privado, independentemente do meio, do país de sua sede ou de onde estejam localizados os respectivos dados, desde que:

(i) a operação seja realizada no território nacional;

(ii) a atividade de tratamento tenha por objetivo a oferta, o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

(iii) os dados pessoais objetos de tratamento tenham sido coletados no território nacional, ou seja, quando o titular dos dados se encontre no Brasil no momento da coleta.

Por utilizar expressões novas e não usuais, que podem levar à confusão dos intérpretes e operadores do Direito, acertadamente, a LGPD, em seu artigo 5º, trouxe conceitos e definições necessárias à compreensão de suas regras. Sobre o objetivo da LGPD, Crespo[11] destaca que a aplicação de referida norma se interliga ao tratamento de dados pessoais, tanto no meio físico como no meio digital, a fim de assegurar os direitos fundamentais das pessoas físicas, na tentativa de impedir abusos por pessoas jurídicas, violando a privacidade e o livre desenvolvimento das pessoas naturais, ou seja, traz um poder de proteção aos titulares dos dados no manuseio de informações sensíveis por terceiros, seja em caráter de boa-fé ou má-fé, responsabilizando-se o agente por qualquer ato ilegal praticado no que concerne ao controle dos dados.

---

9 BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

10 LGPD, "Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objetos do tratamento tenham sido coletados no território nacional." (BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

11 CRESPO, Marcelo. Compliance Digital. *In:* NOHARA, Irene Patrícia; PEREIRA, Flávio de Leão Bastos. Governança, compliance e cidadania. 2. ed. São Paulo: Thomson Reuters Brasil, 2019 *apud* LIMA, Ana Paula Moraes Canto de Lima; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. **LGPD Lei Geral de Proteção de Dados**: sua empresa está pronta?. São Paulo: Literare Books International, 2020. p. 41.

Por sua vez, Carlos Negrão[12] esclarece que a Lei Geral de Proteção de Dados conferiu uma maior segurança aos titulares de dados, em que pese a existência de legislações que apresentavam espécie de disposições sobre os referidos fatos, como o Código de Defesa do Consumidor, Marco Civil da Internet ou a Lei do Sigilo Bancário, apresentando-se inclusive como um sistema de regramentos que incidirá em todos os setores com punições e disposições que devem ser seguidas por todos os ramos necessários ao controle dos dados.

Ou seja, é uma lei geral que tem aplicabilidade em todos os setores sociais inerentes ao controle de dados, conduzindo um sistema de regras para obstar danos à coletividade, sendo aplicáveis em todos os níveis sociais, econômicos e comerciais existentes.

Em comparativo ao GDPR, profícuos ensinamentos de Pinheiro e Bomfim[13] enfatizam o fato de que embora a LGPD não traga dispositivos expressos de aplicação no Direito do Trabalho, "sua incidência a ele é irrefutável, pois a relação de trabalho sequer teria como se iniciar e desenvolver sem a coleta, a recepção, o armazenamento e a retenção de dados pessoais dos empregados ou a candidatos a empregos".

Portanto, a primeira grande reflexão consiste em verificar que a LGPD propriamente dita não contempla disposições específicas sobre o direito do trabalho, mas se trata de uma lei que regulamenta, especificamente, as diversas regras do imenso fluxo de dados pessoais que, até então, "circulava livremente", representando um avanço.

2.1.3 Dos dados pessoais, dados pessoais sensíveis, dados de uso público e dados de acesso público

Apresentado o histórico e evolução da Lei, surge a necessidade de definir os termos utilizados pela legislação e aplicá-los na prática, ou seja, como são tratados e como devem ser zelados para conferir segurança jurídica aos titulares e agentes manuseadores de tais informações. Os dados pessoais ganharam e ganham cada vez mais relevância econômica em decorrência da evolução tecnológica e do controle de dados por agentes de tratamento. Segundo Maia[14], "[...], os dados pessoais ganharam um valor econômico jamais visto, sendo atualmente

---

12 NEGRÃO, Antônio Carlos. Economia digital, proteção de dados e competitividade. *In:* DONEDA, Danilo; MENDES, Laura Schertei; CUEVA, Ricardo Villas Bôas. **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade**: contribuições para a implementação da LGPD. São Paulo: Revista dos Tribunais, 2020. p. 30.

13 DONEDA, Danilo; MENDES, Laura Schertei; CUEVA, Ricardo Villas Bôas. **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade**: contribuições para a implementação da LGPD. São Paulo: Revista dos Tribunais, 2020. p. 186.

14 MAIA, Daniel de Oliveira. As Hipóteses Autorizativas de Tratamento de Dados Pessoais nas Relações de Trabalho Sob a Ótica da LGPD e do GDPR. *In:* MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA,

tratados como verdadeiros ativos, comodities, sendo considerados, para alguns, o "'petróleo da atualidade".

Primeiramente, para melhor compreensão da temática aqui estudada, é necessário analisar o conceito de "dados", assim como a diferenciação entre "dados" e "informação".

Sobre a distinção entre "dados" e "informação", Doneda[15] explica que enquanto a "informação" denota um sentido, uma interpretação, dotada de conteúdo, o "dado", por sua vez, representa "uma informação em estado potencial", o que significa a ausência de veracidade suficiente para a transmissão a terceiros, diferentemente do dado que já é algo concreto com conteúdo suficiente para ser transmitido. Inclusive, sustenta que a transmissão irregular é capaz de gerar danos ao titular dos referidos dados e penalizações aos agentes responsáveis pelo tratamento.

Como visto, um dado, por si só, simplesmente existe no mundo. Já a informação, representa um sentido, uma interpretação, dotado de conteúdo. E no tocante ao Direito do Trabalho como a questão de "dados" se encaixa no cotidiano de situações nascentes nas relações vinculadas ao labor[16]?

No âmbito do Direito do Trabalho a questão é muito mais complexa, pois, de forma direta ou indireta, os funcionários estão diariamente tratando com dados pessoais e pessoais sensíveis de clientes, tratamento que deverá ser regulamentado pelo empregador. Esse é o pensamento de Carloto e Guerra[17], destacando-se que como os funcionários estão sempre tratando com dados pessoais e pessoais sensíveis de clientes, a empresa terá que realizar uma regulação completa, inclusive as boas práticas com todos os funcionários da empresa, uma vez que esses podem causar incidentes, em que a maioria assim poderá fazer por desconhecimento. Será relevante realizar a regulação completa, não só de uma área.

Concebe-se, com isso, que o Direito do Trabalho e o próprio Direito Processual do Trabalho atuam em conjunto com as demais áreas do Direito. O inverso também é verdadeiro, as demais áreas do Direito caminharão lado a lado com o Direito do Trabalho. Daí decorre a multidisciplinariedade do Direito, com a interligação entre as diversas áreas.

Nessa toada, tanto o empregador como o funcionário estarão diante de situações peculiares. E não somente isso. Quando um funcionário, por exemplo, ao acessar um site de

---

André. **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2021. *E-book* (não paginado).

15 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Revista dos Tribunais, 2021. p. 140.

16 Destaca-se aqui o labor como gênero.

17 CARLOTTO, Selma; GUERRA, Elaine. **Manual prático de adequação à LGPD com enfoque nas relações de trabalho**. São Paulo: LTr, 2021. p. 9.

conteúdo indesejado ou receber um e-mail malicioso, clica em um acesso contendo inúmeras "armadilhas", esse ato ultrapassa a atuação das empresas. Nesse sentido, Carloto e Guerra[18] salientam que os colaboradores de empresas precisam entender os motivos do objetivo da segurança da informação, baseando-se no programa de conscientização, educação e treinamento para todos os funcionários, consequentemente, visualizando-se impactos positivos e negativos para a empresa. É notório que mero conhecimento da legislação não é suficiente para evitar incidentes de segurança, pelo contrário, faz-se necessário o aperfeiçoamento por intermédio de cursos de segurança e práticas educacionais para que tais incidentes não aconteçam durante atividades empresariais.

Segundo o artigo 5º[19] da Lei 13.709/2018, há uma enorme diferença acerca da definição de "dados" de forma específica. Veja-se que "dado" é gênero com as suas respectivas espécies. Contudo, observa-se que não há um tipo legal relacionado a dado laboral[20]. Poderia

---

[18] CARLOTTO, Selma; GUERRA, Elaine. **Manual prático de adequação à LGPD com enfoque nas relações de trabalho**. São Paulo: LTr, 2021. p. 197.

[19] LGPD, "Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);" (BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

[20] Salienta-se que não é só a área Trabalhista que está vivendo este impasse, quanto à ausência de previsão legal no tocante à aplicação da Lei Geral de Proteção de Dados. A área Penal também enfrenta a cada dia situações que não foram vivenciadas antes, como se pode perceber numa entrevista ao JOTA acerca da seleção de jurados e as suas respectivas proteção de dados no incêndio da Boate Kiss. Veja-se que a área Criminal vem utilizando os princípios gerais previstos na Lei n.º 13.709/2018: "*Como consequência do previsto no artigo 4º, inciso III, alínea "d", da Lei 13.709/2018, **a Lei Geral de Proteção de Dados Pessoais não se aplica ao tratamento de dados pessoais realizado exclusivamente no âmbito da segurança pública e nas ações penais**. **Não há, assim, uma lei geral de proteção de dados nestes campos**. **Porém, os princípios gerais de proteção de dados e os direitos mínimos dos titulares desses dados devem ser observados pelos órgãos de polícia e de Justiça criminal, nas investigações e nos processos penais**. Não esqueçamos que, em breve, como resultado da Proposta de Emenda à Constituição Federal 17/2019, **o novo inciso LXXIX do artigo 5º da Constituição Federal assegurará o direito à proteção de dados como direito fundamental**. Embora o § 1º do artigo 4º da LGPD assevere que o tratamento de dados pessoais para fins exclusivos de segurança pública e de persecução criminal "será regido por legislação específica", é essencial notar, desde já, que tal diploma futuro* "deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular". *Tais direitos e princípios já estão listados na LGPD. **Portanto, a futura "LGPD penal", como tem sido chamado o futuro diploma, deverá observar os mesmos parâmetros, que, desde já, devem***

ser utilizado outro termo, como por exemplo, “dado organizacional” ou “dado empresarial” (público e privado) ou, até mesmo, “dado da empresa e do funcionário”.

Como visto, no artigo 5º da Lei 13.709/2018, o legislador foi taxativo ao arrolar 03 (três) espécies de dados: (*i*) dado pessoal; (*ii*) dado pessoal sensível; e (*iii*) dado anonimizado. Para cada classificação é importante distinguir as diferenças e contextualizar, ao se utilizar na interpretação do caso concreto.

Segundo Carloto e Guerra[21], sobre a aplicação da LGPD, verifica-se que a legislação se destina diretamente às pessoas naturais, identificadas ou identificáveis. No entanto, com relação às pessoas jurídicas, aplica-se a elas de forma indireta, pois todas as pessoas jurídicas possuem dados de pessoas naturais, inclusive sócios, empregados e outros trabalhadores. Logo, é incontestável que realmente a LGPD se aplica tanto às pessoas naturais quanto às pessoas jurídicas, sejam elas do ramo público, sejam elas do ramo privado.

E certamente se aplicará às pessoas jurídicas, pois, afinal, “as pessoas jurídicas, também denominadas pessoas coletivas, morais, fictícias ou abstratas, podem ser conceituadas como sendo conjuntos de pessoas ou de bens arrecadados, que adquirem personalidade jurídica própria por uma ficção legal”. Trata-se da aplicação da teoria da realidade técnica, segundo Tartuce[22]. Ou seja, a pessoa jurídica como ser coletivo, seja no âmbito público ou na esfera privada, detém consigo informações de uma população inerente ao respectivo setor (funcionários, sócios, clientes, entre outros titulares), correspondendo aos dados naturais em geral.

Prosseguem Carloto e Guerra[23], diferenciando dado pessoal direto de dado pessoal indireto. O primeiro se relaciona à pessoa identificada, são exemplos: nome, RG, CPF, título de eleitor, número de passaporte, endereço, estado civil, número da OAB, número do CRM, número do COREN, telefone, entre outros. Por sua vez, o dado pessoal indireto identifica o titular indiretamente, sendo necessárias informações adicionais. Em suma, enquanto no dado pessoal direto é possível identificar a pessoa diretamente, no dado pessoal indireto são necessárias informações adicionais para identificar o titular de forma indireta.

---

ser aplicados ao tratamento de dados pelo Poder Público, tendo em vista o* princípio do efeito imediato*, insculpido no §1º do artigo 5º da Constituição*.”*(Grifo nosso). (ARAS, Vladimir. Boate Kiss: a seleção dos jurados e o direito à proteção de dados pessoais. **Jota,** São Paulo, 04 jan. 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/boate-kiss-selecao-jurados-direito-protecao-dados-04012022. Acesso em: 04 jan. 2022).

21 CARLOTTO, Selma; GUERRA, Elaine. **Manual prático de adequação à LGPD com enfoque nas relações de trabalho**. São Paulo: LTr, 2021. p. 13.

22 TARTUCE, Flávio. **Direito Civil**: Lei de Introdução e parte geral. 9. ed. São Paulo: Método, 2016. p. 219.

23 CARLOTTO, Selma; GUERRA, Elaine. **Manual prático de adequação à LGPD com enfoque nas relações de trabalho**. São Paulo: LTr, 2021. p. 15.

Ato contínuo, o inciso II, do artigo 5º, da Lei 13.709/2018, prevê o dado pessoal sensível. Dentro da categoria de dados sensíveis, há dado pessoal sobre: (*i*) origem racial ou étnica; (*ii*) convicção religiosa; (*iii*) opinião política; (*iv*) filiação a sindicato ou a organização de caráter religioso, filosófico ou político; (*v*) dado referente à saúde ou à vida sexual; e (*vi*) dado genético ou biométrico, quando vinculado a uma pessoa natural. Percebe-se que quando se fala em dados pessoais sensíveis, caso ocorra alguma desconformidade, o titular dos dados poderá sofrer prejuízos maiores.

Na ótica trabalhista, ou melhor, nas relações de trabalho, existirá o manuseio de dados pessoais sensíveis, de forma legítima, por obrigação legal, principalmente de dados de saúde, entre outros, muitas vezes necessários. Como se trata de relações de trabalho, dados e informações estão fortemente presentes no cotidiano de trabalhadores, empresas, órgãos públicos, enfim, numa sociedade pautada na informação. Ou seja, é perceptível que no Direito do Trabalho, que muito evoluiu desde a sua concepção elementar, o binômio máquina-humano faz parte quase que intrinsecamente um do outro, seja na necessidade de elaborar atos processuais ou, até mesmo, para comunicação com clientes.

Certamente, os dados são intrínsecos às relações humanas, sendo utilizados também nas relações de trabalho. Salienta-se que o legislador, ao elaborar o inciso II, do artigo 5º, da Lei 13.709/2018, inseriu questões sensíveis interligadas às relações de trabalho, como por exemplo, filiação a sindicato, dado relativo à saúde e dado biométrico.

Em relação à proteção de dados pessoais, a Lei em si não apontou uma especialização de áreas, não prevendo sua aplicação na área do Direito do Trabalho, do Direito Penal, ou do Direito Tributário, por exemplo. Conforme dispõe em seu artigo 1º, a LGPD abrange tão somente "[...] o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". Em parágrafo único, o dispositivo ainda dispõe que "as normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrato Federal e Municípios", ou seja, se aplicam-se a todos.[24] Sendo assim, de forma direta, aplica-se a LGPD aos mais diversos ramos do Direito, justamente por ser geral e aplicável a todos os campos.

Quando o artigo 5º, inciso III, da Lei 13.709/2018, dispõe sobre o dado anonimizado, será que se perdura a utilização de algum dado anônimo?

---

[24] BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

Veja-se que, segundo o artigo 13, § 4º, da Lei, "a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro".[25] *In verbis*:

> Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.[26]

Veja-se que o caminho a percorrer consiste em trazer segurança informacional para toda a sociedade, em todas as áreas da vida humana, uma vez que, conforme histórico apresentado, em que pese a existência em legislações diversas sobre controle de dados, a promulgação da LGPD trouxe à tona aspectos de controle, conceitos, responsabilidades e penalidades para infratores que descumprirem a referida legislação.

Portanto, enfatiza-se o grande desafio: atribuir a devida responsabilidade, a fim de punir os infratores de forma efetiva, assim como, nos termos do artigo 50 da LGPD, que estabelece regras de boas práticas e de governança para que os dados naturais sejam tratados corretamente por cada colaborador envolvido nos processos existentes.

2.1.4 A distinção entre dados privados, dados de uso público e dados de acesso público

A LGPD, conforme acima narrado, é uma legislação criada para proteger dados sensíveis, pessoais, públicos e privados em caráter efetivo, justamente por conter informações que possam comprometer titulares de dados, seguindo-se um caráter pedagógico e punitivo aos infratores. Contudo, é preciso diferenciar os conceitos de "dados privados", "dados de uso público" e "dados de acesso público", porque cada qual se aplica a cada caso concreto, sendo que o incidente de segurança inerente ao vazamento de dados pode envolver empresa de direito privado como também empresa de direito público.

---

[25] BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

[26] BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

Também, a forma pela qual se obteve determinado dado poderá ser relevante, uma vez que se o dado é público, o mesmo está disponível (tanto o uso como o acesso). Do contrário, se o dado é privado, ele não está disponível, sendo que algumas pessoas possuem acesso ao dado privado. Portanto, essa distinção será relevante para determinar a gravidade do incidente de segurança de dados e os efetivos atos de punição aplicáveis ao caso concreto.

Segundo afirma Lima[27], é prudente destacar que "[...] a privacidade tem relação com a vida privada, com o direito de ter sua intimidade protegida e está intimamente relacionada com a dignidade da pessoa humana". Ocorre que a diferença entre privado e privado, diga-se necessária, muitas vezes se confunde, pois em que momento o indivíduo se encontra na esfera pública e em que período a pessoa se encontra na esfera privada?

Nesse contexto, Bernabè[28] faz três grandes perguntas que leva à reflexão sobre a aplicação dos conceitos de "público" e "privado" na vida pessoal de todos: "De quem são os dados pessoais? Do usuário que os criou ou do provedor da plataforma que os arquiva? Qual o modo correto de administrar e usar os dados pessoais conforme as leis fundamentais que regulamentam a privacidade?".

Importante destacar que ao se falar em "dado privado" e em "dado público", parece que ambos os conceitos se destinam às definições de "posse"[29] e de "propriedade"[30], porque no campo digital, por exemplo, fala-se em ciberespaço. Contudo, embora os conceitos de "posse" e de "privado" se apliquem aos direitos reais, é preciso verificar se, na sua utilização, esses

---

27 LIMA, Ana Paula Moraes Canto de Lima; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. **LGPD Lei Geral de Proteção de Dados**: sua empresa está pronta?. São Paulo: Literare Books International, 2020. p. 36.

28 BERNABÈ, Franco. **Liberdade vigiada**: Privacidade, segurança e mercado na rede. Rio de Janeiro: Sinergia, 2013. p. 75.

29 Conceito de posse à luz do art. 1.196 do Código Civil: "Art. 1.196. Considera-se possuidor todo aquele que tem de fato o exercício, pleno ou não, de algum dos poderes inerentes à propriedade." (BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022).

30 Conceito de propriedade à luz do art. 1.228 do Código Civil: "Art. 1.228. O proprietário tem a faculdade de usar, gozar e dispor da coisa, e o direito de reavê-la do poder de quem quer que injustamente a possua ou detenha. § 1º O direito de propriedade deve ser exercido em consonância com as suas finalidades econômicas e sociais e de modo que sejam preservados, de conformidade com o estabelecido em lei especial, a flora, a fauna, as belezas naturais, o equilíbrio ecológico e o patrimônio histórico e artístico, bem como evitada a poluição do ar e das águas. § 2º São defesos os atos que não trazem ao proprietário qualquer comodidade, ou utilidade, e sejam animados pela intenção de prejudicar outrem. § 3º O proprietário pode ser privado da coisa, nos casos de desapropriação, por necessidade ou utilidade pública ou interesse social, bem como no de requisição, em caso de perigo público iminente. § 4º O proprietário também pode ser privado da coisa se o imóvel reivindicado consistir em extensa área, na posse ininterrupta e de boa-fé, por mais de cinco anos, de considerável número de pessoas, e estas nela houverem realizado, em conjunto ou separadamente, obras e serviços considerados pelo juiz de interesse social e econômico relevante. § 5º No caso do parágrafo antecedente, o juiz fixará a justa indenização devida ao proprietário; pago o preço, valerá a sentença como título para o registro do imóvel em nome dos possuidores." (BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022).

dados ocupam lugar no espaço, sejam no modo físico, sejam no modo virtual, culminando na função social da utilização de dados. Ou seja, a valoração dos dados perfaz nas escolhas em que os indivíduos terão que tomar, ao decidir compartilhar ou não um dado ou uma informação, por exemplo.

Partindo dos conceitos de "dados privados" e de "dados públicos", ambos se interconectam com "privacidade" e com "confidencialidade". Assim, Doneda[31] destaca sobre a profusão de termos, quando o assunto diz respeito à privacidade, podendo-se mencionar vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos utilizados, como "privatividade" e "privaticidade", por exemplo. Sendo assim, se torna prudente verificar essas nomenclaturas, a fim de enquadrar cada situação segundo uma classificação própria.

Bernabè[32] destaca perfeitamente o artigo 8º da Convenção Europeia sobre os Direitos do Homem, enfatizando a importância do mundo privado, entendendo-se que o direito à privacidade é como proteção e proibição de divulgação de uma série de informações relativas à questões como lugares, relações e vínculos familiares, como exemplo narrado pelo autor.

Quanto ao direito de acesso, o artigo 5º, inciso XXXIII, da Carta Magna brasileira, aduz que todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, *in verbis*:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]
> XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;[33]

Já o artigo 7º, § 3º, da Lei 13.709/2018, aduz que o acesso ao tratamento de dados pessoais é público, devendo-se considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. *In verbis*:

---

31 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Revista dos Tribunais, 2021. p. 102.

32 BERNABÈ, Franco. **Liberdade vigiada**: Privacidade, segurança e mercado na rede. Rio de Janeiro: Sinergia, 2013. p. 77.

33 BRASIL. (Constituição [1988]). **Constituição da República Federativa do Brasil**. Brasília, DF: Congresso Nacional, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 abr. 2022.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...]
> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.[34]

Como visto, há grande diferença entre dados que já nascem públicos e dados que se tornam públicos. No mesmo sentido, há diferença entre dados de uso público e dados de acesso público. Nesse sentido, a Lei 12.527/2011, em seu artigo 4º, arrola diversos conceitos primordiais para melhor entendimento sobre o conceito de dado público e de dado de acesso público, merecendo destaque os incisos I e III:

> Art. 4º Para os efeitos desta Lei, considera-se:
> I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
> [...]
> III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;[35]

Veja-se que o dado público é aquele que não confere acesso público, decorrendo daí a finalidade pública para cada situação. A título de exemplo, tem-se o artigo 23, caput[36], da Lei 13.709/2018, em que consagra o tratamento de dados pelo Poder Público. Segundo Prudente do Amaral[37], "o que realmente importa, para além da finalidade de atendimento do interesse público, são as condições que devem ser observadas pelo Poder Público para a realização do referido tratamento". Em outras palavras, a cautela que o ente público deverá ter, ao tratar dados privados, que podem se tornar públicos.

---

34 BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

35 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. Brasília, DF: Presidente da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 03 maio 2022.

36 LGPD, "Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:" (BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

37 BLUM, Renato Opice. **Proteção de dados**: Desafios e soluções na adequação à Lei. Rio de Janeiro: Forense, 2021. p. 89.

Nesse aspecto, Pinheiro[38] afirma que os dados pessoais se tornam públicos desde que preservada a boa-fé e a finalidade. Portanto, nessas situações, pode-se afirmar que os dados pessoais tornados públicos não podem ser originários de vazamento, por exemplo, ou, quando o próprio titular os tornam públicos, significando dizer que se trata de uma manifestação (intenção).

Outrossim, outra questão que se relaciona com o presente embate diz respeito ao tratamento de dados pela Administração Pública, que, segundo Cots e Oliveira[39], será necessário quando envolver execução de políticas púbicas (exemplos: políticas para implementação de saneamentos básicos, pagamentos de auxílios em geral, como o bolsa família, cadastramento de empresas que receberão incentivos fiscais etc.).

Carlotto e Guerra[40] destacam que, em "[...] situações que coloquem em exposição a saúde ou incolumidade física do titular ou de um terceiro", consagrar-se-á a proteção da vida ou da incolumidade física do titular ou de terceiros. No que diz respeito às relações de trabalho, os autores consideram que é um dever constitucional de tutelar o meio ambiente de trabalho. Logo, se deve ponderar as situações, aplicando-se os direitos e garantias fundamentais, sendo o direito à vida e a proteção integral do titular ou de terceiros os máximos pilares de importância inerente a proteção do titular dos dados.

Os artigos 7º, inciso VII, e 11, inciso II, alínea "e", da LGPD, tratam sobre a proteção da vida ou da incolumidade física do titular ou de terceiros:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...]
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; [...]
> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...]
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: [...]
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;[41]

---

38 PINHEIRO, Patricia Peck. **Proteção de dados pessoais comentários à Lei n. 13.709/2018 (LGPD)**. 3. ed. São Paulo: Saraiva Jur, 2021. p. 107.

39 COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 81.

40 CARLOTTO, Selma; GUERRA, Elaine. **Manual prático de adequação à LGPD com enfoque nas relações de trabalho**. São Paulo: LTr, 2021. p. 37-38.

41 BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022

Diante de alguns cuidados no âmbito da empresa, pode-se destacar alguns exemplos para o tratamento de dados pessoais, como a coleta de dados na portaria ou entrada da empresa, o uso de câmeras no ambiente de trabalho, acidentes com desaparecidos ou pessoas sequestradas.

Quando se fala em exercício regular de um direito em processo judicial, administrativo ou arbitral, os artigos 7º, inciso VI, e 11, inciso II, alínea "d", da LGPD, justificam a atuação do jurídico sem o consentimento (inclusive dados de funcionários):

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...]
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); [...]
> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...]
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: [...]
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);[42]

Veja-se que considerando o consentimento do funcionário, a finalidade e a boa-fé, enfim, diante de toda sistemática dentro de uma empresa, o dado privado terá caráter público (publicidade dentro de uma empresa, por exemplo, no site) e o dado público poderá ser utilizado no ramo privado, tudo a depender do legítimo interesse.[43]

Evidentemente, ante o caráter generalista da LGPD e às particularidades de cada dado (público ou privado) utilizado na empresa, com seu determinado ramo de atuação, diante da

---

[42] BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

[43] LGPD, "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; [...]. Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: [...] I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei. § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial." (BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

forma de acesso à determinada informação pelo funcionário e considerando-se, ainda, o tipo de dado manuseado, haverá implicação na avaliação de conduta, quando houver incidente de segurança de dados, podendo definir a gravidade de cada ato, ou seja, verificando-se o viés preventivo e punitivo da LGPD, salvaguardando as garantias e os direitos fundamentais das pessoas naturais e das pessoas jurídicas.

Nota-se que os dados podem ser considerados como públicos, naturais e todos consequentemente envolvem informações que demandam a valoração necessária para realizar escolhas em que os indivíduos terão que tomar, ao decidir compartilhar ou não um dado ou uma informação, o que demonstra a necessidade de uma análise analítica do ato recebido, se dado ou informação e a forma que isso será transmitido, uma vez que, a irregularidade acarreta em um vazamento ensejador de danos eventualmente irreparáveis.

No contexto do trabalho, há contato com todas as modalidades de dados, contudo, a transmissão desses dados pode ocasionar danos aos agentes, titulares de dados e consequentemente a empresa, sendo, portanto, necessária a avaliação da conduta do agente, especialmente pelos dados tratados durante a atividade empresarial, bem como, pela responsabilidade no que concerne ao dado manuseado, conforme ver-se-á adiante, a fim de verificar o cabimento de uma eventual penalidade sob a esfera da LGPD e CLT.

2.1.5 Dados manuseados por empregados em atividades empresariais

Como será visto no presente tópico, a depender do tipo de prestação de serviços, o dado poderá ser de caráter privado, se a atividade for do tipo privado, ou de caráter público, se a atividade se classifica como sendo do tipo pública. De qualquer modo, tanto uma empresa privada pode ter dados públicos, como uma empresa pública pode ter dados privados.

Tal observação é relevante, uma vez que com o fenômeno da globalização e da evolução dos sistemas de comunicação, as empresas de modo geral têm acessos a dados privados de clientes ou terceiros naturais. Ocorre que, na maioria das oportunidades de manuseio de dados pelos entes, independentemente de se tratar de dados privados ou públicos, quando se referem a dados de pessoas naturais que contenham raça, gênero, cor, documentos pessoais e cadastrais são considerados sensíveis e o vazamento pode gerar danos aos responsáveis pelo tratamento dos dados.

Dessa forma, todo e qualquer dado natural utilizado e tratado por um funcionário se enquadrará como sendo pessoal sensível, nos termos do artigo 5º, inciso II[44], da Lei 13.709/2018. Nesse aspecto, a exegese do inciso II, do artigo 5º, da Lei 13.709/2018, é mais específica, trazendo elementos próprios que estão fortemente presentes no cotidiano das empresas.

Outrossim, em determinados casos a empresa pode ser definida como "controladora" (Lei 13.709/2018, art. 5º,VI[45]) e o funcionário pode ser classificado como "operador" (Lei 13.709/2018, art. 5º, VII[46]), contudo, em cada caso concreto deverá ser analisada a operação realizada. Além disso, haverá momentos em que os dados poderão e deverão ser anonimizados[47], ou seja, os que eventualmente poderão ter acesso público. Portanto, os dados manuseados por empregados em atividades empresariais podem ser classificados como (*i*) pessoal; (*ii*) pessoal sensível; e (*iii*) anonimizado.

Sobre a relevância do tratamento de dados nas relações de trabalho, Sousa e Gonçalves[48] ponderam que embora o contexto das relações de trabalho pareça ser menos prioritário, ao se comparar com as áreas da saúde, do setor bancário (dados bancários) e do comércio (transações comerciais online), o tratamento de dados pessoais no âmbito laboral comporta uma análise cautelosa, uma vez que a execução de contrato de trabalho possui um ambiente próprio à gestão de um conjunto elevado de dados pessoais.

---

44 LGPD, "Art. 5º [...]; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;" (BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

45 LGPD, "Art. 5º [...]; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;" (BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

46 LGPD, "Art. 5º [...]; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;" (BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

47 LGPD, "III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;" (BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

48 SOUSA, Duarte Abrunhosa; GONÇALVES, Rui Coimbra. Da necessidade de conservação de dados pessoais dos trabalhadores no período pós-contratual. **Revista de Direito do Trabalho e Seguridade Social,** São Paulo, v. 212, v. 46, p. 119-145, jul./ago. 2020. p. 120.

Em complementação, Miziara e Mollicone [49] abordam as recentes alterações na legislação trabalhista e seus reflexos na questão da segurança de dados nas relações de trabalho, merecendo maiores explanações a questão relacionada aos limites do poder de direção do empregador, como por exemplo, o monitoramento da utilização de e-mails corporativos e pessoais, o uso de câmeras no ambiente de trabalho para o controle de condutas, entre outros.

Ou seja, o poder de direção visa justamente tentar diminuir os impactos relacionados aos incidentes de segurança de dados, detendo nitidamente o caráter da prevenção, ao tomar medidas cautelares. Veja-se que esse fator será reduzido por conta da educação digital que deve ser fornecida pelo empregador ao empregado justamente para cientificá-lo das regras e em decorrência disso, apresentar mecanismos de controle e transmissão indevida de dados.

É notório que as atividades laborais serão analisadas com o viés amplo da proteção de dados, na medida em que todo e qualquer contrato será elaborado com dados pessoais e sensíveis, justamente pela necessidade de qualificação das partes para nomeá-los corretamente no instrumento, bem como toda e qualquer operação, financeira ou administrativa, conterá informações que, se transmitidas, poderão descumprir os preceitos do controle de dados.

Veja-se que a discussão ora envolvida no presente tópico vislumbra a definição de LGPD e consequentemente o impacto no que concerne ao tratamento e transmissão de dados.

Sendo assim, fundamentalmente há a necessidade de contextualizar e instrumentalizar o empregador em suas atividades, deveres e poderes, na proteção de dados pessoais dos seus obreiros, garantindo o cumprimento tanto da legislação de proteção de dados quanto da trabalhista, além de esclarecer os principais impactos que a Lei Geral de Proteção de Dados impõe às relações de emprego.

Diante do presente cenário, é possível elencar que, apesar da inexistência de previsão de disposições laborais na LGPD, a referida legislação é aplicável nas esferas laborais a fim de suprir eventuais omissões porventura existentes, em ato complementar.

Em paralelo, empregados e empregadores manuseiam dados sensíveis, públicos ou privados durante a prestação de serviços, o que gera, portanto, um dever de responsabilidade sob as informações e dados recebidos, bem como, o dever de não os transmitir irregularmente.

Contudo, tal fato pode ser descumprido e gerar um vazamento de dados ao mundo externo capaz de prejudicar o agente titular dos dados e consequentemente a empresa que tinha o dever de guarda dos dados recebidos por conta dos preceitos da LGPD, o que demandará, por consequência, a instituição de um incidente de segurança para apuração da responsabilidade,

---

[49] MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2021. p. 233.

grau dos danos causados e consequentemente, punibilidade do agente, que serão abordados na sequência.

3 VAZAMENTO DE DADOS COMO UMA ESPÉCIE DE INCIDENTE DE SEGURANÇA

Ao se falar em vazamento de dados como uma espécie de incidente de segurança, prementemente se pensa em sanções, em punições e em apurações, preocupando-se nos impactos econômico, financeiro e principalmente, na imagem que pode repercutir, quando o vazamento ultrapassa os limites estabelecidos pela legislação, levando uma empresa, por exemplo, a enormes prejuízos.

Portanto, além do aspecto econômico, deve-se verificar a conduta do funcionário, que poderá agir com culpa ou com dolo, resultando-se nos elementos de aplicação da justa causa, a depender de cada situação, conforme se verificará mais adiante em capítulo próprio sobre o instituto da justa causa.

Sendo assim, o viés punitivo – tanto da LGPD como da CLT – reforça a primordialidade de se empregar boas condutas, a fim de se evitar históricos negativos de vazamento de dados.

3.1 Vazamento de dados à luz da LGPD

Popularmente, convencionou-se designar como vazamento de dados qualquer problema relacionado a incidentes de informação, contudo, tal convenção carece de complementação, uma vez que o vazamento de dados é uma espécie de incidente de segurança.

Os incidentes de segurança são definidos, segundo o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), como um "simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer operações de negócio de uma organização".[50] Ainda, tomando por base os conceitos clássicos de segurança da informação, pode-se definir um incidente de segurança como "qualquer evento adverso, confirmado ou suspeito, que afete a tríade da segurança da informação: confiabilidade, integridade ou disponibilidade dos dados".[51] Logo, tal conceito não

---

50 SISTEMA DE ADMINISTRAÇÃO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO (SISP). Tratamento de Incidentes. *In:* PORTAL SISP, 2019. Disponível em: https://www.gov.br/governodigital/pt-br/sisp. Acesso em: 09 nov. 2020.

51 PALMA, Fernanda. Incidentes de segurança da informação: conceitos, exemplos e cases. *In:* PORTAL GSTI, 2014. Disponível em: https://www.portalgsti.com.br/2014/01/incidentes-de-seguranca-da-informacao-conceito-exemplos-e-cases.html#:~:text=Segundo%20CERT.br%2C%20um%20incidente%20de%20seguran%C3%A7a%20pode%20ser,sob%20risco%20%C3%A9%20considerado%20um%20incidente%20de%20seguran%C3%A7a. Acesso em: 09 nov. 2020.

se resume tão somente ao vazamento ou exposição de dados, sendo algo muito mais amplo do que uma brecha de segurança.

Veja-se que a LGPD não foi taxativa ao definir o que é um incidente de segurança. Em seu artigo 46, a Lei arrola, de forma exemplificativa, algumas possíveis situação que se encaixam naquele conceito, como acessos não autorizados e situações acidentais ou ilícitas, de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito. *In verbis*:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.[52]

Por sua vez, a Autoridade Nacional de Proteção de Dados conceitua incidente de segurança com dados pessoais como:

> [...] qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.[53]

Diante dessa definição, é possível compreender que o incidente de segurança é gênero e o vazamento de dados é espécie, sendo elemento grave ao se verificar violação, seja ela acidental, seja ela ilícita.

Nesse contexto, se pode citar os seguintes exemplos de incidentes de segurança: (*i*) perda ou roubo de dispositivos físicos, tais como notebooks ou pen-drive; (*ii*) perda ou roubo de documentos que contenham dados pessoais de clientes, empregados e fornecedores; (*iii*) acesso não autorizado a dados pessoais; (*iv*) em virtude de "erro humano", a divulgação inadequada de dados pessoais; e (*v*) a divulgação de dados pessoais em virtude de um golpe, como resultado de procedimentos inadequados de verificação de identidade, além de outras espécies existentes.

---

52 BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

53 BRASIL. Autoridade Nacional de Proteção de Dados. **Incidentes de Segurança com dados pessoais e sua avaliação para fins de comunicação à ANPD**. Brasília, DF, 22 fev. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 28 set. 2022.

Cots e Oliveira[54] destacam a imperatividade da norma aduzindo que "[...] vale notar que o verbo 'devem' é impositivo da lei, ou seja, não se trata de faculdade: é uma obrigação legal que, se não cumprida, poderá ensejar a aplicação de sanções administrativas e responsabilidade civil". Diante disso, necessário também se pautar pela experiência estrangeira, principalmente no contexto da General Data Protection Regulation (GDPR) da União Europeia, cuja definição de incidentes de segurança perpassa uma análise maior dos riscos de segurança, dos impactos na vida, autodeterminação, desenvolvimento da personalidade dos indivíduos e das práticas para tratamento dos dados em curso.

A GDPR, em seu artigo 4 (12), define "incidentes de dados pessoais, ou personal data breach", como a violação de segurança que conduz à "destruição, perda, alteração, divulgação ou acesso não autorizados, de maneira acidental ou ilícita, de dados pessoais transmitidos, armazenados ou tratados de qualquer outra maneira".[55] Em síntese, tomando por base três importantes princípios da segurança da informação, tais incidentes se categorizam como incidentes de (*i*) confidencialidade; (*ii*) integridade; e (*iii*) disponibilidade. Isso posto, de acordo com essa classificação, existem três tipos de incidentes de segurança. O primeiro, o incidente de confiabilidade, abrange as ocorrências em que ocorre a divulgação ou o acesso não autorizado a dados pessoais. O segundo, o incidente de integridade, ocorre quando há alguma alteração acidental ou não autorizada dos dados e, por fim, o incidente de disponibilidade se dá quando há a perda de acesso ou destruição, acidental ou não autorizada, desses dados.

Por conseguinte, a avaliação dos riscos de cada ocorrência independe da categoria em que se insere, estando sujeita à avalição casuística, considerando especificidades de cada uma, como a natureza do incidente, a natureza e o volume dos dados e a gravidade das consequências. Ademais, o grau de risco também pode variar ao longo do tempo, diante das inovações tecnológicas e o estado das medidas de segurança e mitigação de riscos disponíveis no mercado. Neste contexto, percebe-se a importância da documentação dos procedimentos envolvidos no tratamento de dados, posto que caberá aos agentes de tratamento avaliar se o risco colocado ao titular pelo incidente é alto suficiente para ensejar a notificação da ocorrência seja ao próprio titular e/ou à autoridade de proteção dos dados. A título de informação, cabe dizer que a Information Commissioner´s Office (ICO), autoridade de proteção de dados do Reino Unido,

---

54 COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 186.

55 Art. 4 (12) da GDPR. "Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized of, or access to, personal data transmitted, stored or otherwise processed". (EUROPEAN UNION. **General Data Protection Regulation (GDPR)**. May 25, 2018. Disponível em: https://gdpr-info.eu/art-12-gdpr/. Acesso em: 12 abr. 2022).

por exemplo, determina a notificação de incidentes que "coloquem em risco direitos e liberdades das pessoas", excluindo dessa obrigação os casos que não ofereçam "riscos para além da inconveniência dos agentes de tratamento de dados". Por sua vez, a autoridade francesa de proteção de dados, a Commission Nationale de L´informatique et des Libertés (CNIL), determina que deverão ser notificados os incidentes que "coloquem em risco a vida privada dos titulares, ou seja, os que sejam de risco elevado".

Como visto, delimitar o conteúdo normativo da expressão "incidente de segurança" demanda uma avaliação de risco que considera as especificidades de cada caso, a natureza dos dados e os indivíduos envolvidos. Demanda, também, um compromisso com a transparência de dados e a prestação de contas, conforme previsto no artigo 5º, inciso X, da própria LGPD. De qualquer modo, apesar de não apresentar definição taxativa do que seja incidente de segurança, a LGPD converge com a GDPR ao estabelecer a adoção de medidas visando "proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, comunicação, alteração ou qualquer outra forma de tratamento inadequado ou ilícito", mas difere da norma europeia ao configurar como incidente de segurança o "tratamento inadequado ou ilícito".

No mesmo sentido, à luz do GDPR, serão o risco ou os danos relevantes aos titulares, os critérios balizadores para a tomada de decisão do controlador em comunicar à ANPD e o titular dos dados pessoais acerca dos incidentes de segurança havidos sob sua responsabilidade, como expõe o artigo 48, *caput*, da LGPD, convergindo para a hipótese de vazamento de dados.

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.[56]

Portanto, as empresas devem adotar medidas de segurança, a fim de assegurar que não ocorra vazamento de dados, adequando-se aos procedimentos e processos de segurança inerentes ao tratamento dos dados, haja vista que, a irregularidade nesse controle gera o descumprimento da legislação e consequentemente as penalidades previstas na Lei.

---

[56] BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

3.2 Sanções ao cometer violações à Lei Geral de Proteção de Dados

A LGPD é rigorosa quanto à aplicação das sanções, quando se configura ato ilícito. E assim tem que ser, pois, como visto, o vazamento de dados pode prejudicar milhões de vidas, pode destruir economias, a nível local e mundial.

Reza o artigo 52 da LGPD que as infrações cometidas podem ocasionar, advertências, multas com um limite total de até R$ 50.000.000,00 (cinquenta milhões de reais, publicização da infração, bloqueio e eliminação de dados pessoais, suspensão parcial do funcionamento do banco de dados pelo período máximo de 06 (seis) meses, bem como, proibição total ou parcial a atividade relacionada ao tratamento de dados[57].

Vale ponderar inclusive que o artigo 54 da LGPD prevê a necessidade de apuração do grau da conduta para valoração da multa a ser aplicada, bem como, o prejuízo ocasionado ao titular dos dados:

> Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.
> Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.[58]

Como pondera Justen Filho[59], "não se admite o silêncio legislativo e nem a adoção de cláusula legislativa geral, delegando à Administração a competência discricionária para

---

[57] LGPD, "Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes *sanções administrativas* aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

[58] BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

[59] JUSTEN FILHO, Marçal. **Curso de Direito Administrativo**. 12. ed. São Paulo: Revista dos Tribunais, 2016. p. 460.

determinar os ilícitos e escolher as sanções a eles correspondentes", sob pena de gerar insegurança jurídica. Logo, é basilar que a lei defina e individualize cada uma das sanções cabíveis, deixando à avaliação do administrador, tão somente, a interpretação do caso concreto e a dosimetria da pena, momentos em que também estará sujeito a outros princípios da Administração Pública, a proporcionalidade e a razoabilidade.

Inicialmente, pode-se dizer que as sanções administrativas apresentam dois objetivos distintos: (*i*) ressarcimento de danos; e (*ii*) retribuição. Uma vez que a ressarcitória tem seu fundamento nos artigos 186, 187 e 927 do Código Civil, destinando-se aos prejudicados, pode-se concluir, pela previsão do artigo 52 da LGPD, que as sanções ali previstas não se destinam a tal fim, caracterizando-se como retributivas, imputando ao agente infrator o mal causado de acordo com o ato ilícito por ele praticado e com o intuito de evitar a prática de novos atos igualmente ilícitos. Nesse contexto, vê-se que o artigo 52 é claro ao estabelecer que as sanções são aplicadas "em razão das infrações cometidas às normas previstas nesta Lei". Considerando-se que o legislador não fez qualquer distinção no artigo, afirma-se que as penalidades serão aplicadas a qualquer infração à LGPD**,** incluindo àquelas menos objetivas, como a não observância dos princípios.

O rol de sanções do artigo 52 é exaustivo, concentrando todas as hipóteses possíveis, não havendo outras a serem aplicadas na esfera administrativa. Contudo, isso não significa que, no âmbito judicial, o juiz não possa aplicar outras sanções que entenda necessário para a efetividade de sua tutela, bem como, o próprio artigo 52, §2º, também permite que sanções administrativas, civis e penais, definidas em outros diplomas legais, sejam aplicadas, como aquelas previstas no Código de Defesa do Consumidor, por exemplo.

De acordo com o destacado por Alves[60], é ponderado na doutrina a convergência semântica entre o Direito Penal e o Direito Sancionatório, posto o seu propósito punitivo. Assim, é pacífica a jurisprudência que admite a aplicação de preceitos e princípios próprios do Direito Penal na seara sancionatória, ainda que administrativa, em especial os princípios da taxatividade e da legalidade, mesmo que venha a ser utilizado em prejuízo do agente infrator. Para sustentar o que alega, o autor colaciona o seguinte julgado para reflexão:

> Constitucional e penal. Acessórios de celular apreendidos no ambiente carcerário. Falta grave caracterizada. Inteligência do art. 50, II, da Lei 7.210/84, com as alterações introduzidas pela Lei 11.466/2007. Inexistência de ofensa ao princípio da reserva legal. Interpretação Extensiva. Possibilidade.

[60] ALVES, Fabrício Mota. Da Fiscalização. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **LGPD – Lei Geral de Proteção de Dados Comentada**. São Paulo: Revista dos Tribunais, 2019. p. 366.

> Precedente. 1. Pratica infração grave, na forma prevista no art. 50, VII, da Lei 7.210/84, com as alterações introduzidas pela Lei 11.466/2007, o condenado à pena privativa de liberdade que é flagrado na posse de acessórios de aparelhos celulares em unidade prisional. 2. A interpretação extensiva no direito penal é vedada apenas naquelas situações em que se identifica um desvirtuamento na mens legis. 3. A punição imposta ao condenado por falta grave acarreta a perda dos dias remidos, conforme previsto no art. 127 da Lei 7.210/84 e na Súmula Vinculante n. 9, e a consequente interrupção do lapso exigido para a progressão de regime. 4. Negar provimento ao recurso (STF, RHC 106.481, rel. Min. Carmen Lúcia, 1ª T. j. 08.02.2011).[61]

Esse julgado demonstra a extensão da aplicação do Direito Penal ao âmbito sancionador, pois no caso concreto ilustrado, o agente cometeu uma falta grave e diante da infração, houve a extensão dos efeitos da punição, uma vez que como o agente já estava cumprindo pena e em decorrência da nova ilicitude cometida, houve nova punição em razão da falta grave cometida. Logo, ao se tratar de justa causa em razão de incidentes de segurança de dados, especialmente, no vazamento de informações e dados sensíveis, além do aspecto reparatório da LGPD, seja por intermédio de multa, suspensão ou advertência punitiva, é possível estender a validade dos efeitos no aspecto laboral para o agente responsável pelo ato praticado.

Vale observar que a LGPD prevê a adoção de diversas sanções (gênero), as quais poderão ser aplicadas de forma gradativa, desde uma simples advertência até a aplicação de multa, que apresenta o percentual de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração. Evidentemente, os valores elevados circundam a economia como um todo, pois imagina-se a aplicação de uma multa de R$ 50.000.000,00 (cinquenta milhes de reais), por exemplo, em decorrência da prática de 20 (vinte) infrações tipificadas.

Será que o viés punitivo da LGPD no âmbito laboral retira o valor social do trabalho? Isso promoverá a cultura digital e a educação digital? Ou, o inverso, a cultura e a educação digital podem influenciar na mudança do ambiente de trabalho? Tais questões serão abordadas no transcorrer da dissertação, contudo, é notório o caráter punitivo e regulador da LGPD.

Veja-se que o viés punitivo da LGPD visa proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural e o

---

[61] ALVES, Fabrício Mota. Da Fiscalização. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **LGPD – Lei Geral de Proteção de Dados Comentada**. São Paulo: Revista dos Tribunais, 2019. p. 366.

caráter social do trabalho é independente, sempre esse aspecto social deve estar presente nas relações de trabalho.

A promoção da cultura digital e da educação digital é questão que exige tempo, tratando-se de um processo paulatino, mas que deve ser divulgada, incentivada e traçada estratégias de ampliação na sociedade. Na globalidade social, muitas empresas serão as maiores protagonistas de suporte, para que os seus colaboradores estejam atentos às práticas digitais.

Consequentemente, a cultura e a educação digital podem influenciar na mudança do ambiente de trabalho e o ambiente de trabalho pode influenciar na ampliação da cultura e da educação digital.

Veja-se que não se trata de questões fáceis e o processo para se alcançar determinadas diretrizes requerem conjuntura de apoio, tanto do funcionário como da empresa e da sociedade no que concerne ao cumprimento da norma inerente ao controle e proteção dos dados

Aqui se aplica a equação de que "para chegar numa sanção", operou-se o insustentável, ou seja, a quebra de confiança na relação entre a empresa e o funcionário. Funciona como uma espécie de ultima ratio, assim como é o Direito Penal e assim como é a aplicação da justa causa no Direito do Trabalho. Nesse ponto, Pinheiro [62] afirma que "a imputação de sanções administrativas faz com que os entes responsáveis pelo tratamento de dados pessoais atentem-se à garantia da segurança das informações que estão utilizando". Dessa forma, a atenção plena que os responsáveis pelo tratamento de dados (agentes de tratamento de dados) terão que ter é muito séria, ou seja, a LGPD tem a raiz da aplicação de seus dispositivos em caráter preventivo.

No caso concreto aqui analisado, discutido e em fase de reflexão, parece que a empresa não adotou critérios preventivos para que o ex-funcionário não compartilhasse dados. Todavia, parece também que fugiu da alçada da empresa, uma vez que ela não poderia prever que uma pessoa compartilharia uma planilha com diversos dados sigilosos. Nesse cenário, indaga-se se a justa causa é uma sanção quando se trata da LGPD? E quanto às aplicações normativas, na ausência de regras e de sanções específicas na LGPD relacionadas ao Direito do Trabalho, a CLT pode ser interpretada no contexto de incidentes de segurança?

A justa causa é o reflexo no cometimento de infração (ilicitude) envolvendo a LGPD, regendo-se as relações de trabalho, conforme os princípios da proporcionalidade e da razoabilidade. Além disso, à luz da segurança jurídica e do princípio da legalidade, a LGPD poderia elencar situações expressas relacionadas ao Direito do Trabalho, sendo que por ora, a CLT pode ser interpretada no contexto de incidentes de segurança.

---

62 PINHEIRO, Patricia Peck. **Proteção de dados pessoais comentários à Lei n. 13.709/2018 (LGPD)**. 3. ed. São Paulo: Saraiva Jur, 2021. p. 155.

Ainda, sobre a aplicação do princípio da proporcionalidade, Pinheiro[63] esclarece que as sanções devem sempre observar a proporcionalidade, como sendo um critério de prevenção e de inibição de abusos do poder estatal. Isso porque, as novas leis que regulam as matérias relacionadas à proteção de direitos no âmbito da transformação digital impactam imensamente nos modelos de negócios, sendo que uma das formas para que se possa cumprir a lei consiste na previsão de penas altas. No entanto, é preciso existir uma dosagem das penas, sob pena de impactar diretamente a pequena empresa ou mesmo os projetos de maior inovação que tendem a assumir mais riscos operacionais.

Sendo assim, o princípio da proporcionalidade é primordial na tentativa de impedir o cometimento de desvios, de abusos e de ilegalidades na aplicação da lei pelo poder estatal.

Segundo pesquisa divulgada pelo Correio Braziliense, apenas 11% das instituições estão em conformidade com a LGPD:

> Pesquisas realizadas entre novembro/2020 e fevereiro/2021 apontam que somente 11% das instituições estão em conformidade com a lei. Como se vê, a adesão ainda é muito baixa. Falta conscientização a respeito da importância do novo regramento, o que naturalmente aconteceria com a aplicação das sanções administrativas pela Autoridade Nacional.[64]

Consubstancialmente, a LGPD determina diversos regramentos, cujo objetivo é alcançar a proteção de dados pessoais. Para tanto, impõe a observação de inúmeros princípios, os quais certamente se correlacionam no âmbito laboral e cuja violação acarreta sanções.

Verifica-se que os princípios aplicáveis às relações de trabalho são: (*i*) finalidade, (*ii*) necessidade, (*iii*) adequação, (*iv*) transparência, (*v*) segurança, (*vi*) qualidade, (*vii*) livre acesso, (*viii*) não discriminação, (*ix*) prevenção e (*x*) responsabilidade e prestação de contas. Especialmente, segundo afirmam Carloto e Guerra[65], considerando a transparência de todos os tratamentos de dados dos funcionários, as empresas deverão informar sobre o que farão com os dados obtidos nessa relação entre empresa e trabalhador, observando-se a boa-fé, a finalidade e a necessidade, ante a necessidade de controle e apresentação aos titulares dos dados, cumprindo-se as determinações da LGPD.

---

63 PINHEIRO, Patricia Peck. **Proteção de dados pessoais comentários à Lei n. 13.709/2018 (LGPD)**. 3. ed. São Paulo: Saraiva Jur, 2021. p. 157-158.

64 STRICKLAND, Fernanda; ÍCARO, Pedro. Sanções da LGPD estão em vigor e instituições devem ficar atentas às novas normas. **Correio Braziliense,** Brasília, 1º ago. 2021. Disponível em: https://www.correiobraziliense.com.br/politica/2021/08/4941113-sancoes-da-lgpd-entram-em-vigor-e-instituicoes-devem-ficar-atentas-as-novas-normas.html. Acesso em: 11 fev. 2022.

65 CARLOTO, Selma; GUERRA, Elaine. **Manual Prático de Adequação à LGPD com enfoque nas relações de trabalho**. São Paulo: LTr, 2021. p. 55-56.

Assim, consagrar-se-á o equilíbrio do viés preventivo, a aplicação da sanção e o respeito aos princípios máximos da LGPD, em total ação com as normas trabalhistas.

Desta forma, elencando-se o escopo da LGPD, a generalidade da legislação e as penalidades impostas pelo descumprimento, far-se-á necessário adentrar ao conjunto de regramento trabalhistas e especificamente as modalidades de punição aos empregados no controle de dados naturais de clientes para imputar a efetiva responsabilidade pelos atos praticados, o que demandará, por consequência, a análise do escopo da justiça laboral, responsabilidade civil dos agentes e enquadramento da LGPD nas demandas envolvendo empregador e empregador.

4 DISTINÇÃO ENTRE RELAÇÃO DE EMPREGO E DE TRABALHO E O INSTITUTO DA JUSTA CAUSA

Conforme já anteriormente exposto, a generalidade da LGPD acarreta na possibilidade de aplicação imediata dos efeitos da legislação em todos os setores sociais, econômicos e legais. Por tal cenário, a CLT, admitindo-se a aplicação de legislações complementares, pode utilizar-se de preceitos, conceitos e determinações legais da LGPD para, em conjunto da legislação, aplicar punições e imputar responsabilidades a agentes que tratam dados, sejam sensíveis, naturais ou de terceiros.

A distinção entre relação de emprego e de trabalho e a visualização do instituto da justa causa serão necessárias, diante das inúmeras relações de trabalho (gênero) que abrangem as diversas relações de emprego (espécies), sendo que ambos serão determinantes para se aplicar ou não a justa causa, pois, por exemplo, diante de um contrato de prestação de serviços, é evidente que podem existir justos motivos para que se opere rescisão contratual, porém, para cada modalidade de relações de emprego avaliar-se-á o tipo de punição, bem como, a responsabilidade de cada agente nas funções exercidas.

Portanto, em detrimento dos diversos tipos de punições existentes (enquadrando-se, inclusive, procedimentos administrativos) no âmbito trabalhista, o grau da ilicitude se relacionará com o tipo de punição (advertência, suspensão, inquérito administrativo e justa causa) e em decorrência do ato praticado, as opções do empregador no cumprimento das regras estabelecidas.

Mediante tal escopo e consequentemente da apuração da responsabilidade sob o âmbito da LGPD, a conduta do agente será valorada para aplicação da penalidade pertinente em decorrência da avaliação do ato praticado.

4.1 Escopo e objeto da Justiça do Trabalho

Sem delongar quanto aos aspectos históricos da Justiça do Trabalho, bem como aos seus demais aspectos e riqueza do processo até a efetiva consolidação, se faz necessário apresentar as definições de trabalho e de relação de trabalho, para melhor compreender o que de fato a Justiça do Trabalho julga.

Segundo Pinto Martins[66], trabalho é "[...] o esforço decorrente da atividade humana visando à produção de uma utilidade. É um fator da produção. É o fim da atividade econômica, tendo por objetivo gerar riquezas". Por sua vez, a relação de trabalho "[...] é o gênero que abrange a relação de emprego como espécie. Tem sentido mais amplo. Compreende o trabalho humano".

Nesse diapasão, é imperioso destacar o artigo 114 da Constituição Federal, que aduz sobre a competência da Justiça do Trabalho, contém, em seu inciso I, a previsão do processamento e do julgamento das ações oriundas da relação de trabalho, abrangendo, inclusive, os entes de direito público externo e da administração pública direta e indireta da União, dos Estados, do Distrito Federal e dos Municípios. Ou seja, quando envolver violações à LGPD dentro do ambiente laboral e do contexto da relação de trabalho, a Justiça do Trabalho é competente para julgar as ações.

Ainda, segundo Pinto Martins[67], "Toda relação de emprego é uma relação de trabalho, mas nem toda relação de trabalho é de emprego, como a dos funcionários públicos, dos trabalhadores autônomos".

Oportunamente, Amauri Mascaro Nascimento e Sônia Mascaro Nascimento [68] apresentam a seguinte definição de relação de trabalho, citando Potthoff, no sentido que se trata de uma relação de organização jurídico-social na qual não há troca de bens ou valores patrimoniais, porém, um homem que se compromete a si próprio a prestar serviços mediante sua atividade própria em benefício de outrem.

Ambas as definições tratam do cunho organizacional das relações de trabalho, figurando o homem como o elemento central do labor, pois é o ser humano a força motriz da sociedade e desenvolvedor da produtividade.

Os autores, referendando Mario de La Cueva e Evaristo de Moraes, também aduzem sobre a definição de relação de emprego, suscitando que se trata de um acordo bilateral de vontades prevendo direitos e obrigações, mediante a prestação de serviços por pessoa natural, regrados de direitos e obrigações, recebendo uma contraprestação mensal pelas atividades realizadas, formalizando-se tal ato por intermédio de contrato elaborado para o referido fim[69].

---

66 MARTINS, Sergio Pinto. **Direito Processual do Trabalho.** 41. ed. São Paulo: Saraiva Jur, 2019. p. 170-171.

67 MARTINS, Sergio Pinto. **Direito Processual do Trabalho.** 41. ed. São Paulo: Saraiva Jur, 2019. p. 175.

68 NASCIMENTO, Amauri Mascaro; NASCIMENTO, Sônia Mascaro; **Curso de Direito do Trabalho.** 29. ed. São Paulo: Saraiva, 2014. *E-book*. p. 451-452.

69 NASCIMENTO, Amauri Mascaro; NASCIMENTO, Sônia Mascaro; **Curso de Direito do Trabalho.** 29. ed. São Paulo: Saraiva, 2014. *E-book*. p. 455.

Veja-se que pelas definições ora suscitadas, a relação empregatícia e laboral é regida por um ser central, que prestará serviços ora contratados, formalizados por um contrato específico para o referido fim, recebendo-se uma contraprestação pelo ato realizado, mediante um conjunto de regras e direitos que se descumpridos, gerar a possibilidade de indenização ou responsabilização pelo ato praticado.

A relação de emprego é algo concreto e firmado em caráter contratual, vinculando as partes ao ônus das responsabilidades e deveres recíprocos. Por sua vez, a relação de trabalho é um comprometimento com a atividade sem vínculo específico entre as partes envolvidas. Desse modo, a diferenciação entre ambas é regida pela formalidade e cumprimento dos requisitos legais previstos na Consolidação das Leis Trabalhistas (CLT).

Ainda, se faz necessário verificar o conceito de contrato de trabalho, que, segundo Pinto Martins[70], é "[...] o negócio jurídico firmado entre empregado e empregador sobre condições de trabalho", nesse caso, aplicável às relações empregatícias acima citadas. Significa dizer que, quando o funcionário descumpre o negócio jurídico firmado com o empregador, poderá ensejar em justa causa, à luz do princípio da continuidade da relação de emprego. Nesse ponto reside uma questão importante, pois, quando se fala em aplicação de justa causa, que possui previsão legal no artigo 482, da CLT, também se está falando do instituto da responsabilidade civil, assunto que será melhor detalhado mais adiante.

Falar em demissão por justa causa é falar na ultima ratio no Direito do Trabalho. É dizer que há o rompimento, o término de uma relação contratual. Embora, inicialmente, possa parecer que esse término se dá de forma unilateral, ao final, verifica-se a sua bilateralidade, pois se dá por motivos relevantes, tanto para quem pratica o ato ensejador da justa causa (falhas), quanto para quem toma a decisão de demitir. Pode-se dizer que se forma uma relação insustentável entre empresa e funcionário, quando o ato final é a demissão por justa causa. Lembrando que para toda causa justa, há um justo motivo. Esse é exatamente o ponto-chave para se configurar uma demissão por justa causa.

E é justamente sobre o limite do relacionamento divergente, ou melhor dizendo, sobre os excessos cometidos pelo funcionário, que se faz necessária a presente abordagem acerca da demissão por justa causa. Considerando fortemente o contexto atual, falando-se em demissões acentuadas, numa vertigem célere que reflete imensamente na economia do Brasil. Afinal, se falar sobre demissão é algo que preocupa a muitos, ponderar sobre a demissão por justa causa é mais preocupante ainda, principalmente para quem cometeu o ato grave, resultando numa

---

[70] MARTINS, Sergio Pinto. **Direito Processual do Trabalho.** 41. ed. São Paulo: Saraiva Jur, 2019. p. 171.

mácula que não pode impedir a recolocação profissional, pois viola o princípio da continuidade da relação de emprego.

Atualmente, por exemplo, tem se levantado a seguinte questão: "o funcionário que se recusa a tomar vacina contra Covid-19 pode ser demitido por justa causa?". Acima disso, "o funcionário que compartilhou dados pode ser demitido por justa causa?". Questões complexas, que dividem a interpretação lógica jurídica, culminando em inúmeros caminhos ensejadores de reflexão, tanto para quem acha que é aplicável a justa demissão, quanto para quem considera que não se aplica o justo motivo demissional.

Dessa forma, é primordial ponderar sobre (*i*) o conceito e os requisitos da demissão por justa causa e (*ii*) as hipóteses de demissão por justa causa; questões que geram dúvidas, impactando em tomadas de decisões e riscos para muitas empresas, bem como, a responsabilidade civil dos agentes em decorrência do incidente de segurança pelo vazamento de dados, enquadrando-o nas penalidades celetistas existentes de acordo com a gravidade da conduta. E quando se fala em violações à LGPD, as dúvidas quanto à aplicação ou não da rescisão contratual por justo motivo são ampliadas.

4.2 A demissão por justa causa e o tratamento no Direito Brasileiro

A demissão por justa causa é uma espécie do gênero "rescisão"[71]. Segundo Maurício Godinho Delgado[72], trata-se da rescisão do contrato de trabalho em decorrência de falta grave praticada pelo funcionário. Para que a demissão por justa causa seja válida, os seguintes requisitos devem ser observados: (*a*) tipicidade – o ato praticado deve ser enquadrado em uma das hipóteses previstas em lei (CLT, art. 482); (*b*) atualidade - praticada na mesma ocasião a

---

[71] Amauri Mascaro Nascimento elucida três sistemas fundamentais de justa causa: o genérico, o taxativo e o misto. Segundo Mascaro, "O sistema genérico é aquele em que uma lei autoriza o despedimento do empregado sem mencionar ou tipificar as diferentes hipóteses casuísticas, mas apenas apontando em tese e de modo amplo uma definição geral e abstrata. Nos casos concretos submetidos à decisão judicial, é feita ou não a subsunção do fato à norma, segundo o critério de valor do julgador". Por sua vez, "No sistema taxativo, do Brasil, a lei enumera os casos de justa causa, fazendo-o exaustivamente. Desse modo, somente a lei é fonte formal típica. Impossível será a estipulação de justa causa por meio de outras normas jurídicas, como as convenções coletivas de trabalho, os regulamentos de empresa etc. Argumenta-se que esse sistema dispensa maior proteção ao trabalhador, porque restringe as hipóteses faltosas, e permite às partes e aos Tribunais do Trabalho um critério mais rigoroso e seguro de apreciação dos casos concretos. A julgar pela experiência brasileira, pouca ou nenhuma diferença haveria entre o sistema genérico e o taxativo, tão amplas são as causas previstas em nossa lei, de modo a ser possível enquadrar sempre um ato eticamente reprovado". E por fim, "O sistema misto é o resultado da combinação dos dois critérios anteriores. A lei, além de enumerar as hipóteses de justa causa, é também genérica, permitindo que seja considerado como tal um fato mesmo não contido na descrição legal". (NASCIMENTO, Amauri Mascaro; NASCIMENTO, Sônia Mascaro; **Curso de Direito do Trabalho.** 29. ed. São Paulo: Saraiva, 2014. *E-book*. p. 928-929).

[72] DELGADO, Mauricio Godinho. **Curso de direito do trabalho**. 17. ed. São Paulo: LTr, 2018. p. 176.

que se segue a rescisão contratual, perdendo a eficácia uma falta pretérita, ocorrida muito tempo antes; como consequência da atualidade, tem-se (*b.1*) imediatidade – a punição deve ser imediata a fim de que não ocorra o perdão tácito; (*c*) gravidade da conduta – em outras palavras, a justa causa deve ser grave para autorizar o despedimento do funcionário. Uma falta leve cometida pelo trabalhador não será reconhecida tecnicamente como justa causa; (*d*) não dupla punição – em homenagem ao Direito Penal, o Direito do Trabalho adota o princípio do *non bis in idem*, significando que a mesma falta do funcionário não pode ser duplamente punida. Punir duplamente a mesma transgressão quer dizer aplicar uma penalidade pela segunda vez ao mesmo funcionário sem que nada tenha feito além do que já fez.

Somando-se aos termos anteriormente apresentados, segue em continuação ao rol: (*e*) não discriminação – demitir um funcionário por justa causa e aplicar advertência para outro funcionário, para uma mesma falta considerada grave, no mesmo contexto, por exemplo. É vedada a discriminação nesse caso; e (*f*) nexo de causa e efeito – entre a justa causa e a rescisão do contrato de trabalho deve haver um nexo de causa e efeito, de tal modo que esta é determinada diretamente por aquela.

Aprofundando sobre o instituto da despedida por justa causa, faz-se necessária a observação das hipóteses pormenorizadas, em outros dizeres, estar-se-ão observando o rol (taxativo) para constituir justa causa ensejadora da rescisão do contrato de trabalho pelo empregador, previsto no artigo 482 da Consolidação das Leis do Trabalho (tipicidade).

A CLT, no seu artigo 482, alíneas de “a” a “m” e parágrafo único, determina que caracterizam justa causa para rescisão contratual as seguintes hipóteses ou motivos propriamente ditos: (*i*) improbidade; (*ii*) incontinência de conduta; (*iii*) negociação habitual no ambiente de trabalho; (*iv*) condenação criminal do empregado; (*v*) desídia no desempenho das respectivas funções; (*vi*) embriaguez habitual ou em serviço; (*vii*) violação de segredo da empresa; (*viii*) ato de indisciplina ou de insubordinação; (*ix*) abandono de emprego; (*x*) ofensas físicas, tentadas ou consumadas; (*xi*) prática constante de jogos de azar; e (*xii*) perda da habilitação profissional.

Igualmente, constitui justa causa para dispensa de funcionário, a prática, devidamente comprovada em inquérito administrativo, de atos atentatórios à segurança nacional. Por fim, também que configuram justa causa (*i*) a recusa do ferroviário de fazer horas extras em casos de urgência ou acidente (CLT, art. 240); (*ii*) a participação em greve abusiva e os excessos praticados durante a greve (CF, art. 9º, § 2º); e (*iii*) a recusa injustificada do empregado de observar as instruções expedidas pelo empregador e de usar equipamentos de segurança do trabalho (CLT, art. 158, parágrafo único).

Configurar e aplicar a demissão por justa causa depende de cada caso em concreto. É primordial verificar o preenchimento de todos os requisitos necessários à sua configuração, pois os sujeitos da relação contratual de trabalho se confrontarão com máxima de pôr fim ou não à relação de emprego, especialmente, a conduta do agente que praticou o ato, a extensão do dano e os impactos decorrentes da ação no ambiente laboral ou perante terceiros.

Vale ressaltar, que não há atualização em referida disposição em decorrência dos preceitos da LGPD, o que demanda, portanto, análise específica dessa questão sob tal preceito de aplicabilidade perante os vínculos empregatícios. Contudo, a referida legislação, por seu caráter geral, tem expressa aplicabilidade nas atividades e preceitos laborais e possibilidade de enquadramento nos preceitos e alíneas do artigo 482 da CLT.

Ainda assim, a análise do caso concreto será realizada a partir das possíveis provas apresentadas pelo empregador, conforme preceitos do artigo 818 da CLT[73], uma vez que deve ser comprovado o cumprimento dos requisitos da legislação para confirmar a legalidade da justa causa.

4.3 Modalidades de punição sob o âmbito trabalhista: advertências, suspensão e inquéritos administrativos

Além da justa causa ora narrada, há ainda outras possibilidades de punições que o empregador pode direcionar ao empregador em decorrência de condutas faltosas ou em desrespeito às normas laborais em geral, o que será sempre avaliado pela gravidade e dano decorrente do ato realizado.

O artigo 158, parágrafo único[74], da CLT, prevê que constitui ato faltoso do empregado a recusa injustificada à observância das instruções expedidas pelo empregador, na forma do item II[75], do artigo 157, da CLT); e a recusa ao uso dos equipamentos de proteção individual

---

[73] CLT, "Art. 818. O ônus da prova incumbe: I - ao reclamante, quanto ao fato constitutivo de seu direito; II - ao reclamado, quanto à existência de fato impeditivo, modificativo ou extintivo do direito do reclamante." (BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 12 abr. 2022).

[74] CLT, "Art. 158 - Cabe aos empregados: [...] Parágrafo único - Constitui ato faltoso do empregado a recusa injustificada: a) à observância das instruções expedidas pelo empregador na forma do item II do artigo anterior; b) ao uso dos equipamentos de proteção individual fornecidos pela empresa." (BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 12 abr. 2022).

[75] CLT, "Art. 157 - Cabe às empresas: [...] II - instruir os empregados, através de ordens de serviço, quanto às precauções a tomar no sentido de evitar acidentes do trabalho ou doenças ocupacionais;" (BRASIL. **Decreto-**

fornecidos pela empresa.[76] Por sua vez, o artigo 235-B, inciso VII[77] e parágrafo único, da CLT, prevê sobre o dever do motorista profissional empregado de realizar exames toxicológicos, sendo que a recusa pode acarretar em infração disciplinar, passível de penalização.

Cumpre observar que a empresa pode aplicar suspensão, advertência, poder de despedir, com ou sem justa causa, mediante reparações econômicas, pois decorrem das exigências do desenvolvimento técnico da organização patronal para que possa cumprir os seus fins. Nesse sentido, Amauri M. Nascimento e Sônia M. Nascimento[78] ressaltam que nem todas as leis do direito do trabalho destinam-se à proteção do trabalhador, direcionando-se para o atendimento das exigências do desenvolvimento técnico da organização patronal para que possa cumprir os seus fins, como por exemplo, a aplicação de poder disciplinar e de direção do empregador, suspensões e advertências aplicáveis ao empregado, ou seja, na verdade, as leis do trabalho objetivam o equilíbrio das relações de trabalho, tanto para as empresas como para os funcionários.

Nota-se que não há uma regra ou ordem cronológica, pelo contrário, as penalidades são aplicadas em decorrência do ato e dano causado pelo empregado. É fato, contudo, que os motivos da justa causa devem corresponder a impossibilidade de continuação da relação laboral, pautando-se pelas provas obtidas pela empresa em cada caso concreto. Assim, os

---

Lei nº 5.452, de 1º de maio de 1943. Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 12 abr. 2022).

76 CLT, "Art. 158 - Cabe aos empregados: [...] Parágrafo único - Constitui ato faltoso do empregado a recusa injustificada: a) à observância das instruções expedidas pelo empregador na forma do item II do artigo anterior; b) ao uso dos equipamentos de proteção individual fornecidos pela empresa." (BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 12 abr. 2022).

77 CLT, "Art. 235-B. São deveres do motorista profissional empregado: [...] VII - submeter-se a exames toxicológicos com janela de detecção mínima de 90 (noventa) dias e a programa de controle de uso de droga e de bebida alcoólica, instituído pelo empregador, com sua ampla ciência, pelo menos uma vez a cada 2 (dois) anos e 6 (seis) meses, podendo ser utilizado para esse fim o exame obrigatório previsto na Lei nº 9.503, de 23 de setembro de 1997 - Código de Trânsito Brasileiro, desde que realizado nos últimos 60 (sessenta) dias.
Parágrafo único. A recusa do empregado em submeter-se ao teste ou ao programa de controle de uso de droga e de bebida alcoólica previstos no inciso VII será considerada infração disciplinar, passível de penalização nos termos da lei." (BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 12 abr. 2022).

78 NASCIMENTO, Amauri Mascaro; NASCIMENTO, Sônia Mascaro; **Curso de Direito do Trabalho.** 29. ed. São Paulo: Saraiva, 2014. *E-book* . p. 358-359.

artigos 493[79] e 494[80], ambos da CLT, lecionam sobre o instituto da falta grave, que é prática de qualquer dos fatos a que se refere o art. 482, sendo que o empregado acusado de falta grave poderá ser suspenso de suas funções, mas a sua despedida só se tornará efetiva após inquérito, no qual se verifique a procedência da acusação.

Vale ressaltar que, além da "punição" da justa causa pelo vazamento de dados cometido pelo funcionário, esse poderá responder por perdas e danos, em especial, indenização por danos materiais e morais. Isso dependerá do quanto determinada conduta do funcionário poderá impactar na imagem da empresa, ou seja, do ato e gravidade do ato praticado que ocasionou a referida punição. Nesse aspecto, é importante destacar a aplicação do dano extrapatrimonial nas relações de trabalho, pois, como o vazamento de dados, como regra geral, dirá respeito aos dados da empresa, é evidente que também dirá respeito às relações de trabalho, nos termos do artigo 223-A, da CLT:

> Art. 223-A. Aplicam-se *à* repara*ção* de danos de natureza extrapatrimonial decorrentes da rela*ção* de trabalho apenas os dispositivos deste Título.[81]

Ademais, muitas vezes, o vazamento de dados, como dito anteriormente, se relacionará com a imagem, a marca, o nome e o segredo empresarial, nos termos do artigo 223-D, da CLT:

> Art. 223-D. A imagem, a marca, o nome, o segredo empresarial e o sigilo da correspondência são bens juridicamente tutelados inerentes à pessoa jurídica.[82]

Portanto, a aplicação de advertências, a instauração de investigações internas, as suspensões e a efetiva justa causa, são meios de punição, ou melhor, são formas de sinalizar ao funcionário sobre determinada atitude que não está em consonância com o contrato de trabalho.

---

79 CLT, "Art. 493 - Constitui falta grave a prática de qualquer dos fatos a que se refere o art. 482, quando por sua repetição ou natureza representem séria violação dos deveres e obrigações do empregado." (BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 12 abr. 2022).

80 CLT, "Art. 494 - O empregado acusado de falta grave poderá ser suspenso de suas funções, mas a sua despedida só se tornará efetiva após o inquérito e que se verifique a procedência da acusação. Parágrafo único - A suspensão, no caso deste artigo, perdurará até a decisão final do processo." (BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 12 abr. 2022).

81 BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 12 abr. 2022.

82 BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 12 abr. 2022.

Merecendo destaque que “A caracterização da justa causa depende de condições que devem estar presentes para a sua admissibilidade, a saber, a atualidade, a gravidade e a causalidade. É vedada a dupla punição”, segundo Amauri M. Nascimento e Sônia M. Nascimento [83] . Ratificando-se que, além dos referidos meios de punição, ainda há a possibilidade de a empresa requerer a reparação pelos danos causados por ato ilícito praticado pelo empregado, na forma de danos morais e materiais.

Diante do cenário ora narrado, veja-se que não há distinção de penalidades que o empregador possa enfrentar, pelo contrário, faz-se necessária a apuração do ato praticado e da conduta do agente para imputação da responsabilidade e consequentemente a punição por justa causa em decorrência ato gravoso irreparável.

Portanto, uma análise pormenorizada da responsabilidade civil dos agentes, os requisitos para enquadramento, bem como, um modelo comparativo para melhor entendimento sobre o modelo aplicado no âmbito da LGPD e consequentemente, na esfera laboral para a punição de agentes que tratam os dados e cometem incidentes de segurança.

[83] NASCIMENTO, Amauri Mascaro; NASCIMENTO, Sônia Mascaro; **Curso de Direito do Trabalho.** 29. ed. São Paulo: Saraiva, 2014. *E-book*. p. 923.

5 APLICAÇÃO DA RESPONSABILIDADE CIVIL: DEFINIÇÃO, ESPÉCIES E REQUISITOS

Conforme já analisado anteriormente, é possível destacar que (i) a LGPD é legislação aplicável em complemento a CLT nas esferas laborais; (ii) o vazamento de dados gera um incidente de segurança que possui penalidades junto a LGPD e reflexos perante a CLT em decorrência da gravidade de ato; (iii) inexiste uma ordem legal para aplicação da justa causa, devendo-se observar a conduta do agente, dano ocorrido e punibilidade pelo ato praticado, o que será analisado por meio da esfera da responsabilidade civil.

Nesse aspecto, abordar-se-á as diferenças entre responsabilidade civil objetiva e subjetiva; da aplicação da responsabilidade civil em outros diplomas legais; da aplicação no Direito de Família; no Direito do Consumidor; no Direito Tributário; no Direito Societário; finalmente, a responsabilidade civil sob a ótica da LGPD e do Direito do Trabalho.

Enaltecendo-se a relevância, considerando-se qual modalidade de responsabilidade civil será aplicada, quando existir, por exemplo, vazamento de dados pelo funcionário? Nota-se que para tal conclusão, faz-se necessária a análise pormenorizada dos institutos legais e consequentemente analisar os reflexos de tais disposições na LGPD.

Veja que em linhas gerais, segundo Cavalieri Filho[84], sintetizando a lição de San Tiago Dantas, o principal objetivo da ordem jurídica é proteger o lícito e reprimir o ilícito, sendo que para atender a esse fim e garantir a convivência social, a própria lei estabelece *deveres jurídicos*, ou seja, ordens ou comandos dirigidos à inteligência e à vontade dos indivíduos. É fato que as pessoas, instituições e detentores do Direito têm o dever de não prejudicar terceiros, sendo que, ocorrendo a violação do Direito de outrem, surge o ato ilícito e, consequentemente, danos passíveis de reparação.

Assim, o dever da responsabilidade civil configura-se como o dever que alguém tem de reparar o prejuízo decorrente da violação de um outro dever jurídico. Nas palavras de Cavalieri Filho, "há um dever jurídico originário, chamado por alguns de primário, cuja violação gera um dever jurídico sucessivo, também chamado de secundário, que é de indenizar o prejuízo".[85] Na mesma linha, Diniz[86] entende que a responsabilidade civil constitui uma relação obrigacional que tem por objeto o dever de indenizar:

---

84 CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 13-14.

85 CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014.

86 DINIZ, Maria Helena *apud* STOCO, Rui. **Tratado de responsabilidade civil**: doutrina e jurisprudência. 7. ed. São Paulo: Revista dos Tribunais, 2007. p. 112.

> A aplicação de medidas que obriguem alguém a reparar o dano moral ou patrimonial causado a terceiros em razão de ato próprio imputado, de pessoa por quem ele responde, ou de fato ou coisa ou animal sob sua guarda (responsabilidade subjetiva), ou, ainda, de simples imposição legal (responsabilidade objetiva).

Em síntese, a responsabilidade civil consiste em imputar a uma determinada pessoa a obrigação de indenizar e/ou compensar os danos causados à vítima, recolocando-a na situação que estaria antes da ocorrência do evento danoso.[87]

A responsabilidade civil pode ser classificada sob dois diferentes aspectos, em contratual ou extracontratual, a depender da origem do dever jurídico violado; e em objetiva ou subjetiva, a depender do elemento subjetivo da culpa na conduta do agente. No que tange à classificação quanto à origem, pondera-se a explicação trazida por Cavalieri Filho[88], que a diferencia pela previsão em lei ou contrato: se preexistente um vínculo obrigacional, por exemplo, em um vínculo empregatício e há um inadimplemento contratual, tem-se a responsabilidade contratual (denominada de ilícito contratual ou relativo); se houve lesão a direito subjetivo, sendo que inexiste relação jurídica entre vítima e ofensor, tem-se a responsabilidade extracontratual (chamada de aquiliano ou absoluto), como por exemplo, em demandas indenizatórias decorrentes de atos praticados por terceiros.

Entretanto, no que se refere ao critério da culpa, o que as diferencia é a presença ou não desse elemento subjetivo, empregado em sentido amplo, abrangendo não apenas a culpa em sentido estrito, mas também o dolo. Na responsabilidade objetiva, baseada na teoria do risco, a reparação do dano deve ocorrer independentemente da conduta culposa do agente, bastando o nexo de causalidade entre a ação e o dano sofrido. Já na subjetiva, a vítima só será indenizada se provar a culpa do agente.[89]

O ordenamento jurídico brasileiro, de acordo com o exposto no art. 186 do Código Civil[90], adotou, como regra, a teoria subjetiva, colocando a culpa como o principal pressuposto da responsabilidade civil.[91] Porém, só ela não é suficiente, o dever de indenizar também requer a presença dos demais pressupostos que serão abordados a seguir.

---

87 CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 26.
88 CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 30.
89 CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 32.
90 CC, "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito." (BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022).
91 CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 30.

5.1 Responsabilidade civil objetiva e subjetiva

Diante da conceituação anteriormente apresentada, é possível concluir que a responsabilidade civil é pautada nos preceitos contratuais ou extracontratuais, bem como, se o ato deve ser respondido em caráter subjetivo ou objetivo, ou seja, se existe ou não a necessidade de comprovação do dano, ilícito e nexo causal. Diante da referida conceituação preliminar, se faz imperiosa a apresentação de diferenciação entre a responsabilidade civil objetiva e a responsabilidade civil subjetiva, pois é determinante para verificar a presença ou não dos elementos dolo e culpa a fim de responsabilizar empregados em eventuais atos de transmissão de dados naturais, sensíveis ou privados em desrespeito a LGPD

Não obstante, isso é fato preponderante na gradação de eventual punibilidade, influenciando na classificação de natureza (leve, média, grave ou gravíssima), quando ocorrer vazamento de dados e qual a penalidade aplicada ao empregado analisando-se o caso concreto.

Assim, são quatro os pressupostos gerais da responsabilidade civil: conduta humana, dolo ou culpa, dano e nexo de causalidade. A conduta humana, segundo Diniz[92], trata-se do "ato humano, comissivo ou omissivo, lícito ou ilícito, voluntário e objetivamente imputável, do próprio agente ou de terceiro, ou o fato de animal ou coisa inanimada, que cause dano a outrem, gerando o dever de satisfazer os direitos do lesado".

A ação é a forma mais comum de exteriorização da conduta, pois, se existe o dever geral de abstenção (não causar prejuízos a outrem), a sua violação se dá através de um fazer. É o ato que não deveria ser efetivado, mas foi. Por sua vez, a omissão também é causadora de danos, adquirindo relevância com a quebra do dever jurídico de agir para impedir o resultado ou pela não prática de um ato que deveria ter sido praticado.[93]

Dessa forma, a conduta humana pode ser lícita ou ilícita e, não obstante existam casos excepcionalíssimos de indenizações por atos lícitos[94], como regra, nos moldes do artigo 927 do

---

92 DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**: Responsabilidade Civil. 26. ed. São Paulo: Saraiva. 2012. v. 7, p. 56.

93 CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 38.

94 "Não há o que se falar em ato lícito se em todos os casos de responsabilidade objetiva – do transportador, do Estado, do fornecedor etc. – há sempre a violação de um dever jurídico preexistente, o que configura o ilícito. Ora será o dever de incolumidade, ora o dever de segurança – mas, como veremos, haverá sempre o descumprimento de uma obrigação originária. Ademais, os casos de indenização por ato lícito são excepcionalíssimos, só tendo lugar nas hipóteses expressamente previstas em lei, como no caso de dano causado em estado de necessidade e outras situações específicas (Código Civil, arts. 188, II, c/c arts. 929 e 930, 1.285, 1.289, 1.293, 1.385, §3º, etc). Nesses e em outros casos não há responsabilidade em sentido técnico, por inexistir violação de dever jurídico, mas mera obrigação legal de indenizar por ato lícito." (CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 21).

Código Civil[95], o fato gerador da responsabilidade civil é o ato ilícito, ou seja, o comportamento humano contrário à ordem jurídica.[96] No entanto, não basta apenas a ilicitude para caracterizar a responsabilidade civil, exige-se, ainda, que a conduta humana seja voluntária e imputável. Aqui, a voluntariedade não se traduz na intenção de causar o dano, mas na consciência objetiva daquilo que está sendo feito. O agente deve agir de acordo com a sua livre capacidade de autodeterminação, sendo consciente sobre seu ato e sobre as consequências dele decorrentes.[97] Além disso, é necessária a imputabilidade, isto é, o agente deve ser mentalmente são (sanidade mental) e desenvolvido (maturidade) para que a responsabilidade possa ser a ele atribuída.[98]

Por ter, o Direito brasileiro, adotado a teoria subjetiva, a obrigação de indenizar não decorre tão somente da prática da conduta, é preciso que ela seja culpável, fazendo da culpa o segundo e principal pressuposto da responsabilidade civil. De acordo com Cavalieri Filho[99], o artigo 186 do Código Civil, ao estabelecer que aquele que age com culpa, violando direitos e causando danos a outrem comete ato ilícito, a emprega em sentido lato, abrangendo também o dolo.[100] Com dolo, o agente age intencionalmente e deseja o resultado ilícito ou assume o risco de produzi-lo. Tanto a conduta quanto o resultado são voluntários, lembrando que, nesse caso, a voluntariedade é empregada como intenção de causar o dano. Já na culpa stricto senso, não existe a intenção de lesar. A conduta é voluntária, mas o resultado não. O agente não deseja o resultado ilícito, mas acaba por atingi-lo por inobservância do dever de cuidado, o qual revela-se pela imprudência, negligência ou imperícia.

Sobre o tema, importante destacar a opinião de Cavalieri Filho[101], pois um ponto em comum no dolo e na culpa reside no fato que ambas as situações há conduta voluntária do agente. Ocorre que no dolo a conduta já nasce ilícita, ou seja, o agente "quer a concretização

---

95 CC, "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo." (BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022).

96 CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 20, 23.

97 GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de Direito Civil:** Responsabilidade Civil. 10. ed. São Paulo: Saraiva. 2012. v. 3, p. 74.

98 CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 40.

99 CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 44-46.

100 CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 44.

101 CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014.

de um resultado antijurídico". Enquanto na culpa a conduta nasce lícita, sendo que o resultado ilícito ocorre por desvio acidental de conduta em razão da falta de cuidado do agente.

Contudo, essa distinção, como previsto pela própria lei[102], não tem relevância para fins de responsabilidade civil, pois essa não será medida em razão do grau da culpa do agente, mas pela extensão do dano causado. Seja dolosa ou culposa, o dano deverá ser ressarcido. Além da voluntariedade, outro elemento base da culpa é a previsibilidade, que é a possibilidade de prever o resultado da ação. Se, através das circunstâncias do momento, o agente tinha condições de prever que o resultado ilícito poderia ocorrer, a culpa estará configurada, assim como o dever de indenizar.[103]

O terceiro pressuposto é o dano, conceituado como a lesão a um bem ou interesse juridicamente tutelado. Como concluído por Cavalieri Filho[104], o dano é o centro da obrigação de indenizar, ou seja, se não houver dano a ser ressarcido, não existe responsabilidade civil, nem indenização. São várias as suas modalidades, dentre as principais, destacam-se o dano material ou patrimonial e o dano moral ou extrapatrimonial, diferenciando-se de acordo com a natureza do direito violado. Será material, quando atingir o patrimônio do ofendido; será moral, quando violar seus direitos da personalidade.

Por último, mas não menos importante, está o nexo de causalidade, que trata da relação causa e efeito entre o dano e a conduta do agente. É o elemento mais complexo de ser identificado, principalmente quando várias circunstâncias concorrem para o evento danoso, tornando mais difícil determinar qual delas é a causa real do resultado.[105] Segundo Pereira e Tepedino, é "aquilo que o ofendido efetivamente perdeu em consequência do fato danoso".[106] Por sua vez, Câmara complementa dizendo que o dano "incluirá, também, tudo aquilo que a vítima despendeu com vistas a evitar a lesão ou o seu agravamento, bem como outras eventuais despesas relacionadas ao dano sofrido".[107]

Em breve síntese, a fim de distinguir os preceitos da responsabilidade civil, vislumbra-se o ato subjetivo, que demandará a comprovação de culpa e o ato subjetivo, que demandará

---

[102] CC, "Art. 944. A indenização mede-se pela extensão do dano." (BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022).

[103] CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 45, 51.

[104] CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 92, 93.

[105] PEREIRA, Caio Mário da Silva *apud* CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014. p. 61.

[106] PEREIRA, Caio Mário da Silva; TEPEDINO, Gustavo. **Responsabilidade civil**. 12. ed. Rio de Janeiro: Forense, 2018.

[107] CÂMARA, Marcelo Oliveira. **Responsabilidade civil**. Rio de Janeiro: SESES, 2018.

somente o ato ilícito do agente que irá gerar o dever legal de indenizar, conforme exposto anteriormente.

Na tentativa de solucionar o problema, existem três teorias a respeito: equivalência dos antecedentes, causalidade adequada e causalidade direta ou imediata. A doutrina se divide ao dizer qual foi a adotada pelo ordenamento jurídico brasileiro. Embora alguns autores, como Cavalieri Filho, sejam favoráveis à causalidade adequada, a maioria, baseando-se, sobretudo, no artigo 403 do Código Civil[108], aponta para a causalidade direta ou imediata, ou, como também é chamada, teoria da interrupção do nexo causal ou da causalidade necessária.[109]

Tais teorias e dispositivos devem ser analisados em caráter comparativo, ou seja, confrontá-los no sentido de confirmar se há aplicabilidade na LGPD e se tais requisitos foram compreendidos no modelo adotado pela lei de proteção de dados.

5.2 Da responsabilidade civil em outros diplomas legais

Brevemente, trazer a aplicação da responsabilidade civil em outros diplomas legais é importante, pois além se verificar como o ordenamento jurídico vem aplicando a responsabilidade civil em outras áreas, a forma pela qual vem se decidindo ao se deparar com condutas ilícitas, pode direcionar o caminho na aplicação da responsabilidade civil no Direito do Trabalho (que se trata de contrato de trabalho), bem como, no âmbito da LGPD.

Especificamente, as referidas disposições se demonstrarão como o modo de aplicação da responsabilidade civil em tais esferas podem ou não ter reflexos no modelo aplicado pela LGPD e consequentemente, quais bases a referida legislação incorporou no sistema vigente para delimitação do modelo de responsabilidade dos agentes envolvido no tratamento de dados.

O comparativo entre os diversos institutos narrados deve ao final, traduzir os preceitos invocados pela LGPD e como a existência de tais requisitos foi incorporado na temática inerente a proteção de dados.

---

[108] CC, “Art. 403. Ainda que a inexecução resulte de dolo do devedor, as perdas e danos só incluem os prejuízos efetivos e os lucros cessantes por efeito dela direto e imediato, sem prejuízo do disposto na lei processual.” (BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022).

[109] CAVEDON, Mauro Venturini. Pressupostos da responsabilidade civil no direito brasileiro. *In:* CONTEÚDO JURÍDICO, [s.l.], 1º dez. 2016. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/47878/pressupostos-da-responsabilidade-civil-no-direito-brasileiro. Acesso em: 30 ago. 2022.

Assim, com relação a responsabilidade de civil no âmbito das relações cíveis, Tartuce[110] sustenta que o descumprimento de legislações ou regras estabelecidas em contrato gera o dever da parte que não obedeceu aos preceitos legais em responder civilmente.

Diante disso, entende-se que a responsabilidade civil se relaciona com os mecanismos jurídicos destinados a proporcionar a reparação de danos causados a terceiros. Na mesma linha, Diniz[111] pondera que

> [...] a responsabilidade civil é a aplicação de medidas que obriguem uma pessoa a reparar dano moral ou patrimonial causado a terceiros, em razão de ato por ela mesma praticado, por pessoa por quem ela responde, por alguma coisa a ela pertencente ou de simples imposição legal.

Assim, conforme o ordenamento jurídico vigente, a responsabilidade civil está prevista nos artigos 186 e 927 do Código Civil[112].

Para a caracterização da responsabilidade subjetiva, se faz necessária a comprovação da culpa por parte do causador do dano, enquanto, na objetiva, o dano deverá ser reparado independente de culpa, tão somente pelo risco da atividade, nos termos do regramento civilista aplicável, servindo de base, por consequência, para os demais institutos legais.

Veja-se que o regramento geral é aplicável à LGPD, contudo, ante a teoria da responsabilidade objetiva, o agente é responsabilizado em caráter imediato pelos danos causados, exigindo, na esfera civil, uma análise subjetiva dos requisitos para responsabilização.

5.2.1 Aplicação da responsabilidade civil no Direito de Família

Se faz relevante apresentar a aplicação da responsabilidade civil no Direito de Família, pois além de deter elevada relação com o Direito de Trabalho, no sentido de que as relações familiares se refletem na sociedade, consequentemente, no universo do trabalho, se trata de um ramo que aborda as relações privadas, sendo um importante comparativo e enriquecedor para a temática apresentada e que ao final trará uma possibilidade de conclusão no que concerne a aplicabilidade do modelo de responsabilidade, se objetiva ou subjetiva e se há reflexos no que concerne ao modelo praticado pela LGPD.

---

110 TARTUCE, Flávio. **Direito Civil:** Direito das obrigações e responsabilidade civil. 8. ed. São Paulo: Método, 2013. v. 2, p. 293-294.

111 DINIZ, Maria Helena. **Curso de Direito Civil brasileiro**: Responsabilidade civil. 22. ed. São Paulo: Saraiva, 2007. v. 7, p.35.

112 BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022.

A responsabilidade civil no Direito de Família é um tema que corriqueiramente inspira debates doutrinários e jurisprudenciais, principalmente após a promulgação da Constituição Federal de 1988, momento em que houve a constitucionalização do Direito Civil e, por consequência, das relações privadas.[113]

Por ser o Direito de Família um dos ramos do Direito Civil, também sofreu notória influência da nova ordem constitucional, pois, ao lidar com as mais íntimas relações humanas, deve zelar pela dignidade e determinar que nas relações familiares exista respeito mútuo e ética na convivência.[114] Entretanto, nem sempre é possível garanti-los. São várias as situações em que esses deveres não são respeitados, dando margem à responsabilização civil, que, desde a Constituição Federal, deixou de ser vista apenas como mecanismo de proteção patrimonial.

Hoje, considerando que o objetivo do ordenamento jurídico brasileiro é a proteção da dignidade da pessoa humana, a responsabilidade civil alcançou novo patamar, tutelando não apenas o patrimônio, mas também, e cada vez mais, a personalidade, dignidade e autonomia da vontade dos seres humanos, em especial daqueles considerados mais vulneráveis e merecedores de maior atenção da tutela jurídica, como as crianças e os adolescentes. Nesse contexto, o dano moral foi alçado ao nível de direito fundamental, estando previsto no artigo 5º, incisos V e X, da Constituição Federal, sendo perfeitamente aplicável aos núcleos familiares, que envolvem laços afetivos e outros aspectos pessoais e sentimentais entre seus membros, onde a quebra de qualquer dever pode implicar em violação à dignidade.

Por exemplo, no Recurso Especial 757411/MG, o Ministro Relator Fernando Gonçalves, em seu voto, expôs que tanto o Código Civil, quanto o Estatuto da Criança e do Adolescente já se encarregavam da função punitiva ao preverem a perda do poder familiar no abandono afetivo dos filhos pelos pais, não havendo que se falar em reparação civil de danos.[115] Veja-se que é perfeitamente possível a caracterização da responsabilidade civil no Direito de Família. O Superior Tribunal de Justiça (STJ) e os Tribunais de Justiça locais, em seus julgados, já reconheceram o cabimento[116], concluindo que a obrigação de indenizar, por ser uma cláusula

---

113 WITZEL, Ana Claudia Paes. Aspectos gerais da responsabilidade civil no direito de família. **Âmbito Jurídico**, Rio Grande, v. 16, n. 110, 2013. Disponível em: http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12958. Acesso em: 30 ago. 2018.

114 WITZEL, Ana Claudia Paes. Aspectos gerais da responsabilidade civil no direito de família. **Âmbito Jurídico**, Rio Grande, v. 16, n. 110, 2013. Disponível em: http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12958. Acesso em: 30 ago. 2018.

115 DINIZ, Danielle Alheiros. A impossibilidade de responsabilização civil dos pais por abandono afetivo. *In:* JUS.COM, [s.l.], 24 jun. 2009. Disponível em: https://jus.com.br/artigos/12987/a-impossibilidade-de-responsabilizacao-civil-dos-pais-por-abandono-afetivo#. Acesso em: 31 ago. 2018.

116 BITTENCOURT, Vanessa; TORMIN, Camila. Responsabilidade civil no direito de família: aspectos relevantes da responsabilidade civil no direito de família. *In:* JUSBRASIL, [s.l.], 2015. Disponível em:

genérica, pode ser aplicada a qualquer área, desde que presentes os pressupostos gerais, pouco importando a falta de disposição específica na legislação familiar.[117] Ainda, discordando da minoria, entendem que ao se colocar o Direito de Família em um pedestal inalcançável pela responsabilidade civil, os seus membros deixam de receber a proteção necessária à garantia de sua dignidade humana e de uma vida harmônica em sociedade.[118]

Muito embora o Estado tenha o dever constitucional de proteger a entidade familiar, em razão das intensas transformações que ocorreram ao longo das últimas décadas, não vigora mais no ordenamento jurídico a ideia de que a família é centrada em uma estrutura hierarquizada e controlada pelo domínio do chefe da sociedade conjugal. Pelo contrário, em nome do princípio da igualdade, os indivíduos que compõem o núcleo familiar gozam de proteção aos direitos de que são titulares, em especial aos direitos da personalidade. Logo, hoje, não é mais admissível que os responsáveis pelos danos não sofram qualquer sanção.[119]

Além do mais, o princípio da dignidade da pessoa humana é, sem dúvidas, o mais importante da nova ordem jurídica, possuindo um extenso âmbito de aplicação, no qual se inclui o Direito de Família. Assim, quando instalados os conflitos familiares, ainda que a família goze de especial proteção estatal, a própria Constituição Federal, em seu art. 226, § 8º[120], coloca o indivíduo como merecedor de proteção imediata. Vale dizer, num sopesamento de princípios, que prevalecem os interesses da pessoa em detrimento da entidade familiar, o que, novamente, vem justificar a responsabilidade civil no Direito de Família.[121]

Isso posto, ainda que não seja pacífico o entendimento, a aplicabilidade da responsabilidade civil no âmbito familiar vem sendo cada vez aceita, inclusive para incluir os

---

https://vanbittencourt.jusbrasil.com.br/artigos/306634668/responsabilidade-civil-no-direito-de-familia Acesso em: 31 ago. 2018.

117 WITZEL, Ana Claudia Paes. Aspectos gerais da responsabilidade civil no direito de família. **Âmbito Jurídico**, Rio Grande, v. 16, n. 110, 2013. Disponível em: http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12958. Acesso em: 30 ago. 2018.

118 BITTENCOURT, Vanessa; TORMIN, Camila. Responsabilidade civil no direito de família: aspectos relevantes da responsabilidade civil no direito de família. *In:* JUSBRASIL, [s.l.], 2015. Disponível em: https://vanbittencourt.jusbrasil.com.br/artigos/306634668/responsabilidade-civil-no-direito-de-familia Acesso em: 31 ago. 2018.

119 LIRA, Wlademir Paes de. Responsabilidade civil nas relações familiares: O estado da arte no Brasil. **Revista da Faculdade de Direito da ULP,** Porto, v. 6, n. 6, p. 168-209, fev. 2016. p. 200. Disponível em: https://revistas.ulusofona.pt/index.php/rfdulp/article/view/5352. Acesso em: 31 ago. 2018.

120 CF, "Art. 226, [...]. §8º. O Estado assegurará a assistência à família na pessoa de cada um dos que a integram, criando mecanismos para coibir a violência no âmbito de suas relações." (BRASIL. (Constituição [1988]). **Constituição da República Federativa do Brasil**. Brasília, DF: Congresso Nacional, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 abr. 2022).

121 LIRA, Wlademir Paes de. Responsabilidade civil nas relações familiares: O estado da arte no Brasil. **Revista da Faculdade de Direito da ULP,** Porto, v. 6, n. 6, p. 168-209, fev. 2016. p. 201. Disponível em: https://revistas.ulusofona.pt/index.php/rfdulp/article/view/5352. Acesso em: 31 ago. 2018.

pais adotivos que devolvem os filhos adotados à tutela estatal, como será analisado mais adiante.

Em que pese se tratar de um modelo já consolidado, veja-se que a responsabilidade civil no âmbito do Direito Familiar decorre da necessidade de análise de situações e dos danos apresentados, seguindo uma corrente para o ato subjetivo, o que ao final será analisado em conjunto com os demais institutos e se houve eventual influência no aspecto de proteção de dados.

5.2.2 Responsabilidade civil no Direito do Consumidor

A forma como se aplica a responsabilidade civil no Direito do Consumidor, consagra a possibilidade de nortear as tomadas de decisões no Direito do Trabalho, mormente, nas questões envolvendo incidentes de segurança de dados, danos sofridos por consumidores e infrações de empresas em atividades empresariais, especialmente porque, de acordo com a regra legal, a responsabilidade é objetiva, ou seja, independe dolo e culpa do agente.

Far-se-á necessário entender a influência e o modo de aplicação da responsabilidade objetiva das partes envolvidas a fim de confrontar os institutos ora apresentados.

A responsabilidade civil no âmbito das relações consumeristas é pautada pelo aspecto objetivo, ou seja, não há necessidade de comprovação da culpa para que a parte seja indenizada e qualquer exceção deve ser expressamente comprovada para obstar a compensação indenizatória da vítima.

Veja-se, conforme disposição dos artigos 12 [122] e 14 [123] do Código de Defesa do Consumidor (CDC), a responsabilidade civil é objetiva a fim de compelir o fornecedor a reparar os danos causados aos consumidores por eventuais vícios de produtos, informações insuficientes, inadequadas ou em decorrência de falhas na prestação de serviços, independentemente da necessidade de demonstração de culpa.

---

[122] CDC, "Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos." (BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 08 abr. 2022).

[123] CDC, "Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos." (BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 08 abr. 2022).

Dessa forma, a comprovação da responsabilidade do agente gera o dever de indenizar pelo dano causado, seguindo-se, por consequência, a responsabilidade objetiva do fornecedor nas relações de consumo, o que confirmará as hipóteses de responsabilidade sob a LGPD, especialmente por conta da seguridade necessária ao tratamento dos dados de agentes, pessoas naturais em geral, que também é feito sob o âmbito consumerista.

5.2.3 Responsabilidade civil no Direito Tributário

Novamente, é relevante apresentar a aplicação da responsabilidade civil no Direito Tributário, especialmente o histórico decorrente dessa norma legal, uma vez que permite entender como a responsabilidade civil no Direito Tributária é regida e se há fundamentos utilizados pela LGDP para pautar-se na responsabilidade civil no âmbito de proteção dos dados. Em que pese se tratar de institutos diferentes, a análise pormenorizada da legislação tributária pode apresentar requisitos que também podem ser aplicáveis para aperfeiçoamento da LGPD.

Vale inicialmente frisar que os limites para a imputação da responsabilidade tributária são aqueles definidos pelas regras dispostas em lei complementar, a quem compete regular as normas gerais nessa seara do Direito, nos termos da dicção veiculada pelo artigo 146, inciso III, da Constituição Federal.

Em matéria tributária, a responsabilidade é definida pela Lei 5.172/66, a qual instituiu o Código Tributário Nacional e foi recepcionada pelo ordenamento jurídico vigente com discussões sobre interpretação de lei complementar. A legislação ordinária, nesse contexto, apenas tem espaço de aplicação caso sejam atendidos, primeiramente, os requisitos estipulados pelo Código Tributário Nacional.

Conforme disposição do Código Tributário Nacional, nos termos do artigo 121, à pessoa obrigada ao pagamento de tributo dá-se o nome de sujeito passivo da relação obrigacional tributária, podendo ser denominado como contribuinte ou responsável. Esse mesmo dispositivo, em seu parágrafo único e inciso, estabelece que:

> Parágrafo único. O sujeito passivo da obrigação principal diz-se:
> I – contribuinte, quando tenha relação pessoal e direta com a situação que constitua o respectivo fato gerador;
> II – responsável, quando, sem revestir a condição de contribuinte, sua obrigação decorra de disposição expressa de lei.[124]

[124] BRASIL. (Código Tributário Nacional [1966]). **Lei n.º 5.172, de 25 de outubro de 1966**. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e

Conforme se depreende do aludido preceito legal, a obrigação tributária apresenta a necessidade de ocorrência da hipótese de incidência traçada pelo legislador. O contribuinte é a pessoa que pratica, em concreto, o fato gerador da obrigação tributária. O responsável, por seu turno, é a pessoa que não incorreu na hipótese de incidência tributária, porém foi inserida na relação obrigacional por força de lei. O terceiro, a despeito da prática do evento que atrai a incidência tributária, é o responsável que deve realizar o recolhimento do tribute.

O Código Tributário Nacional descreve determinadas situações que ensejam a responsabilidade tributária, outorgando à lei ordinária a competência para descrever outros eventos passíveis de atrair essa responsabilidade, notadamente nas hipóteses: (*i*) de sucessão, quando ocorrer a transferência da obrigação para outro devedor em consequência do desaparecimento do contribuinte, que pode se dar por morte, fusão, incorporação, transformação ou alienação de empresas ou de estabelecimento comercial, industrial ou profissional, arroladas nos artigos 129 a 133; (*ii*) de terceiros, quando a lei responsabiliza um terceiro pelo cumprimento da obrigação, não sendo esta paga pelo contribuinte, veiculadas pelos artigos 134 e 135; e, por fim, (*iii*) de infração à legislação tributária, descrita nos artigos 136 a 138.

No que tange à responsabilidade tributária dos sócios e dirigentes por débitos de pessoa jurídica, o Código Tributário Nacional determina que:

> Art. 135. São pessoalmente responsáveis pelos créditos correspondentes a obrigações tributárias resultantes de atos praticados com excesso de poderes ou infração de lei, contrato social ou estatutos: [...]
> III - os diretores, gerentes ou representantes de pessoas jurídicas de direito privado.[125]

Nesse cenário, Martins[126] explica que a responsabilidade solidária é legítima quando se trata de atos culposos dos contribuintes e dos contribuintes representados, como demonstra o artigo 135, do Código Tributário Nacional, destacando a orientação legislativa em tornar, para esses casos: a) pessoal, b) total, e c) exclusiva a responsabilidade das pessoas físicas, enunciadas

Municípios. Brasília, DF: Presidente da República, 1966. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm. Acesso em: 12 maio 2022.

[125] BRASIL. (Código Tributário Nacional [1966]). **Lei n.º 5.172, de 25 de outubro de 1966**. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Brasília, DF: Presidente da República, 1966. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm. Acesso em: 12 maio 2022.

[126] MARTINS, Ives Gandra da Silva. **Comentários ao Código Tributário Nacional**. São Paulo: Saraiva, 1998. p. 262-263.

no referido artigo, sempre que o dolo, a fraude e a má-fé forem os agentes deflagradores das obrigações tributárias.

Veja-se que a responsabilidade é atribuída, conforme ressaltado, pela prática de conduta dolosa adotada pelo administrador em detrimento da própria sociedade. Esse é o motivo especial escolhido pela legislação como forma de imputar a responsabilidade aos gestores da sociedade, o que também tem reflexos na forma de apuração da responsabilidade civil no âmbito da LGPD e CLT. Assim, consoante se demonstrou, a responsabilidade, nos casos do art. 135, III, do CTN, é de natureza dolosa, ou seja, demanda a explicitação da conduta adotada pelo gestor da sociedade em detrimento da lei, do contrato ou estatuto social, inclusive e não somente, quando da ocorrência de incidentes de segurança em vazamento de dados, aplicado por analogia ao referido entendimento.

5.2.4 Responsabilidade civil no Direito Societário

No campo corporativo, por detrás da empresa sempre haverá um quadro societário, representado pelos sócios, acionistas, funcionários, diretores que serão responsabilizados em caso de transmissão irregulares de dados em decorrência de incidentes de segurança ocorridos em decorrência do risco da atividade. Somando-se ao referido fato, essa responsabilidade também será direcionada ao agente que estava tratando os dados e por isso, faz-se necessária avaliar o modelo da responsabilidade civil praticada para confrontação com a LGPD.

Conforme exposto anteriormente, a responsabilidade é o dever jurídico de responder por atos ou omissões que impliquem danos a terceiros ou violações de normas jurídicas. O sistema de responsabilidade adotado pelo ordenamento jurídico brasileiro é dualista, coexistindo o subjetivo, baseado na culpa, e o objetivo, fundamentado no risco.

No caso das empresas, a responsabilização por danos causados a terceiro será sempre direcionada à entidade, sendo que os seus administradores e dirigentes somente serão pessoalmente responsabilizados quando praticarem atos ilícitos ou em casos específicos. Vale dizer, a responsabilização apenas da entidade é a regra e a responsabilidade pessoal dos dirigentes é a exceção.

De acordo com a Teoria Dualista aplicada pelo ordenamento jurídico brasileiro, a responsabilidade civil no âmbito das associações é subjetiva, ou seja, requer-se a existência (e comprovação) de ato ilícito causador de dano ao terceiro, praticado por ação ou omissão da associação, baseado em sua negligência ou imprudência, tal como é disciplinado pelo artigo

186 do Código Civil. Sobre o tema, importante trazer o posicionamento de Nery Junior[127], que afirma que aquele que sofreu dano o coloca na posição de recuperar a satisfação de seu direito, em detrimento do sofrimento de ato ilícito, sendo que o devedor responde com o seu patrimônio em decorrência da irregularidade praticada, nos limites da lei.

A conduta adotada nesse tipo de responsabilização poderá ser adjetivada como culposa ou dolosa. O ato ilícito culposo se dá em decorrência de imprudência, negligência ou imperícia do agente causador do dano, em analogia ao que é aplicado às sociedades limitadas, fundamentado no artigo 1.016 do Código Civil, segundo o qual: "Os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções".[128]

Por sua vez, o dolo trata-se da violação deliberada de direito, seja por ação ou omissão. Por exemplo, a hipótese de um dirigente da associação que, conscientemente, abusa de seu poder para locupletar-se às custas da entidade e dos interesses que deveria representar/defender. Nesse caso, é fato que a ilicitude por ele perpetrada tanto pode, como deve, ser alvo de ação de indenização e outras visando à sua punição, haja vista que o ordenamento jurídico brasileiro não admite o enriquecimento sem causa.

Portanto, caso a conduta do sócio ou do próprio dirigente resultar, por dolo, em dano a terceiro, a responsabilidade será direta de quem o causou, não cabendo à entidade a qual representa arcar com os prejuízos, principalmente se a conduta estiver estabelecida pelo Estatuto Social da associação, aplicando-se, assim, a chamada Teoria *ultra vires societatis*, prevista e admitida no Direito brasileiro.

Conforme determina o artigo 1.015 do Código Civil, também analogicamente aplicado às empresas, a referida Teoria visa proteger a pessoa jurídica, estabelecendo que se o administrador, ao praticar atos de gestão, violar o objeto social delimitado no ato constitutivo da entidade, este ato não poderá ser a ela imputado, mas sim ao verdadeiro causador do dano. Nessa hipótese, a entidade responderia somente se viesse a se beneficiar da prática ilícita:

> Artigo 1.015. No silêncio do contrato, os administradores podem praticar todos os atos pertinentes à gestão da sociedade; não constituindo objeto social, a oneração ou a venda de bens imóveis depende do que a maioria dos sócios decidir.
> Parágrafo único. O excesso por parte dos administradores somente pode ser oposto a terceiros se ocorrer pelo menos uma das seguintes hipóteses:

---

[127] NERY JUNIOR, Nelson. **Código Civil Comentado**. 14. ed. São Paulo: Revista dos Tribunais, 2022. p. 361.

[128] BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022.

> I - se a limitação de poderes estiver inscrita ou averbada no registro próprio da sociedade;
> II - provando-se que era conhecida do terceiro;
> III - tratando-se de operação evidentemente estranha aos negócios da sociedade.[129]

Assim, a inobservância dos elementos extrínsecos e intrínsecos do Estatuto/Contrato Social, o ato abusivo discutido deve ser declarado nulo, respondendo o administrador ou o dirigente que ultrapassou às atribuições institucionais, perante o terceiro de boa-fé prejudicado, com seu próprio patrimônio, não se atribuindo qualquer responsabilidade ou ação deste ato à entidade em si considerada, salvo se ela vier a se beneficiar, de alguma forma, com a conduta violadora. Razão pela qual denota-se a responsabilidade objetiva da pessoa jurídica pelos danos causados e subjetivos dos diretores/acionistas, cabendo analisar o benefício econômico objetivo pelo ato praticado pela empresa.

A aplicação da responsabilidade é objetiva e ocorrendo o dano, o empresário será responsabilizado pela reparação, o que tem efetivos reflexos no Direito do Trabalho e consequentemente na LGPD, ante o controle dos dados em caráter empresarial e os danos em caso de transmissão em incidentes de segurança.

5.3 Responsabilidade civil sob a ótica da LGPD e do Direito do Trabalho

Os comparativos nos demais institutos anteriormente apresentados sustentam que a responsabilidade civil dos agentes é valorada de acordo com o modelo da legislação adotada, o que em determinados casos possui impacto no modelo utilizado pela LGPD e consequentemente no Direito do Trabalho.

Segundo Pinheiro e Bomfim[130], sobre a aplicação da responsabilidade civil no Direito e Processo do Trabalho, a tendência doutrinária consiste na aplicação da responsabilidade subjetiva, com culpa presumida, afastando-se, consequentemente, a responsabilidade objetiva do empregador, aplicando-se o artigo 42 e o artigo 43, incisos II e III, da LGPD (isenção de responsabilidade àquele que não violou a lei), sendo que a exceção se faz à relações de consumo (artigo 45, LGPD).

---

[129] BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022.

[130] PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. *In:* MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2021. p. 71-72.

Nesse ínterim, segundo os autores, explica-se a aplicação de lei posterior (LGPD) em detrimento de lei anterior (Código Civil):

> A tese tem amparo, também, no fato de a reparação de dano decorrente de responsabilidade objetiva estar regulada genericamente no Código Civil, lei de mesma hierarquia que a LGPD. Logo, a lei posterior pode revogar a anterior de mesma hierarquia, ou a especial revogar a geral, como é o caso.[131]

Resumidamente, a responsabilidade civil se relaciona com os mecanismos jurídicos destinados a proporcionar a reparação de danos causados a terceiros. Pois, como bem observa Venosa[132], "Em princípio, toda atividade que acarreta prejuízo gera responsabilidade ou dever de indenizar [...]. O termo responsabilidade é utilizado em qualquer situação na qual alguma pessoa, natural ou jurídica, deva arcar com as consequências de um ato, fato ou negócio danoso".

Na seara trabalhista são seguidas as mesmas regras, ou seja, a Responsabilidade Civil do empregador, seja esta pessoa física ou jurídica, está inserida no conceito principal, previsto no artigo 186 do Código Civil.

Adentrando, de forma específica, na área trabalhista, a responsabilidade civil poderá surgir em decorrência de assédio moral, humilhações, cobranças e pressão excessiva, bem como de qualquer tipo de preconceito (cor, idade, gênero, religião), ou em decorrência de acidentes de trabalho, além de doenças relacionadas à atividade laboral. Observa-se que ela poderá ser objetiva ou subjetiva, assim como nos demais regramentos. Na forma objetiva, a indenização independe de intenção ou cautela do empregador. Já na responsabilidade civil subjetiva, a vítima precisa comprovar a culpa do agente para que haja indenização.

Considerando que mesmo antes do Código Civil a jurisprudência já vinha alargando o conceito de culpa, e que a LGPD não trouxe a culpa como elemento para se configurar a responsabilidade, é possível aplicar a responsabilidade subjetiva? Ou a responsabilidade objetiva?

Substancialmente, se destacam os artigos 42 a 45 da Lei Geral de Proteção de Dados, que abordam sobre a atribuição de responsabilidade do controlador e do operador, em razão do exercício de atividade de tratamento de dados pessoas, quando causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, sendo obrigada a reparação:

---

131 PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. *In:* MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2021. p. 72

132 VENOSA, Silvio de Salvo. **Direito Civil:** Responsabilidade civil. 14. ed. São Paulo: Atlas, 2014. v. 4, p. 1.

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei (...).
> [133]

Destaca-as que o parágrafo 1º, inciso I, do artigo 42, prevê a responsabilidade solidária do operador. O mesmo vale para o controlador (parágrafo 1º, inciso II, do artigo 42).

Por sua vez, o juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa (parágrafo 2º, do artigo 42), o que demandará uma análise específica do caso concreto.

Veja-se que, no aspecto da LGPD, a tendente vertente difere da responsabilidade civil trabalhista em decorrência do modelo de assunção dos riscos. Essa corrente inerente à legislação dos dados segue preceitos consumeristas pela teoria do risco da atividade, ou seja, as empresas que prestam os serviços são responsabilizadas em caráter objetivo pelos danos causados. Diante disso, ocorrendo o ato ilícito e configurado o nexo causal, por isso, os agentes de tratamento respondem objetivamente pelo dano causado, admitindo-se excludentes do ato ilícito para obstar eventual reparação.

Aliás, tal previsão segue o quanto previsto no CDC, na medida em que, inexiste necessidade de comprovação de culpa ou dolo, basta a existência de ato praticado em desfavor do consumidor que a empresa será responsabilizada pelo ato praticado.

Em paralelo, os demais modelos apresentados, tem como base a aplicação da responsabilidade sob o aspecto subjetivo, ou seja, demandam a necessidade de comprovação efetiva da conduta do agente, dano causado e nexo causal do que fora praticado para que sejam responsabilizados pelos atos ocorridos. É importante trazer à baila que, apesar de distintos, foram também incrementados pela LGPD na medida em que tal legislação também tem aplicabilidade nas demais esferas legais, por isso, relevantes à discussão em caráter

---

[133] BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

comparativo aos institutos apresentados.

Assim como no GDPR, artigos 24 [134], 25 [135] e 26 [136], que dispõe sobre a responsabilidade do controlador dos dados, mediante utilização de mecanismos necessários a correta certificação do que está sendo manuseado de forma transparente e com os devidos cuidados para evitar a transmissão indevida dos dados, a lei brasileira prevê o caráter solidário da responsabilização do controlador e do operador[137]. Lembrando que o controlador é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (LGPD, art. 5º VI) e o operador é a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (LGPD, art. 5º, VII). Ambos são classificados como agentes de tratamento, conforme dispõe o artigo 5º, inciso IX, da LGPD.[138]

Nota-se que os dispositivos da GDPR são utilizados justamente para que sejam analisados os dados tratados pelos agentes, a responsabilidade do agente/controlador, bem como, a educação interposta nos locais onde os dados são tratados para evitar danos a terceiros, criando-se normas de segurança internas de interesse da coletividade onde a norma deve ser aplicada, como por exemplo, empresas de arquivamento de documentos físicos).

Vale destacar que nos termos do artigo 43 da LGPD, quando há apresentação de provas suficientes que isentem de responsabilidade os agentes do tratamento de dados (controlador e/ou operador), a mesma isenção de responsabilidade lhe deverá ser garantida. Por sua vez, o artigo 44 da LGPD traz as condições de demonstração da ilicitude do tratamento de dados pessoais, da mesma forma que o artigo 6º[139] do GDPR, que pontua condições de licitude do tratamento de dados pessoais, quais sejam, (i) consentimento do titular dos dados para finalidades específicas; (ii) tratamento dos dados à pedido do titular dos dados; (iii) tratamento necessário para o cumprimento de uma determinação legal ou regramento específico; (iv) tratamento para proteção dos interesses vitais do agente titular dos dados; (v) tratamento para

---

134 GDPR, "Art. 24 – (EUROPEAN UNION. **General Data Protection Regulation (GDPR)**. May 25, 2018. Disponível em: https://gdpr-info.eu/art-12-gdpr/. Acesso em: 12 abr. 2022).

135 GDPR, "Art. 25 GDPR – (EUROPEAN UNION. **General Data Protection Regulation (GDPR)**. May 25, 2018. Disponível em: https://gdpr-info.eu/art-12-gdpr/. Acesso em: 12 abr. 2022).

136 GDPR, "Art. 26 GDPR –." (EUROPEAN UNION. **General Data Protection Regulation (GDPR)**. May 25, 2018. Disponível em: https://gdpr-info.eu/art-12-gdpr/. Acesso em: 12 abr. 2022).

137 PINHEIRO, Patricia Peck. **Proteção de dados pessoais comentários à Lei n. 13.709/2018 (LGPD)**. 3. ed. São Paulo: Saraiva Jur, 2021. p. 146-147.

138 BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

139 GDPR, "Art. 6º
(EUROPEAN UNION. **General Data Protection Regulation (GDPR)**. May 25, 2018. Disponível em: https://gdpr-info.eu/art-12-gdpr/. Acesso em: 12 abr. 2022)

desempenho de atividade pública ou por ato de autoridade investida em ato necessário a utilização dos dados; (vi) tratamento for necessário para efeitos dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por um terceiro.

Já o artigo 45 da LGPD apresenta situações quanto ao tipo de violações de direitos do titular, aplicando-se as penalidades previstas no Código de Defesa do Consumidor e/ou pela regra geral do Código Civil Brasileiro, consoante os artigos 186[140], 187[141] e 927[142]. Analisando-se as normas aqui citadas, questiona-se se, diante das situações, aplicar-se-á a responsabilidade objetiva ou a responsabilidade subjetiva?

Segundo Patrícia Peck Pinheiro[143],

> [...] o desenvolvimento do modelo de negócios da economia digital, que passou a ter maior dependência de fluxos internacionais de bases de dados, em especial os relacionados às pessoas, viabilizados pelos avanços da globalização e os avanços tecnológicos, é ponto que toca diretamente essas novas relações, em especial as laborais.

Nos julgados que serão posteriormente apresentados sobre a aplicabilidade da LGPD nas relações empregatícias, restará demonstrado que a responsabilidade aplicada foi a objetiva. Isso porque, certamente, o elemento "culpa" não foi crucial para caracterizar o ilícito.

Além disso, conforme acima suscitado, na responsabilidade objetiva (essa é a regra nas relações de consumo, por exemplo) basta a prova do dano e do nexo causal, ou seja, haverá a obrigação de reparar o dano independentemente da avaliação de culpa quando sua atividade implicar, por sua natureza, risco para os direitos de outrem.

---

[140] CC, "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito." (BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022).

[141] CC, "Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes." (BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022).

[142] CC, "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem." (BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022).

[143] PINHEIRO, Patrícia Peck *apud* CASTRO, Dayane Marciano de Oliveira; MANCUSO, Gisele. Responsabilidade da Empresa frente à proteção dos dados do trabalhador no contexto da Lei Geral de Proteção de Dados no Brasil – LGPD *In:* PERREGIL, Fernanda; CALCINI, Ricardo (org.). **LGPD e *Compliance* trabalhista**: os desafios atuais no Direito do Trabalho empresarial. Leme, SP: Mizuno, 2021. p. 52.

Dessa forma, na Justiça do Trabalho faz-se elementar (i) prever, (ii) diagnosticar, (iii) apontar, (iv) evitar, (v) educar e (vi) promover uma cultura sólida de transparência, a fim de que todas as pessoas possam participar efetivamente do processo de enraizamento da proteção de dados. Vale destacar que a LGPD se preocupa não apenas com a aplicação da responsabilidade por eventuais danos quanto ao descumprimento da norma de proteção de dados, mas também quanto ao papel social que a empresa desempenha.

Nesse sentido, Castro e Mancuso[144] sustentam que um mero contrato ou termo de consentimento assinados pelas partes envolvidas, seja empregados, empregadores, titulares ou responsáveis pelo tratamento dos dados não exime a responsabilidade da empresa em caso de um incidente de segurança.

Pelo contrário, faz-se necessário adequar-se as regras previstas pela LGPD, no sentido de criar um manual de conduta, boas práticas, governança, forma de tratamento dos dados, o que é ou não dado natural ou sensível e consequentemente, atitudes e processos que devem ser realizados em casos de incidentes de segurança, além de eliminação incorreta dos dados e os devidos impactos legais de tal infração, seja por responsabilidade do agente que trata os dados e também da empresa no que concerne aos impactos decorrentes do referido ato.

O fato é que, adequar-se a LGPD, de acordo com os autores, não é meramente a elaboração de documentos e contratos. É necessário, uma mudança de rotina e procedimentos para que seja alterado por completo a forma de guarda, utilização, disposição, eliminação e obstar, por tais disposições, danos à terceiros e até mesmo a atividade empresarial prestada.

Ato contínuo, para melhor entendimento e compreensão acerca da responsabilidade a ser aplicada ao caso concreto, verifica-se que a LGPD não trouxe o elemento culpa, sendo possível a aplicação da responsabilidade objetiva. Nesse sentido, Santos, Silva e Padrão[145] comentam sobre a existência de duas correntes principais sobre o assunto, quais sejam, da responsabilidade civil objetiva, ou seja, que não demandaria qualquer comprovação de dano pelo titular dos dados, bastando-se a ocorrência de dano por ato ocorrido.

Em paralelo, há ainda uma corrente que entende que a responsabilidade demandaria a necessidade de demonstração da culpa para que seja caracterizada o dever de indenizar. Ou

---

144 PERREGIL, Fernanda; CALCINI, Ricardo (org.). **LGPD e *Compliance* trabalhista**: Os desafios atuais no Direito do Trabalho Empresarial. Leme, SP: Mizuno, 2021. p. 55.

145 SANTOS, Camila Ferrão dos; SILVA, Jeniffer Gomes da; PADRÃO, Vinicius. Responsabilidade civil pelo tratamento de dados pessoais na Lei Geral de Proteção de Dados. **Revista Eletrônica da PGE RJ,** Rio de Janeiro, v. 4, n. 3, p. 1-31, set./dez. 2021. p. 11. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/256. Acesso em: 11 fev. 2022.

seja, mesmo com o vazamento de dados, seria necessário comprovar o nexo causal do ato e a culpa do agente para que pudesse ser considerado o dano ao titular dos danos.

Vale ressaltar que os mesmos autores ainda sustentam a existência de outras duas correntes que poderiam ser aplicadas no que concerne à responsabilidade civil das partes em caso de incidentes de segurança, quais sejam, (i) responsabilidade civil proativa, que se baseia na existência da legislação para evitar danos à terceiros, afastando a incidência da responsabilidade civil objetiva ou subjetiva e; (ii) culpa presumida, ou seja, os agentes só não serão responsabilizados se apresentarem excludentes de ilicitude, nos termos do artigo 43 da LGPD.

Portanto, vislumbra-se que a existência de 04 (quatro) institutos com a corrente majoritária para os institutos da responsabilidade civil subjetiva e objetiva. Contudo, conforme será abordado a seguir, na esfera laboral, os casos de responsabilidade civil dos agentes de tratamento de dados adotada pela LGPD, interpretados em conjunto com o artigo 482 da CLT, para melhor aplicação, ou não, de eventual justa causa.

Parece que a solução para que as empresas consigam evitar danos referentes à segurança de dados na esfera do Direito do Trabalho é instituir uma cultura preventiva, pautada, entre outras, nas seguintes medidas: (*i*) a promoção de treinamento com todos os colaboradores; (*ii*) a realização de avaliações e melhorias; (*iii*) a valorização da segurança em Recursos Humanos; (*iv*) a adoção de medidas equilibradas no momento de contratação, começando no processo seletivo, passando-se à execução do contrato de trabalho propriamente dito (ter muita clareza nas cláusulas contratuais, elaborar termo de consentimento etc.); (*v*) a criação de um canal de denúncia ou comunicação interna; (*vi*) verificar o prazo de guarda de documentos trabalhistas, enfim, essas são algumas medidas.[146] Em outras palavras, as medidas apresentadas demonstram perfeitamente que a LGPD foi criada com enfoque de evitar danos. Trata-se de uma sistemática promovida para incentivar o diálogo constante.

Atribuir responsabilidade civil objetiva ou responsabilidade subjetiva, certamente, vai depender da prova robusta produzida em um processo administrativo, judicial ou, até mesmo, extrajudicial, a fim de tentar mensurar o impacto que determinado desvirtuamento causou ou poderia causar, verificando se tal conduta alcançou, ou se poderia alcançar, terceiros.

Em caso divulgado no âmbito do TRT-2, o qual será abordado posteriormente, sobre a aplicação da justa causa por desrespeito à LGPD, a decisão é muito enfática ao verificar o potencial risco que a conduta de compartilhar uma planilha consigo mesmo poderia causar,

---

[146] CARLOTTO, Selma; GUERRA, Elaine. **Manual prático de adequação à LGPD com enfoque nas relações de trabalho**. São Paulo: LTr, 2021. p. 99-123.

considerando os dados naturais transmitidos e o possível risco de vazamento, ainda que sem intenção. No caso, a conduta foi qualificada como mau procedimento e, em decorrência da infração, nos termos do artigo 482 da CLT, configura-se a responsabilidade objetiva e passível de justa causa.

Ou seja, engloba-se a questão da responsabilidade objetiva, diferentemente do que rege a responsabilidade civil laboral, ante a necessidade de comprovação de culpa do agente, mesmo com o risco da atividade tomado pelo empregador.

Assim, tendente vertente no aspecto da LGPD difere da responsabilidade civil trabalhista em decorrência do modelo de assunção dos riscos. A corrente inerente à legislação de proteção dos dados segue preceitos consumeristas pela teoria do risco da atividade, ou seja, as empresas que prestam os serviços são responsabilizadas em caráter objetivo pelos danos causados, por isso, os agentes de tratamento, ocorrendo o ato ilícito e nexo causal, respondem objetivamente pelo dano causado, admitindo-se excludentes do ato ilícito para obstar eventual reparação.

Diante do referido cenário, é possível delimitar que, com exceção do Código de Defesa do Consumidor que prevê a responsabilidade objetiva pelo ato praticados, os demais diplomas adotam a responsabilidade em caráter subjetivo, ou seja, cabendo a comprovação do dano, culpa, dolo e nexo causal para que o ato ilícito seja devidamente compensado.

Aliás, os preceitos consumeristas são, em que pese discutíveis, aplicáveis à LGPD, uma vez que as empresas/agentes que tratam os dados são responsáveis por incidentes de segurança, o que demanda, por consequência, responsabilidade objetiva pelos danos causados.

Assim, vislumbrando-se a responsabilidade objetiva dos agentes no tratamento de dados e também do empresário responsável pelo recebimento dos dados, é possível entender que além de aplicável à esfera laboral, a LGPD tem o condão de subsidiar um eventual ato de rescisão contratual por infração expressa a legislação de dados, seja por desrespeito à legislação ou eventualmente a um incidente de segurança que originou um vazamento indevido de dados.

Desta forma, necessário avaliar individualmente, apesar de sem grandes precedentes, a aplicação da LGPD na prática em face de relações laborais, bem como, incidentes de vazamento de dados para melhor confirmação dos preceitos, princípios e fatores determinantes para consolidação de decisões.

6 DOS CASOS CONCRETOS SOBRE A INTERSECÇÃO DA LGPD E DIREITO DO TRABALHO

Embora a temática inerente a proteção de dados no Brasil esteja ativa desde 2020, já há alguns poucos julgados que tratam sobre o vazamento de dados no contexto do Direito do Trabalho e consequentemente, validando-se o desligamento por justa causa de empregados em vazamento de dados em qualquer hipótese, em decorrência do potencial dano que pode acarretar a empresa e consequentemente ao titular dos dados.

Veja-se que já foi discorrido na presente dissertação sobre o aspecto histórico da LGPD, os impactos sobre a esfera laboral, a aplicabilidade nas demandas entre empregados e empregadores, a responsabilidade civil sob a ótica da LGPD em confrontação com os demais institutos jurídicos paradigmas, contudo, não restou convalidada a aplicação da legislação aos casos concretos para efetivo cumprimento da LGPD na realidade laboral.

Mesmo que não haja um entendimento pacífico, é importante apresentar tais julgados a fim de que seja suscitado qual a base legal utilizada pelo Tribunal julgador, bem como, os argumentos, preceitos e princípios discorridos a fim de formular uma melhor decisão ao caso concreto em discussão, especialmente, o modelo de responsabilidade fixado, as penalidades impostas e se efetivamente é convalidada a falta grave para ocorrência do desligamento por justo motivo.

Somando-se ao referido fato, far-se-á uma análise de decisões estrangeiras julgadas pela autoridade nacional local em incidentes de vazamento de dados, que demonstrará a seriedade da legislação internacional e consequentemente as penalidades impostas que serão também utilizadas no Brasil em caso de descumprimento da legislação, caso as empresas não se adequem ao modelo atualmente vigente.

6.1 Dos julgados no Brasil

Ao longo do presente estudo, fez-se primordial pesquisar inúmeras decisões relacionadas à LGPD. No entanto, quanto à temática especificamente, ou seja, a aplicação da justa causa com embasamento no vazamento de dados, localizou-se apenas duas decisões que merecem destaque.

No julgado ora destacado, o Tribunal Regional do Trabalho da Segunda Região (TRT-2) não considerou relevante a finalidade do compartilhamento de uma planilha contendo dados sensíveis de clientes, os quais não poderiam ser transmitidos ou compartilhados. Ocorre que

funcionário compartilhou a referida planilha apenas com ele mesmo, sem a divulgação de dados a terceiros, ou seja, não se configurou a publicidade e a disseminação da informação a outras pessoas.

Nesse sentido, o TRT 2 entendeu que o vazamento de dados por si só já configura ato gravíssimo, até mesmo porque, no presente caso, tratava-se de vazamento de uma planilha com mais de oito mil linhas de dados de cartões do cliente MRV, podendo-se acarretar um potencial dano a empresa empregadora[147].

Veja-se que o referido desligamento ocorreu porque na planilha manuseada e transmitida para o e-mail pessoal havia dados de terceiros, com nome, RG, CPF e outros. Dados que, caso fossem compartilhados, poderiam ocasionar problemas para a empresa e para os responsáveis pelos dados vazados. Nota-se que a atitude do empregador foi imediata, no sentido de prontamente rescindir o contrato por justo motivo, em decorrência do incidente de segurança verificado e os impactos que poderia causar, tanto à empresa como ao cliente. Em verdade, confirmou-se que os dados naturais sensíveis devem ser preservados sob qualquer aspecto, inclusive para transmissão a *e-mail* particular de empregado. Ainda, a objetividade da LGPD caracteriza necessidade de ato imediato e a justa causa aplicável preveniu danos maiores aos terceiros e a empregadora, cumprindo-se o requisito do artigo 482 da CLT.

No exemplo apresentado, em sede de Acórdão prolatado pelo TRT-2[148], houve o entendimento pela manutenção da justa causa, uma vez que o ex-funcionário compartilhou consigo mesmo uma "planilha com mais de 08 (oito) mil linhas de dados de cartões do cliente MRV, infringindo assim o Código de Ética, caracterizando ação dolosa praticada pelo colaborador". Somando-se a isso, o fato de que a planilha continha dados sensíveis e que existia a confidencialidade entre as partes, resta cabida a necessidade de aplicação da LGPD.

Apesar de o compartilhamento ter se dado consigo mesmo (e este é um grande ponto da questão) e não ter ocorrido vazamento de dados a terceiros, o ato *per si* é extremamente grave. Uma vez que a transmissão de dados naturais, em caso de desvio da finalidade ou remessa a terceiro, ainda que sem intenção, configura motivo suficiente para causar danos aos clientes e aos responsáveis pelos dados pessoais, o TRT2 entendeu que houve dolo no ato de compartilhamento da referida planilha.

---

147 BRASIL. Tribunal Regional do Trabalho (2 Região). Primeira Turma. **Reclamatória Ordinária Trabalhista nº 1000612-09.2020.5.02.0043**. Relator Des. Daniel de Paula Guimarães. São Paulo, 22 de outubro de 2021. Disponível em: https://pje.trt2.jus.br/consultaprocessual/detalhe-processo/1000612-09.2020.5.02.0043/2#0359e14. Acesso em: 12 abr. 2022.

148 Processo n.º 1000612-09.2020.5.02.0043

Nesse sentido, relevante ressaltar que o Código Civil prevê que "São os negócios jurídicos anuláveis por dolo, quando este for a sua causa" (art. 145) e determina que o dolo acidental implica na responsabilidade civil (art. 146).[149] Veja-se que ambos os artigos são de fato aplicáveis ao caso em concreto discutido no âmbito do TRT2, afinal, a planilha compartilhada dizia respeito a negócios mercantis da empresa e o reclamante apresentou conduta de dolo positivo (ou comissivo).[150] Pode-se imaginar eventuais prejuízos, caso a planilha vazasse a terceiros, podendo chegar a valores exorbitantes.

Considerando que o dolo relacionado ao reclamante diz respeito ao **"**dolo bom", relevante trazer a lição de Tartuce[151], que diferencia o "dolo bom" do "dolo mau. Enquanto o dolo bom pode ser entendido como tolerável, há também um sentido de trazer a terceiro vantagens por um ato que não teria conhecimento, como por exemplo, fornecer remédio a pessoa alegando ser um mero líquido, visando trazer benefícios expressos a pessoa que tal ato é direcionado. Em paralelo, o dolo mau consiste em ações praticadas pelo agente no sentido de enganar, prejudicar, causar prejuízo e problemas a terceiro com a intenção expressa do ato que está sendo realizado.

Sendo assim, no caso concreto em análise, a grande preocupação foi a de prevalecer os dez princípios destacados a LGPD: (*i*) finalidade; (*ii*) adequação; (*iii*) necessidade; (*iv*) livre acesso; (*v*) qualidade dos dados; (*vi*) transparência; (*vii*) segurança; (*viii*) prevenção; (*ix*) não discriminação; e (*x*) responsabilização e prestação de contas. Princípios que encontram previsão no artigo 6º, incisos I a II, da referida 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,

---

149 BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022.

150 Segundo Tartuce, o dolo positivo (ou comissivo) é o dolo praticado por ação (conduta positiva). (TARTUCE, Flávio. **Direito Civil:** Direito das obrigações e responsabilidade civil. 8. ed. São Paulo: Método, 2013. v. 2).

151 TARTUCE, Flávio. **Direito Civil:** Direito das obrigações e responsabilidade civil. 8. ed. São Paulo: Método, 2013. v. 2, p. 376.

> proporcionais e não excessivos em relação às finalidades do tratamento de dados [...].[152]

Por outro lado, a Justiça do Trabalho, em recente julgado, entendeu que a utilização do bafômetro viola proteção de dados, conforme notícia veiculada na Folha de São Paulo[153]. Trata-se de caso em que um trabalhador, ao ser submetido pela empresa à realização de teste de bafômetro, teve seu contrato rescindido por justa causa. Ocorre que a 1ª Vara do Trabalho de Dourados (MS), ao entender que "a empresa que submeteu o funcionário ao bafômetro descumpriu a LGPD ao não comunicar de maneira explícita a finalidade e a necessidade de realizar o teste. O tipo de dado coletado, por ser uma informação relacionada à saúde, é considerado sensível" (LGPD, art. 5º, II) c/c o consentimento (LGPD, art. 5º, XII) c/c os princípios da finalidade (LGPD, art. 6º, I) e da necessidade (LGPD, art. 6º, III), restou por reverter a justa causa.

Evidentemente, há um choque de normas, pois a CLT, em seu artigo 482, alínea "f"[154], prevê a rescisão por justa causa ao se configurar embriaguez habitual ou em serviço.

A notícia prossegue trazendo números, em que a LGPD já foi utilizada em mais de 2.200 ações trabalhistas. Além disso, a pesquisa revela que as ações que citam "LGPD", "Lei Geral de Proteção de Dados" ou "13709" como também "danos morais" ou "justa causa" nas petições iniciais, no ano de 2020 foram 130; em 2021 foram 2.048; e no ano de 2022 já são 42.[155]

No outro caso, em trâmite perante a 1ª Vara do Trabalho de Dourados (MS), o Juiz decidiu que a empresa, ao realizar teste de bafômetro, violou a LGPD ao não comunicar ao empregado, de maneira explícita, a finalidade e a necessidade do teste, sendo que o tipo de dado coletado, por ser uma informação relacionada à saúde, é considerado sensível. Diante disso, o juiz considerou que aplicação da justa causa não foi correta.

---

[152] BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

[153] BRIGATTI, Fernanda. Uso do bafômetro viola proteção de dados, decide Justiça do Trabalho. **Folha de São Paulo,** São Paulo, 03 fev. 2022. Disponível em: https://www1.folha.uol.com.br/mercado/2022/02/uso-do-bafometro-viola-protecao-de-dados-decide-justica-do-trabalho.shtml?_mather=b8aa1a7a576cc75b&origin=folha. Acesso em: 04 fev. 2022.

[154] CLT, "*Art. 482 - Constituem justa causa para rescisão do contrato de trabalho pelo empregador:[...] f) embriaguez habitual ou em serviço;"* (BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 12 abr. 2022).

[155] BRIGATTI, Fernanda. Uso do bafômetro viola proteção de dados, decide Justiça do Trabalho. **Folha de São Paulo,** São Paulo, 03 fev. 2022. Disponível em: https://www1.folha.uol.com.br/mercado/2022/02/uso-do-bafometro-viola-protecao-de-dados-decide-justica-do-trabalho.shtml?_mather=b8aa1a7a576cc75b&origin=folha. Acesso em: 04 fev. 2022.

Verifica-se que, de fato, a LGPD não prevê a aplicação da justa causa a funcionários que violam questões relacionadas a dados pessoais e sensíveis. Nos dois exemplos, veja-se que o TRT2 não verificou o histórico do funcionário, tampouco averiguou se a empresa respeita o artigo 50 da LGPD, que traz regras de boas práticas e de governança, recaindo toda responsabilidade sob o ex-funcionário, sendo que o artigo 482 da CLT não prevê nenhuma hipótese de justa causa relacionada ao compartilhamento de dados.

Segundo Correia e Boldrin[156], a LGPD deve ser aplicada às relações de emprego para a proteção dos dados pessoais dos empregados, uma vez que, não há previsão expressa na referida legislação sobre as demandas laborais, razão pela qual, ressalta-se o aspecto generalista da referida legislação, preocupando-se com a proteção geral dos dados dos titulares de dados, inclusive empregados e empregadores.

Nos casos em discussão, o ato foi considerado grave porque envolvia o manuseio de dados pessoais de terceiros (clientes), que, caso fossem publicados, causariam danos a terceiros, residindo fundamento no artigo 482 da CLT, confirmando-se a responsabilidade objetiva do agente responsável pelo tratamento de dados.

Num primeiro momento, é possível verificar que o TRT2 aplicou a LGPD em toda a sua essência, de maneira geral. Destaca-se o próprio acórdão que consagrou sentença de piso, invocando o artigo 5º, inciso I, da Lei 13.709/2018:

> Logo, trata-se de dados pessoais de pessoas naturais e que, de forma alguma, podem ser extraviados para meios que escapam do controle da empresa, sob pena, inclusive, de eventual responsabilização da empresa pelas pessoas físicas e jurídicas afetadas. A extração de dados tem se tornado um grande commodity da economia. Tamanha a sua importância econômica e, também, tamanha a possibilidade danosa da publicação de dados, que foi criada a Lei Geral de Proteção de Dados (Lei nº 13.709) e disciplinada a responsabilidade civil daqueles que controlam ou operam tais dados.[157]

Como visto, o reclamante da referida ação compartilhou (sem qualquer autorização ou premissa da LGPD) uma planilha com diversos dados pessoas e naturais de terceiros, configurando ofensa ao artigo 5º, inciso I, da LGPD, culminando na atribuição de responsabilidade, segundo preconiza o artigo 42 do mesmo diploma legal.

---

156 CORREIA, Henrique; BOLDRIN, Paulo Henrique Martinucci. Lei Geral de Proteção de Dados (LGPD) e o Direito do Trabalho. **Revista Síntese Trabalhista e Previdenciária**, São Paulo, v. 31, n. 377, p. 205-217, nov. 2020.

157 BRASIL. Tribunal Regional do Trabalho (2 Região). Primeira Turma. **Reclamatória Ordinária Trabalhista nº 1000612-09.2020.5.02.0043**. Relator Des. Daniel de Paula Guimarães. São Paulo, 22 de outubro de 2021. Disponível em: https://pje.trt2.jus.br/consultaprocessual/detalhe-processo/1000612-09.2020.5.02.0043/2#0359e14. Acesso em: 12 abr. 2022.

Portanto, no caso em comento, o ponto crucial foi a violação ao artigo 5º, inciso I, da Lei n.º 13.709/2018. Pois, ao se tratar de dados sensíveis, não havia a possibilidade de qualquer tratamento ou transmissão dos mesmos, de modo que a ação praticada pelo empregado ensejou ruptura da confiança, quebra do contrato e, por consequência, a necessidade imediata da justa causa, aplicável em conjunto com os preceitos da LGPD pelo tratamento e vazamento indevido de dados sensíveis. Contudo, isso será avaliado pela extensão do dano ocasionado, justamente a base do preceito da LGPD, uma vez que a abertura de incidente de segurança em decorrência do vazamento de dados é ato que demanda a responsabilização das partes envolvidas.

Por sua vez, no caso do bafômetro, a questão é tipificada no artigo 482, alínea "f", da CLT, sendo a embriaguez um ato gravíssimo. Porém, enquanto não se criar um tipo legal para a aplicação segura nas relações de emprego, a interpretação para cada caso concreto terá inúmeros caminhos.

Não obstante, conforme análise dos tópicos anteriores, é possível orientar-se pela corrente da responsabilidade objetiva dos agentes de tratamento de dados, uma vez que confirmada a prestação dos serviços, as partes têm ciência dos dados, responsabilização e segurança do tratamento, inexistindo, portanto, a necessidade de comprovação da culpa. O certo é que, como a LGPD tem caráter preventivo, tanto a empresa como os funcionários trabalharão em conjunto para não incorrer em erros de compartilhamento, armazenamento e/ou publicação de informações. Pois, além das empresas estarem sujeitas a sanções civis e administrativas, tais situações causam impacto negativo a sua imagem, de nodo que a falta de adequação do ambiente de trabalho ao regramento da LGPD pode implicar em pontos de vulnerabilidade para as empresas.

Justamente nesse aspecto, Cots e Oliveira [158] ponderam sobre as sanções administrativas e pendência de regulamento da autoridade nacional reguladora para serem efetivamente aplicáveis, uma vez que, com tal disposição, haverá segurança jurídica dos agentes, controladores e responsáveis pelos dados no que concerne aos impactos da lei e efetivamente as penalidades que serão impostas em casos de descumprimentos.

Assim, conforme fatores apontados, que a LGPD tem aplicação na seara trabalhista, podendo, inclusive, caracterizar justa causa quando o empregado, ultrapassando os limites do ponderável e do razoável, manuseia dados (especialmente os dados sensíveis) e descumpre os regramentos legais da proteção de dados.

---

[158] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 210.

Cumpre dizer, que os julgados aqui analisados se tratam de decisões iniciais sobre o tema, tendo em vista a recente vigência da Lei. Contudo, conforme forem surgindo novos casos, a jurisprudência, inclusive dos Tribunais Superiores, irá se pacificar, formalizando entendimentos inerentes ao controle de dados por empregadores, aplicação dos institutos jurídicos e danos causados as pessoas naturais.

Aliás, assim como a GDPR serviu de paradigma para a elaboração da LGPD, há precedentes também já ocorridos sob a ótica da GDPR com punições estabelecidas pelas autoridades de dados que serão analisados para trazer à tona elementos de discussão e consequente multas estabelecidas nos casos.

6.2 Precedentes inerentes à Proteção de Dados na União Europeia à luz da GDPR

Além dos precedentes acima apresentados inerentes a aplicação da LGPD na Justiça Laboral e de acordo a norma brasileira, é importante ressaltar que já há casos que a autoridade internacional aplicou penalidades a diversas empresas por incidentes de segurança ocorridos que acarretaram em vazamento de dados de diversos titulares de dados.

Diante da preocupação global com o uso indevido de dados pessoais, o (GDPR) foi aprovado, em 15 de abril de 2016, pelo Parlamento Europeu e, após dois anos de transição para as empresas, iniciou sua vigência efetiva em 25 de maio de 2018, com o objetivo de prever regras relacionadas à proteção e transferência de dados das pessoas naturais. Segundo Ribeiro[159], "A GDPR exerceu forte influência na LGPD, inclusive com a utilização na legislação brasileira de termos europeus, de forma que ao entender aquela lei, é possível entender a nossa".

O que se percebe, desde o advento da Lei 13.709/2018, a partir da análise de julgados (os poucos até então prolatados sobre a temática), é uma verdadeira interpretação minuciosa sobre a aplicação da LGPD, ao verificar se os princípios previstos foram ou não violados, especialmente, a análise do confronto entre público e privado.

Diferentemente da norma europeia, que possui artigo específico quanto ao processamento dos dados pessoais dos empregados no contexto de trabalho, mais precisamente no artigo 88 do GDPR, a LGPD prevê a proteção e o processamento de dados de forma geral:

---

[159] RIBEIRO, Cinthya Imano Vicente. **Privacidade digital das instituições bancárias**. 2019. Dissertação (Mestrado em Direito Comercial) - Pontifícia Universidade Católica de São Paulo, São Paulo/SP, 2019. p. 71. Disponível em: https://tede2.pucsp.br/bitstream/handle/22990/2/Cinthya%20Imano%20Vicente%20Ribeiro.pdf. Acesso em: 04 maio 2022.

> Art. 88 – Processamento no contexto do emprego:
> 1 Os Estados-Membros podem, por lei ou por acordos coletivos, estabelecer regras mais específicas para garantir a proteção dos direitos e liberdades no que diz respeito ao processamento dos dados pessoais.[160]

Dividida em 11 capítulos, o GDPR determina regras, princípios, deveres e direitos direcionados a cidadãos e autoridades sobre o uso de dados, em bancos de empresas, de cidadãos europeus dentro e fora do continente. Em sua versão atualizada, a Data Protection Directive de 1995 (Diretiva 95/46/CE) se aplica aos negócios nas marketplaces ou lojas virtuais, pois a antiga regulação ficou defasada no que diz respeito à proteção dos dados bancários transacionados de maneira virtual.

O primeiro avanço implementado pela lei europeia foi a obrigação imposta às empresas e organizações de incluírem em seus contratos dispositivos que informassem o uso dos dados pessoais aos seus titulares em razão da entrada em vigor da lei. Além disso, também passou a ser obrigação das empresas implementarem, regularmente, avisos de privacidade, explicando como elas conseguem permissão para usar os dados dos cidadãos e qual a finalidade de seu uso. Mesma obrigação se aplica no Brasil, desde que a passou a vigorar a LGPD, pois estabelece como princípios norteadores da atividade de tratamento de dados pessoais a finalidade, necessidade, adequação, livre acesso e transparência.

Outro avanço implementado pelo GDPR foi a imposição de multas severas aos casos de descumprimento de padrões de segurança para coleta e/ou utilização de dados dos consumidores. No que diz respeito às sanções, vale mencionar que vão além da questão financeira, incluindo a imposição de procedimentos típicos de compliance, como por exemplo, efetuar monitoramento e treinamento das pessoas/empresas envolvidas no tratamento de dados.

Em síntese, ao longo de seus 05 anos de aprovação e 03 de vigência, o GDPR funcionou como um catalisador de mudanças, não só legais, mas comportamentais, motivando a criação de diversos diplomas relacionados ao tema em outros países, como a edição da LGDP no Brasil, que foi claramente influenciada pela legislação europeia.

Importante registrar que o item 5, do artigo 30º, do GDPR, preconiza que as micro, pequenas e médias empresas que possuírem menos de 250 (duzentos e cinquenta) trabalhadores estarão dispensadas de manter o registro de suas atividades de tratamento de dados. O mesmo vale para o artigo 13, do GDPR. Outrossim, o artigo 9º dispõe sobre o processamento de

---

[160] BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

categorias especiais de dados pessoais, podendo ser realizado, se necessário, para efeitos de medicina do trabalho ou para avaliação da capacidade de trabalho do empregado.

O GDPR estabelece regras mais específicas para garantir a proteção dos direitos e liberdades no que diz respeito ao processamento dos dados pessoais dos empregados no contexto de trabalho. Enaltece-se a situação específica, em seu caráter coletivo, dentro de um grupo de empresas ou a um grupo de empresas envolvidas em uma atividade econômica conjunta e sistemas de monitoramento no local de trabalho.

Fundamentalmente, Alves [161] destaca os fundamentos do GT29 envolvendo a declaração e orientação a grupos de trabalhos inerentes à proteção de dados, quais sejam:

> No mais, conforme consta das próprias diretrizes do GT29, é preciso destacar que o âmbito da aplicação das orientações ali dispostas leva em consideração uma diversidade de fundamentos, a saber:
> *a)* a declaração do Grupo de Trabalho do Artigo 29º para a Proteção de Dados 14/EN WP 2186;
> *b)* as orientações do Grupo de Trabalho do Artigo 29º sobre o encarregado da proteção de dados 16/EN WP 2437;
> *c)* o parecer do Grupo de Trabalho do Artigo 29º sobre a limitação das finalidades 13/EN WP 2038; e
> *d)* normas internacionais, como, por exemplo, a norma ISO 31000: 2009 (Gestão do Risco – Princípios e linhas de orientação), ISO/ETC 29134 (Tecnologias da informação – Técnicas de segurança – Avaliação de impacto na privacidade – Orientações).

Em seu Capítulo VIII, o GDPR prevê as sanções que deverão ser aplicadas, caso suas disposições sejam violadas. Segundo o artigo 83, no caso de diversas violações às disposições da GDPR, no âmbito das mesmas operações de tratamento de dados, o infrator estará sujeito à multa, em valores expressivos, a ser aplicada a cada caso, de forma efetiva e proporcional. Assim, a norma prevê 02 faixas de multa, a serem aplicadas de acordo com a gravidade das infrações, sendo que o valor não poderá ultrapassar o valor atribuído à infração mais gravosa. Para infrações mais leves, as multas poderão chegar a EUR 10 milhões ou 2% do faturamento bruto mundial da empresa ou conglomerado no exercício fiscal anterior à instauração do processo, o que for maior. Já para as infrações mais graves, o patamar é elevado a EUR 20 milhões ou 4% do faturamento bruto mundial.

Percebe-se, portanto, que assim como foi instituído pela LGPD, o GDPR, ao aplicar sanções, também leva em consideração as circunstâncias do caso concreto, elencando, em rol

---

[161] MALDONADO, Viviane Nóbrega; BLUM, Renato (coord.). **Comentários ao GDPR**: Regulamento Geral de Proteção de Dados da União Europeia. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 201-202.

exemplificativo, alguns fatores que contribuem na fixação do valor da multa, tanto para atenuar como agravar este montante.

Diante das referidas explicações e dos paradigmas internacionais, faz-se necessário apresentá-los a fim de demonstrar o entendimento sobre a temática e como paradigmas para a aplicação de penalidades aos responsáveis pelo uso dos dados recebidos:

6.2.1 British Airway – Reino Unido

No dia 16 de outubro de 2020, o Information Comissioners Office (ICO), à luz do GDPR, multou a British Airway no montante de £ 20.000.000,00 (vinte milhões de libras) por não proteger os dados pessoais e financeiros de mais 400.000 clientes.[162]

Não obstante, em 2018, a empresa, durante dois meses, foi alvo de ataques cibernético. Acredita-se que os invasores tenham acessado dados pessoais de clientes e funcionários, como nomes completos, endereços, números de cartões de pagamento e códigos de segurança, bem como os nomes de usuários e as senhas das contas de funcionários e administradores. Após a devida investigação, a ICO apurou que a British Airway, na realidade, tratou grande quantidade de dados pessoais sem adotar as medidas de segurança adequadas, infringindo a lei de proteção de dados pessoais. Além disso, concluiu que a empresa, se tivesse identificado suas fraquezas de segurança e adotado medidas corretivas e preventivas, poderia ter evitado o ataque. Dentre as medidas que poderiam ter sido adotadas: (*i*) limitado o acesso de aplicativos, dados e ferramentas a somente ao que era necessário; (*ii*) realizado testes rigorosos, simulando ataques cibernéticos; (*iii*) protegido as contas dos funcionários e terceiros com autenticação multifatorial; e (*iv*) adotado outras medidas adicionais.

Ao fundamentar a multa de 20 milhões de Libras, a Comissária de Informações Elizabeth Denham alegou que:

> As pessoas confiaram seus dados pessoais à British Airway e ela não tomou as medidas adequadas para manter esses detalhes seguros. Quando as organizações tomam decisões ruins em torno dos dados pessoais das pessoas, isso pode ter um impacto real na vida delas. A lei (GDPR), agora, nos dá ferramentas para incentivar as empresas a tomarem melhores decisões sobre dados, incluindo investir em segurança atualizada.[163]

---

[162] SHEAD, Sam L. British Airways multada em £ 20 milhões por violação de dados que afetou mais de 400.000 clientes. *In:* CNBC, [s.l.], 16 out. 2020. Disponível em: https://www.cnbc.com/2020/10/16/british-airways-fined-20-million-for-data-breach-by-ico.html. Acesso em: 12 maio 2022.

[163] KUCHLER, Hannah. Punição britânica ao Facebook abre precedentes. **Valor,** São Paulo, 12 jul. 2018. Disponível em: https://valor.globo.com/empresas/noticia/2018/07/12/punicao-britanica-ao-facebook-abre-precedentes.ghtml. Acesso em: 12 maio 2022.

Posto a violação ter ocorrido em junho de 2018, antes do Reino Unido deixar a União Europeia, a sanção pôde ser aplicada e a IOC investigou os fatos em nome de todas as autoridades da União Europeia, como autoridade supervisora líder da GDPR.

6.2.2 Marriot International - Reino Unido

A Marriot International, no dia 30 de outubro de 2020, foi condenada à segunda maior pena de multa do Reino Unido, no valor de £ 18.400.000,00 (dezoito milhões e quatrocentos mil Libras), após a devida investigação e apuração de violação de dados pelo ICO.[164] A referida multa foi aplicada pela violação de dados envolvendo o sistema de reservas de hóspedes Starwood. A falha de segurança começou com um ataque cibernético contra a Starwood Hotels and Resorts Wordwide, em julho de 2014. Em 2016, a Marriot International adquiriu a Starwood, mas não conseguiu detectar a brecha até setembro de 2018.

Os dados vazados incluíam nomes, *e-mails*, telefones, números de passaporte e, em alguns casos, informações criptografadas do cartão de pagamento. A Marriot estima que a violação expôs informações pessoais de, aproximadamente, 339 milhões de clientes em todo o mundo, contudo não foi capaz de dar um número mais preciso, já que pode ter ocorrido vários registros para clientes individuais. Até hoje, a ICO não conseguiu identificar a identidade do invasor. Porém, em suas investigações, constatou que houve graves falhas da Marriot, que não adotou medidas técnicas ou organizacionais adequadas para proteger os dados pessoais que estavam sendo processados em seus sistemas, como exige a GDPR.

6.2.3 Google Inc. - França

Em 21 de janeiro de 2019, a Google Inc. foi condenada, pela Comissão Nacional de Proteção de Dados da França (CNIL), a pagar multa no valor de € 50.000.000 (cinquenta milhões de Euros), por violar os termos da GDPR no que tange à falta de transparência, informações inadequadas e falta de consentimento em relação à personalização dos anúncios.[165]

Em 25 e 28 de maio de 2018, imediatos à vigência da GDPR, as associações None of Your Business (NOYB) e a La Quadrature du Net (LQDN) apresentaram reclamações à CNIL,

---

[164] SCHWARTZ, Matthew J. Marriott recebe multa de privacidade de US$ 24 milhões do GDPR por violação. *In:* BANK INFO SECURITY, [s.l.], 2 nov. 2020. Disponível em: https://www.bankinfosecurity.com/marriott-hit-24-million-gdpr-privacy-fine-over-breach-a-15288. Acesso em: 12 maio 2022.

[165] COMITÉ restrito da CNIL impõe uma sanção financeira de 50 milhões de euros à Google LLC. *In:* EDPB – European Data Protection Board, França, 21 jan. 2019. Disponível em: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc. Acesso em: 14 maio 2022.

alegando que a Google não tinha base jurídica válida para processar os dados pessoais dos usuários de seus serviços, especialmente para fins de personalização dos anúncios. Após as inspeções, a Comissão constatou que a Google cometia dois tipos de violações à GDPR. Primeiramente, violava as obrigações de transparência e informações, pois dificultava aos usuários o acesso a informações essenciais, como os fins do processamento de dados, os períodos de armazenamento ou as categorias de dados pessoais utilizadas para a personalização dos anúncios, bem como outras informações relevantes.

Além disso, quando disponibilizadas, tais informações não eram claras, nem abrangentes. Os usuários não tinham a capacidade de entender, de forma clara e completa, a extensão das operações de tratamento de dados pessoais realizadas pela Google. Aos serem descritos de forma genérica e vaga, os respectivos processos não permitiam que o usuário entendesse que a base legal de operações de processamento para personalização dos anúncios não era o legítimo interesse da empresa, mas sim o consentimento.

Quanto ao consentimento, averiguou-se que ele não era obtido de forma válida, pois, além de os usuários não serem informados a seu respeito, seu teor não era inequívoco, nem específico. A multa, no valor de €50.000.000, contra a Google Inc. se justificou pela gravidade das infrações praticadas em violação a três princípios essenciais da GDPR: a transparência, a informação e o consentimento. Cabe salientar que esses três princípios também são aplicados na LGPD, sendo o consentimento um dos princípios mais valorados pela Lei brasileira de proteção de dados.

Diante das referidas perspectivas, no Mundo, estima-se que no ano de 2021 os prejuízos envolvendo riscos cibernéticos alcançaram 6 (seis) trilhões de dólares. [166] Indubitavelmente, na era do fluxo internacional de dados, é certo que a expressão digital trade é muito comum. Segundo Bialer e Couto[167], sobre a OCDE e o Conselho da Europa:

> Com a constatação de que a tecnologia era cada vez mais transnacional e que suas consequências sociais não poderiam ser exaustivamente tratadas por leis nacionais, o fluxo de dados transfronteiriços começava a se estabelecer como uma característica das aplicações de informática e um dos desafios em termos de garantia de comércio internacional. Tanto é assim que, atualmente, é comum a referência à expressão digital trade para abordar discussões relevantes sobre fluxo internacional de dados. Para a OCDE havia, naquele momento, uma necessidade de convergência nas abordagens adotadas por

[166] LIMA, Ana Paula Moraes Canto de Lima; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. **LGPD Lei Geral de Proteção de Dados**: sua empresa está pronta?. São Paulo: Literare Books International, 2020. p. 163.

[167] BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Claudia. **Proteção de dados pessoais no Brasil**: Uma nova visão a partir da Lei n.º 13.709/2018. Belo Horizonte: Fórum, 2019. p. 227.

> seus Estados Membros para lidar com o tema do fluxo internacional de dados pessoais.

Por sua vez, Pinheiro[168] afirma que, na "União Europeia, conseguiu-se alcançar o objetivo de consolidar em um único regulamento geral a regra de 28 Estados-Membros, conquistado com o GDPR; a mesma sorte não houve nas demais regiões do planeta".

Diante das referidas diretrizes e com base nos paradigmas ora elencados, é possível verificar que, no Brasil, a LGPD ainda terá um longo caminho a percorrer no que concerne as inovações apresentadas e a forma de controle/sanção em face de empresas. Contudo, é algo que efetivamente acrescentará um cenário de controle de dados, a fim de reduzir danos à toda coletividade, com base nos preceitos estrangeiros ora arrolados.

---

[168] PINHEIRO, Patricia Peck. **Proteção de dados pessoais comentários à Lei n. 13.709/2018 (LGPD)**. 3. ed. São Paulo: Saraiva Jur, 2021. p. 71.

7 DA CONTRIBUIÇÃO PARA CASOS CONCRETOS: MELHORES PRÁTICAS E MANUAL DE CONDUTA INTERNO PARA EDUCAÇÃO EMPRESARIAL EM SEGURANÇA E CONTROLE DE DADOS

Conforme já foi apresentado anteriormente, as regras de proteção de dados atualmente em vigor buscam, em um caráter geral com aplicabilidade em um viés social, econômico e jurídico trazer aos titulares de dados segurança suficiente para evitar a transmissão indevida de dados e consequentemente danos que podem surgir em caráter financeiro ou até mesmo sob o aspecto criminal.

Além do referido fato, as empresas em geral não estão preparadas para a adequação nos moldes das determinações constantes das normas e em decorrência disso, podem ser penalizadas pelos aspectos legais da LGPD, justamente pela falta de adequação, irregularidades e danos causados aos titulares de dados, especialmente pela responsabilidade civil objetiva prevista no tratamento dos dados naturais decorrentes da atividade empresarial prestada.

Em que pese os julgados apresentados, veja-se que não há em nenhum descritivo, a apresentação de um manual de boas práticas ou programas de compliance para atuar, prevenir ou remediar um incidente de segurança, tratando-se, portanto, de um tema essencial aos empresários e manuseadores de dados naturais, sensíveis e privados.

Nesse sentido, o presente tópico abordará um aspecto de segurança educacional as empresas, uma vez que, não é necessário somente seguir à legislação, pelo contrário, é essencial a formalização de estudos e planos de segurança para que as empresas se adequem a atividade prestada, no sentido de fornecer um manual com as melhores práticas para guarda, transmissão, exclusão, transferência e tratamento de dados, bem como, determinações em caso de incidentes de segurança ocorridos durante a atividade empresarial.

Nesse sentido, como pontuado anteriormente, a entrada em vigor da Lei Geral de Proteção de Dados colocou o Brasil na lista de países que contam com legislação específica quanto à proteção de dados e da privacidade. Como a LGPD estabelece uma série de regras com as quais as empresas e organizações atuantes no Brasil terão que se compatibilizar, estar em *compliance* é necessário, principalmente para o fim de permitir que os cidadãos tenham maior controle sobre o tratamento que é dado as suas informações pessoais, assim como prevenir a prática de ilícitos e evitar a aplicação de penalidades.

Em síntese, estar em compliance significa estar em conformidade com leis e regulamentos internos e externos. Trata-se do conjunto de regras internas que regulam as mais diversas atividades da empresa, a fim de que esteja em consonância com as normas vigentes e

a ela aplicáveis.[169] Será a partir das regras de compliance que a empresa poderá coibir comportamentos futuros inadequados que possam macular a sua reputação, além de lhe trazer outras vantagens, como descontos em linhas de crédito, melhor retorno de investimentos[170] e, no caso de eventuais incidentes de segurança, a possibilidade de atenuar as sanções administrativas que venham a ser impostas, ou melhor, de evitar a sua prática.

A falta de adequação ao regramento da LGPD, além de sujeitar as empresas a sanções civis e administrativas, também traz riscos a sua imagem. Justamente nesse aspecto, Cots e Oliveira[171] afirmam sobre as sanções administrativas, a pendência de regulamento e as consequentes punições previstas no artigo 54 da LGPD dependem de um regramento específico da autoridade nacional para que sejam delimitadas as penalidades, apresentando-se as hipóteses, metodologia e o cálculo base para aplicação das multas. Tal regramento visará garantir segurança jurídica aos agentes de tratamento dos dados, bem como, fortificar a necessidade das empresas em criar mecanismos e manuais de segurança para a realização da atividade empresarial, uma vez que, não bastará somente seguir a legislação se a adequação dos agentes não for viabilizada.

No atual cenário da sociedade, como praticamente os contratos e quaisquer conexões são preenchidos/gerados com dados pessoais, dados pessoais sensíveis e banco de dados, uma vez pontuadas as atividades a serem exercidas pelas empresas através do controlador, operador e encarregado, haverá uma melhor visualização acerca dos direitos dos titulares dos dados pessoais. Somando-se ao referido fato, a responsabilidade objetiva do controlador dos dados que, ciente dos procedimentos de segurança e da necessidade de guarda dos dados, não poderá alegar desconhecimento das demandas internas da empresa.

Parece que a LGPD vem consagrar a intimidade e a privacidade no ramo do Direito do Trabalho, assim como em todas as áreas do Direito.

É notório que há uma grande preocupação das empresas sobre a divulgação de maneira correta de informações pelos funcionários, com o intuito de preservar os mais diversos dados. Como visto, primordialmente, cabe a empresa tomar a devida cautela ao coletar dados

---

169 UGGERI, Karollyne. Compliance digital: os benefícios da implementação. *In:* MIGALHAS, São Paulo, 1º mar. 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI275349,51045Compliance+digital+os+beneficios+da+implementacao. Acesso em: 11 nov. 2020.

170 UGGERI, Karollyne. Compliance digital: os benefícios da implementação. *In:* MIGALHAS, São Paulo, 1º mar. 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI275349,51045Compliance+digital+os+beneficios+da+implementacao. Acesso em: 11 nov. 2020.

171 COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 210.

(exemplo: entrevista de emprego); produzir dados (exemplo: elaboração de contratos); recepcionar dados (exemplo: via e-mail ou telefone); classificar dados (exemplo: público ou privado); e utilizar dados (exemplo: usar somente dentro da empresa).

Se a cultura da preservação de dados não imperar, resultados drásticos existirão, entre eles, e de forma acentuada, a demissão por justa causa. Pois, o mau proceder está acima do desrespeito às normas internas daquela empresa. Esse mau proceder se baseia na medida errada perante o próprio ser, trazendo malefícios para um pequeno grupo e, consequentemente, à sociedade.

Cautelosamente, empregador-funcionário possuem responsabilidades sociais e, certamente, estão acima daquele ato particular. No campo do Direito do Trabalho, na relação entre empresa e funcionário, enquanto o contrato de trabalho estiver ativo e até o momento de sua eventual rescisão, haverá o tratamento de dados pessoais entre empregador-funcionário, nos termos dos incisos I e III, do artigo 15, da LGPD

Salienta-se que o artigo 3º da LGPD é categórico ao aduzir que:

> Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.[172]

Mas, e se o funcionário divulgar dados em caráter internacional? Aplicar-se-á a demissão por justa causa, com base na LGPD? Nesse contexto, Reis[173] assevera a preocupação da aplicação da LGPD nas relações de trabalho, uma vez que, as informações de clientes e titulares de dados não tem o condão de segurança adequado para resguardar as partes envolvidas, demandando-se, por consequência, a necessidade de cumprimento da norma por

---

[172] BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

[173] REIS, Beatriz de Felippe. A cultura de compliance em matéria de proteção de dados e sua adoção no âmbito laboral. **Revista de Direito do Trabalho e Seguridade Social**, São Paulo, v. 46, n. 214, p. 323-340, nov./dez. 2020.

intermédio de manuais, boas práticas e programas de compliance para garantir o cumprimento e respeito aos direitos fundamentais de inviolabilidade de todos os agentes no processo de tratamento de dados.

Nesse contexto, a partir da LGPD, renasce a ideia de compliance digital, sub-ramo existente, mas cuja relevância não era vista com tanta imprescindibilidade como atualmente, em especial, frente às necessidades de proteção e correto tratamento dos dados pessoais.

Na seara empresarial, o compliance digital consiste na análise de riscos e na adoção de medidas preventivas para a adequação da empresa às regras aplicáveis às tecnologias da informação.[174] Ao contribuir para a manutenção da imagem e do valor das empresas, hoje, a sua prática constitui ferramenta essencial, tanto que, ao lado da legitimação de investigações, uma de suas vantagens é a demonstração de boa governança e respeito.

A discussão sobre compliance digital ganhou maior destaque após as ondas de ataques cibernéticos, o que alertou o mercado, em especial, o brasileiro, para a insuficiência de cuidados relativos à segurança de dados. Contudo, a sua aplicação, por si só, não é suficiente à proteção empresarial, sendo necessária a revisão constante das políticas de controle e a análise de riscos por meio de uma fiscalização eficiente. São essas condutas preventivas que evitarão os ilícitos.

Além de contribuir para a criação de um ambiente empresarial mais seguro e eficiente, a instauração de políticas de compliance digital também colabora para construção de relações transparentes entre as empresas e seus respectivos fornecedores e clientes.[175] Por mais que a LGPD só tenha entrado em vigor em 18 de setembro de 2020, com o fim de evitar as penalidades legalmente previstas pelo tratamento irregular de dados pessoais, que variam desde multas até a suspensão de tal atividade, aos times de *compliance* cabe planejar as estruturas e procedimentos internos das empresas, adequando-os ao nela disciplinado.

Indubitavelmente, para uma empresa, o objetivo maior é a proteção de dados próprios e, até mesmo, de terceiros. Do contrário, ou seja, a falta de proteção de dados da empresa pelos funcionários poderá gerar danos, muitos deles incalculáveis, resultando na possível demissão por justa causa (podendo aplicar a figura do "mau procedimento", conforme previsto na alínea "b", do artigo 482, da CLT). Não se trata de um projeto de uma única área, mas de toda a

---

174 UGGERI, Karollyne. Compliance digital: os benefícios da implementação. *In:* MIGALHAS, São Paulo, 1º mar. 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI275349,51045Compliance+digital+os+beneficios+da+implementacao. Acesso em: 11 nov. 2020.

175 UGGERI, Karollyne. Compliance digital: os benefícios da implementação. *In:* MIGALHAS, São Paulo, 1º mar. 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI275349,51045Compliance+digital+os+beneficios+da+implementacao. Acesso em: 11 nov. 2020.

empresa. A adequação às normas da LGPD consiste em um plano multidisciplinar, envolvendo os mais diversos setores, como jurídico, tecnologia, segurança da informação, recursos humanos, marketing, ética empresarial, responsabilidade social, entre outros. As regras e os princípios da privacidade e os relativos à proteção de dados pessoais, portanto, precisam ser inseridos e previstos como valores e missões de toda a corporação.[176]

Nesse sentido, Vainzof, Lima e Tamer[177] asseguram que:

> Os empresários que enxergarem a proteção de dados pessoais como importante direito dos indivíduos, que pode se tornar inclusive fundamental, e não somente como mais uma obrigação a ser cumprida, certamente executarão de forma melhor as necessidades legais, mitigarão mais riscos e ganharão a confiança dos cidadãos e do mercado.

A ideia é que os agentes de tratamento tenham uma área estruturada e um plano de adequação às normas da LGPD, de modo que possam mapear e classificar as suas atividades, instruir os profissionais envolvidos e/ou contratar novos, se necessário, reformular estruturas, planejar e implantar normas internas de acordo com a legislação, entre outras.

Em seu estudo, Vainzof, Lima e Tamer[178] destacam que o primeiro passo à adequação e, consequentemente, para evitar a prática de ilícito sujeito às sanções, é o mapeamento das atividades da empresa, também conhecido como *data flow*, ou seja, entender tudo aquilo que a empresa coleta e trata a título de dados pessoais. Ou seja, no desempenho de suas atividades (artigo 37), os funcionários devem manter o registro das operações de tratamento de dados pessoais que realizarem. Partir de tal análise, é possível traçar um retrato do fluxo de dados de todas as áreas da empresa.

---

176 VAINZOF, Rony; LIMA, Caio César Carvalho; TAMER, Maurício Antonio. Compliance e LGPD: plano de adequação como ferramenta de mitigação de riscos legais. *In:* JOTA, [s.l.], 07 abr. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-adequacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019. Acesso em: 20 nov. 2020.

177 VAINZOF, Rony; LIMA, Caio César Carvalho; TAMER, Maurício Antonio. Compliance e LGPD: plano de adequação como ferramenta de mitigação de riscos legais. *In:* JOTA, [s.l.], 07 abr. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-adequacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019. Acesso em: 20 nov. 2020.

178 VAINZOF, Rony; LIMA, Caio César Carvalho; TAMER, Maurício Antonio. Compliance e LGPD: plano de adequação como ferramenta de mitigação de riscos legais. *In:* JOTA, [s.l.], 07 abr. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-adequacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019. Acesso em: 20 nov. 2020.

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseados em legítimo interesse.[179]

O mapeamento das atividades empresariais permite avaliar quais bases legais de tratamento são necessárias; se é ou não possível realizar a comunicação ou o uso compartilhado de dados entre as empresas; o quanto vale a pena investir em medidas de anonimização; qual o ciclo de vida dos dados pessoais dentro da empresa; se há ou não padrões/normas técnicas específicas; compreender quais departamentos e quais colaboradores precisam ser instruídos; onde devem ser aplicadas as soluções tecnológicas e de segurança; quais procedimentos devem ser adotados para garantir a contenção de tais informações; e, principalmente, qual a categorização legal da empresa, se se enquadra como controladora ou operadora de dados pessoais.[180]

O objetivo dessa primeira etapa é definir quais medidas de adequação devem ser adotadas e a quais riscos de responsabilização a empresa estará submetida.[181] Ademais, cabe aos agentes de tratamento avaliar se o risco que poderá ser colocado ao titular por eventual incidente é alto o suficiente para ensejar a notificação da ocorrência, seja à autoridade seja ao próprio titular. Não obstante, é com base nesses registros e documentação das operações de tratamento de dados que a Agência Nacional de Proteção de Dados (ANPD) se baseará ao dosimetrar a sanção a ser aplicada, em caso de violações aos termos legais.

A segunda providência, ainda segundo Vainzof, Lima e Tamer[182], diz respeito ao comprometimento dos profissionais que detêm o poder de direção com a adequação da empresa. O ideal é que os gerentes e administradores tenham consciência de que, para prevenir as empresas/organizações de eventuais prejuízos sancionatórios e de reputação, é preciso fazer investimentos financeiros e em pessoal. Nas palavras dos autores, "é o investimento a ser feito hoje que irá diminuir os riscos de incidentes de dados pessoais amanhã".

---

179 BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

180 VAINZOF, Rony; LIMA, Caio César Carvalho; TAMER, Maurício Antonio. Compliance e LGPD: plano de adequação como ferramenta de mitigação de riscos legais. *In:* JOTA, [s.l.], 07 abr. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-adequacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019. Acesso em: 20 nov. 2020.

181 VAINZOF, Rony; LIMA, Caio César Carvalho; TAMER, Maurício Antonio. Compliance e LGPD: plano de adequação como ferramenta de mitigação de riscos legais. *In:* JOTA, [s.l.], 07 abr. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-adequacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019. Acesso em: 20 nov. 2020.

182 VAINZOF, Rony; LIMA, Caio César Carvalho; TAMER, Maurício Antonio. Compliance e LGPD: plano de adequação como ferramenta de mitigação de riscos legais. *In:* JOTA, [s.l.], 07 abr. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-adequacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019. Acesso em: 20 nov. 2020.

Outra medida de suma importância seria a nomeação do encarregado, cargo similar ao DPO, previsto na legislação europeia, dando cumprimento ao disposto no artigo 41 da LGPD[183]. O encarregado, como detalhado em item anterior, é o elo de comunicação entre o controlador, os titulares de dados pessoais e a ANPD, sendo responsável por fiscalizar o cumprimento da lei, receber e processar as reclamações e promover o adequado treinamento dos colaboradores da empresa sobre a proteção de dados. Seja através da fiscalização que exerce ou do treinamento daqueles que irão tratar os dados pessoais, a sua presença e atuação dentro da empresa é fator positivo para a inibição de infrações legais e incidentes de segurança.

O quarto passo, e um dos mais relevantes para evitar ou reduzir as sanções se, eventualmente, aplicadas, é adoção de medidas de segurança**.** Tais medidas visam mitigar acessos não autorizados aos dados pessoais tratados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilegal, como pontua o artigo 46 da LGPD.[184] Aqui, se tem inserte a imprescindibilidade do consentimento do titular como uma das medidas de segurança mais importantes. Como decorrência lógica da privacidade e da autodeterminação, as empresas apenas poderão tratar dados pessoais se tiverem o consentimento do respectivo titular, sendo, inclusive, a primeira base legal estabelecida pela Lei para tratamento de dados.

Não obstante, pondera-se no presente ato a necessidade de fornecimento de cursos, palestras e orientações a todo grupo de empregados que manuseia dados e tem conhecimento dessa possibilidade de vazamento, cabendo a demonstração dos controles fornecidos pela empresa para evitar incidentes de segurança.

---

183 LGPD, "Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
§ 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados." (BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

184 LGPD, "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito." (BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

Vainzof, Lima e Tamer[185] enfatizam a necessidade de implementação das medidas de boas práticas e governança, conforme disciplinadas no artigo 50 da LGPD[186], que prevê a necessidade de boas práticas pelos controladores e operadores de dados, a fim de que possam adequar os procedimentos de reclamações, normas de segurança e padrões técnicos da empresa para atuar em conjunto com a autoridade nacional em todo e qualquer ato ocorrido.

São medidas que, por sua vez, implicam na criação ou no ajustamento das políticas internas de segurança da informação da empresa, impondo, assim, o comprometimento dos agentes de tratamento de dados na busca pelo cumprimento e adequação à legislação, utilizando-se os preceitos, princípios e conceitos gerais da LGPD.[187]

Aliás, quanto a esses últimos dois passos, verifica-se que a própria LGPD, em seu artigo 52, §1º, estimula que todas as medidas de segurança sejam adotadas, considerando-as, inclusive, como critérios para dosimetria das sanções administrativas. Dessa forma, mesmo que acidentalmente ocorra algum incidente de segurança que possa causar danos, caso a empresa tenha, previamente, adotado medidas de segurança, boas práticas e de governança, tal postura será considerada a título de atenuante.

> §1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:[...]
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; [...].[188]

Por fim, e não menos importante, talvez, até a mais, seria a criação de uma cultura de proteção de dados a todos os empregados. Tendo por intuito demonstrar a importância da

---

185 VAINZOF, Rony; LIMA, Caio César Carvalho; TAMER, Maurício Antonio. Compliance e LGPD: plano de adequação como ferramenta de mitigação de riscos legais. *In:* JOTA, [s.l.], 07 abr. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-adequacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019. Acesso em: 20 nov. 2020.

186 BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022

187 VAINZOF, Rony; LIMA, Caio César Carvalho; TAMER, Maurício Antonio. Compliance e LGPD: plano de adequação como ferramenta de mitigação de riscos legais. *In:* JOTA, [s.l.], 07 abr. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-adequacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019. Acesso em: 20 nov. 2020.

188 BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

temática e esclarecer os riscos aos quais a empresa e os seus profissionais estão sujeitos, recomenda-se a promoção de cursos e palestras sobre o conteúdo da Lei e sua repercussão no cenário empresarial tecnológico, assim como simulações com seus colaboradores, a fim de treiná-los para evitar incidentes graves, como o vazamento de dados.

Acredita-se que é indispensável fazer uma mudança na mentalidade corporativa, inserir no "espírito" da empresa a importância da transparência na coleta, no uso e no tratamento de dados pessoais. As empresas devem enxergar além das penalidades a que poderão estar sujeitas e entender que estar em conformidade com a legislação é mais do evitar perdas financeiras, é dar atenção a outros valores tão importantes quanto, como a reputação e a confiança dos clientes, fornecedores e funcionários.[189]

Quando se fala em melhores práticas/sugestões que as empresas poderão adotar diante de um incidente de segurança, tal assunto sempre está diretamente relacionado com os impactos direcionados às empresas, ao poder público e à sociedade como um todo. Significa dizer que o impacto na empresa vítima de vazamento de dados poderá ser incalculável, dependendo da situação, da forma como ocorreu o vazamento, as pessoas atingidas, enfim, os danos ocasionados efetivamente. Nesse cenário, o funcionário que eliminar algum dado de forma indevida, poderá ser demitido por justa causa, ante o estabelecimento de regras de segurança que se apliquem a toda coletividade empresarial.

Parece que o meio digital solucionou grande parte do problema das empresas quanto à existência de espaços físicos. Contudo, atualmente, a grande preocupação é ter bons servidores com uma ótima capacidade de memória para guardar todos os documentos adequadamente.

Sobre a abstratividade dos prejuízos financeiros, considerando-se, ainda, a possibilidade de se tratar de um crime (ou melhor, *cibercrime*), Almeida[190] sustenta que, além da necessidade de mitigação dos riscos pelas boas práticas, faz-se necessária a contratação de seguro e reserva financeira no aspecto financeiro. Além disso, existem os danos reputacionais que podem ocorrer em crimes digitais que devem ser pautados na necessidade de reparação dos danos, por isso, a constituição de reserva financeira para que haja possibilidade social de prosseguimento da

---

189 PERONGINI, Maria Fernanda Hosken. Efeitos da compliance na proteção de dados pessoais. *In:* MIGALHAS, São Paulo, 21 ago. 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI285967,21048-Efeitos+da+compliance+na+protecao+de+dados+pessoais. Acesso em: 13 jun. 2019.

190 LIMA, Ana Paula Moraes Canto de Lima; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. **LGPD Lei Geral de Proteção de Dados**: sua empresa está pronta?. São Paulo: Literare Books International, 2020. p. 175.

atividade no futuro, ponderando-se, inclusive, o risco de falência em decorrência de atos ocorridos sob tal ótica.

Prosseguindo, a autora lista algumas medidas relacionadas tanto à empresa como aos indivíduos, sendo que, com relação as responsabilidades as empresas, é possível listar (i) senhas rigorosas; (ii) políticas de arquivamento e backup de documentos; (iii) política de privacidade; (iv) criptografia; (v) assinatura e certificado digital; (vi) certificado digital; (vii) controle de acesso; (viii) antivírus e (ix) registro de eventos.

Em paralelo, com relação aos indivíduos, a autora sustenta a necessidade de (i) uso de senhas complexas e diferentes com dois fatores de autenticação das senhas utilizadas; (ii) substituição de senhas em caráter periódico; (iii) não abrir e-mail que seja de fonte não confiável ou desconhecida; (iv) não fazer comentários, posts ou declarações sobre dados sensíveis envolvendo a empresa ou clientes em geral; (v) realize as atividades com maior grau de atenção para evitar erros e transmissão indevidas de informações que possam acarretar em descumprimentos da legislação de proteção de dados.[191]

Outro aspecto relevante diz respeito aos atos preventivos a serem adotados pelas empresas, como por exemplo, as frentes de trabalho para a implementação da LGPD, como bem ilustra Blum[192], elaborando-se um mapeamento de todas as atividades e caminhos percorridos pelos dados para melhor entendimento sobre a adequação dos processos em confrontação com a LGPD, contendo-se como linhas gerais para execução do projeto o aspecto regulatório, a fim de que sejam analisados os processos, contratos envolvidos e forma de entrega e armazenamento da documentação, soluções fornecidas pela empresa, sistemas e tecnologia aplicada nos processos internos e consequentemente a comunicação com o Mundo externo, ou seja, a forma como o dado é transmitido, a fim de que seja analisado se há cumprimento dos aspectos da LGPD.

Veja-se que, diante da implementação do referido procedimento e a atuação conjunta dos colaboradores, a adoção de atos preventivos servirão de preceitos para que os dados manuseados sejam tratados sem risco de ocasionar danos a terceiros, especificamente clientes das empresas. Contudo, ocorrendo algum incidente de segurança, a primeira medida a ser tomada pelo controlador é a notificação às autoridades, órgãos fiscalizadores e os clientes.

---

[191] LIMA, Ana Paula Moraes Canto de Lima; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. **LGPD Lei Geral de Proteção de Dados**: sua empresa está pronta?. São Paulo: Literare Books International, 2020. p. 182.

[192] BLUM, Renato Opice. **Proteção de dados**: Desafios e soluções na adequação à Lei. Rio de Janeiro: Forense, 2021. p. 175.

Como visto, ocorrendo o efetivo vazamento de dados, o responsável pelo seu tratamento, ou seja, o controlador, em prazo razoável, deverá notificar tanto o titular dos dados como a ANPD, desde que a violação apresente risco de relevância aos direitos e liberdades dos indivíduos. Caso a notificação não seja feita ou feita em prazo não razoável, o controlador estará sujeito às penalidades legais, inclusive sujeito ao desligamento por justo motivo, pautado pela desídia do empregado, insubordinação pela ausência de comunicação ao responsável e, por fim, improbidade nas atividades laborais, nos termos do artigo 482 da CLT.[193]

À luz do que dispõe o §1º do artigo 48, na notificação, o controlador deverá relatar, obrigatoriamente: (*i*) a descrição da natureza dos dados pessoais afetados; (*ii*) as informações sobre os titulares envolvidos; (*iii*) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; (*iv*) os riscos relacionados ao incidente; (*v*) os motivos da demora, no caso de comunicação não imediata; e (*vi*) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Notificada, a ANPD avaliará a natureza, a gravidade e as consequências do incidente, o número de titulares afetados, as jurisdições impactadas e os respectivos efeitos adversos. Se julgar necessário, poderá determinar que o controlador tome medidas adicionais, como a ampla divulgação do ocorrido em canais de comunicação, assim como meios para que se possa reverter ou mitigar os efeitos do incidente.[194]

O mesmo procedimento se aplicará para a notificação dos titulares dos dados afetados, cujo objetivo é alertá-los e permitir que se previnam contra as possíveis consequências negativas do incidente. A não ser que a ANPD determine de modo contrário, a notificação aos titulares pode ser realizada por diversos meios, incluindo mensagens diretas, *e-mail*, SMS, *banners*, notificações em sites, comunicações postais ou anúncios.

É importante destacar que além das obrigações previstas na LGPD, os agentes de tratamento deverão observar as eventuais regulações setoriais a que estão submetidos. Dentre elas, o Decreto 9.936/2019, que regulamenta a Lei do Cadastro Positivo (Lei 12.414/2011),

---

193 CLT, "Art. 482 - Constituem justa causa para rescisão do contrato de trabalho pelo empregador: a) ato de improbidade; e) desídia no desempenho das respectivas funções; h) ato de indisciplina ou de insubordinação;" (BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 12 abr. 2022).

194 LGPD, "Art. 48, [...]. §2º. A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente." (BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022).

que determina que, na ocorrência de vazamento de informações de cadastrados ou de outro incidente de segurança que possa acarretar risco ou prejuízo relevante a cadastrados, o gestor de banco de dados deverá comunicar o fato, dentro do prazo de dois dias úteis, à ANPD, ao Banco Central do Brasil, quando envolver fornecimento de dados prestados por instituições autorizadas a funcionar pela autarquia federal, e a Secretaria Nacional do Consumidor (Senacon), quando houver o envolvimento do fornecimento de dados de consumidores.

Diante do exposto, reunindo-se as possibilidades de boas práticas e recomendações para os empregadores em geral, faz-se necessário: (*i*) criar uma política de boas práticas; (*ii*) criar regramento da LGPD aplicada na empresa; (*iii*) fornecer cursos, palestras, seminários e instruir os colaboradores na prática sobre os riscos da atividade e como os dados devem ser tratados; (*iv*) criar uma política de controle dados interna da empresa; (*v*) adotar medidas de segurança no que concerne ao controle dos dados; e (*vi*) formalizar equipe com pleno conhecimento dos atos praticados (agentes de tratamento, controladores, encarregados), a fim de que todos os passos necessários sejam tomados por segurança jurídica nas operações diárias.

Ressalta-se, por fim, que ocorrendo o descumprimento de quaisquer procedimentos inerentes ao controle/segurança de dados, todos os envolvidos - colaborador, agentes de tratamento, controlador ou responsáveis pelo estabelecimento - estão sujeitos às penalidades legais e, no aspecto laboral, à rescisão motivada dos contratos de trabalho.

8 CONCLUSÃO

É notório que, cada vez mais, a informação percorre longos caminhos num curto período de tempo. Em outras palavras: é muito “fácil” ter acesso à informação. Claro que no cenário atual estão “em jogo” as desigualdades de pleno acesso à internet, eis que sem isso, as pessoas não têm acesso a dados, tampouco, a informações plenas.

Isso se deve a evolução histórica da legislação que, desde o início, buscava apresentar ao titular dos dados inviolabilidade de informações, da vida e consequentemente da liberdade exercida, somada a evolução tecnológica que desencadeou a necessidade de promulgar uma legislação específica para a proteção dos dados, imputação de responsabilidade e penalidades por danos ocasionados a coletividade em geral.

Assim, sob tal aspecto, restou validada a aplicação da LGPD no aspecto laboral, seja no momento de concessão de sigilo em decorrência de dados sensíveis ou, em paralelo, na análise da transmissão de dados sensíveis de clientes, terceiros ou colaboradores em geral, manuseados por empregados e que, culposamente ou dolosamente, realizaram uma transmissão ou tratamento indevido, o que, obrigatoriamente, gera um incidente de segurança que deve ser cumprido de acordo com a norma prevista na Lei.

No âmbito laboral, verificou-se que o que se pretende é muito mais do que atribuir responsabilidade a esta ou àquela pessoa ou aquele agente, sejam coletores de dados, sejam transmissores de informações, dependendo, muitas das vezes, do contexto e da atividade que determinada empresa desempenha na órbita daquele universo. O reflexo da LGPD em caráter geral é proteger dados naturais de toda a coletividade, sejam no âmbito laboral, social, econômico ou nas demais áreas do Direito.

É fato que dados naturais, atualmente preservados e amparados por uma legislação, não podem ser manuseados ou transmitidos aleatoriamente, com o risco de serem utilizados em ambientes não autorizados e causar, em decorrência desse ato, danos a terceiros que podem não ser remediados.

Por tal premissa, restou comprovado pela análise dos julgados apresentados, que a justa causa é plenamente aplicável quando da transmissão, tratamento ou infração a dados naturais, de qualquer espécie, no ambiente laboral. Ainda que haja necessidade de vislumbrar os princípios laborais da razoabilidade e da proporcionalidade, a proteção dos dados sensíveis é primordial, devendo ser observados de forma séria e correta para que sejam preservadas as relações (*i*) entre cliente e empresa e (*ii*) entre a empregado e empregador, pautando-se sempre pela confiança mútua.

É relevante, em qualquer hipótese, analisar a conduta do agente e se efetivamente foram seguidos os procedimentos de segurança (não somente assinatura de contratos) para que a valoração da punibilidade seja compatível com o ato realizado.

A atividade empregatícia deve ser pautada pelo controle dos dados manuseados, especialmente para que não seja necessária a utilização dos preceitos do artigo 482 da CLT, que gerem a aplicação da penalidade de justo motivo, amparada, nesse caso, pelos princípios da LGPD e pela determinação legal de preservação dos dados naturais.

Certamente, conciliar a aplicação da LGPD aos negócios trabalhistas será o desafio de todo e qualquer cidadão. Pois, não somente os juristas, mas toda a sociedade marchará para tentar obter a cultura e a educação digitais.

É indubitável que a educação transforma e não seria diferente na era digital, onde tudo se transforma, como uma informação líquida ("o conceito de informação líquida está ancorado nos atributos dos meios líquidos, em razão da capacidade de alterar sua forma conforme seu recipiente"[195]).

Ressaltando os ensinamentos de Sêmola[196], corrobora-se que "a luta pela proteção das informações do negócio deve ser contínua, dinâmica e ágil". Afinal, "o evento de vazamento de informações é um dos danos de primeiro nível, dentre muitos outros, potencialmente produzidos pela ação bem-sucedida de uma ameaça que compromete diretamente a confidencialidade", e que pode restar por comprometer a integridade e a disponibilidade.

A evolução tecnológica vem assegurando novos meios de se combater o vazamento de dados; máquinas surgem quase que constantemente; pessoas trabalham e estudam para formar uma educação sólida e atualizada com o mundo atual, sendo que, a atuação em conjunto de ambas as legislações têm somente a crescer e preservar os ambientes laborais e de controle de dados.

Não obstante, faz-se necessário que cada empresa se adeque à realidade inerente ao controle de dados, desenvolvendo manual/guia de boas práticas inerentes ao processamento de dados para que, em caso de incidentes de segurança, os atos praticados sejam condizentes com a legislação e obstem um evento danoso irreparável.

Veja-se que a prática da proteção dos dados não é somente a formalização de contratos ou documentos que supostamente conferem a validação e cumprimento dos regramentos da

---

[195] PECK PINHEIRO, Patrícia. **Segurança digital**: Proteção de dados nas empresas. São Paulo: Atlas, 2021. p. 176.

[196] PECK PINHEIRO, Patrícia. **Segurança digital**: Proteção de dados nas empresas. São Paulo: Atlas, 2021. p. 77, 79.

legislação. Pelo contrário, faz-se necessária uma atuação ativa da empresa no que concerne a formulação de manuais de boas práticas, programas de compliance, treinamentos e efetivamente um modo de atuação capaz de educar os agentes, terceiros, empregados e responsáveis pelos dados no que concerne as políticas corretas que devem ser abordadas no dia a dia da empresa, seja no armazenamento, tratamento, transmissão ou exclusão de dados.

Com tais aspectos formalizados e de conhecimento do público necessário, as práticas inerentes aos incidentes de segurança serão analisados sob a ótica da legalidade da empresa e da responsabilidade objetiva do agente que tratou os dados irregularmente e ocasionou os danos à empresa e ao titular dos dados vazados, tratando-se, preliminarmente, de uma política preventiva para evitar qualquer ato ilícito inerente ao controle de dados.

Dessa forma, validada a relação empregatícia com a legislação de dados, aplicar a justa causa a determinado funcionário será medida correta quando ocorrer a transmissão indevida de dados naturais, pautando-se na responsabilidade objetiva da controladora de dados, ainda que sem a intenção de causar danos, atribuindo-se ao referido ato o caráter pedagógico e legal pelo cumprimento das regras legais.

REFERÊNCIAS

AGUIAR JUNIOR, Ruy Rosado (org.). **Jornada de Direito Civil, 3**. Brasília: CJF, 2005.

ALVES, Fabrício Mota. Da Fiscalização. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato (Coord.). **LGPD – Lei Geral de Proteção de Dados Comentada**. São Paulo: Revista dos Tribunais, 2019.

ARAS, Vladimir. Boate Kiss: a seleção dos jurados e o direito à proteção de dados pessoais. **Jota,** São Paulo, 04 jan. 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/boate-kiss-selecao-jurados-direito-protecao-dados-04012022. Acesso em: 04 jan. 2022.

BERNABÈ, Franco. **Liberdade vigiada**: Privacidade, segurança e mercado na rede. Rio de Janeiro: Sinergia, 2013.

BITTENCOURT, Vanessa; TORMIN, Camila. Responsabilidade civil no direito de família: aspectos relevantes da responsabilidade civil no direito de família. *In:* JUSBRASIL, [s.l.], 2015. Disponível em: https://vanbittencourt.jusbrasil.com.br/artigos/306634668/responsabilidade-civil-no-direito-de-familia Acesso em: 31 ago. 2018.

BLUM, Renato Opice. **Proteção de dados**: Desafios e soluções na adequação à Lei. Rio de Janeiro: Forense, 2021.

BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Claudia. **Proteção de dados pessoais no Brasil**: Uma nova visão a partir da Lei n.º 13.709/2018. Belo Horizonte: Fórum, 2019.

BRASIL. (Código Civil [2002]). **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 abr. 2022.

BRASIL. (Código Tributário Nacional [1966]). **Lei n.º 5.172, de 25 de outubro de 1966**. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Brasília, DF: Presidente da República, 1966. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm. Acesso em: 12 maio 2022.

BRASIL. (Constituição [1988]). **Constituição da República Federativa do Brasil**. Brasília, DF: Congresso Nacional, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 abr. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Incidentes de Segurança com dados pessoais e sua avaliação para fins de comunicação à ANPD**. Brasília, DF, 22 fev. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 28 set. 2022.

BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 12 abr. 2022.

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. Brasília, DF: Presidente da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 03 maio 2022.

BRASIL. **Lei nº 13.709, 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [Redação dada pela Lei 13.853, de 2019]. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 set. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 08 abr. 2022.

BRASIL. Tribunal Regional do Trabalho (2 Região). Primeira Turma. **Reclamatória Ordinária Trabalhista nº 1000612-09.2020.5.02.0043**. Relator Des. Daniel de Paula Guimarães. São Paulo, 22 de outubro de 2021. Disponível em: https://pje.trt2.jus.br/consultaprocessual/detalhe-processo/1000612-09.2020.5.02.0043/2#0359e14. Acesso em: 12 abr. 2022.

BRIGATTI, Fernanda. Uso do bafômetro viola proteção de dados, decide Justiça do Trabalho. **Folha de São Paulo,** São Paulo, 03 fev. 2022. Disponível em: https://www1.folha.uol.com.br/mercado/2022/02/uso-do-bafometro-viola-protecao-de-dados-decide-justica-do-trabalho.shtml?_mather=b8aa1a7a576cc75b&origin=folha. Acesso em: 04 fev. 2022.

CÂMARA, Marcelo Oliveira. **Responsabilidade civil**. Rio de Janeiro: SESES, 2018.

CARLOTO, Selma; GUERRA, Elaine. **Manual Prático de Adequação à LGPD com enfoque nas relações de trabalho**. São Paulo: LTr, 2021.

CASTRO, Dayane Marciano de Oliveira; MANCUSO, Gisele. Responsabilidade da Empresa frente à proteção dos dados do trabalhador no contexto da Lei Geral de Proteção de Dados no Brasil – LGPD. *In:* PERREGIL, Fernanda; CALCINI, Ricardo (org.). **LGPD e *Compliance* trabalhista**: os desafios atuais no Direito do Trabalho empresarial. Leme, SP: Mizuno, 2021.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014.

CAVEDON, Mauro Venturini. Pressupostos da responsabilidade civil no direito brasileiro. *In:* CONTEÚDO JURÍDICO, [s.l.], 1º dez. 2016. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/47878/pressupostos-da-responsabilidade-civil-no-direito-brasileiro. Acesso em: 30 ago. 2022.

COMITÉ restrito da CNIL impõe uma sanção financeira de 50 milhões de euros à Google LLC. *In:* EDPB – European Data Protection Board, França, 21 jan. 2019. Disponível em: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc. Acesso em: 14 maio 2022.

Constituição [1988]). **Constituição da República Federativa do Brasil**. Brasília, DF: Congresso Nacional, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 abr. 2022.

CORREIA, Henrique; BOLDRIN, Paulo Henrique Martinucci. Lei Geral de Proteção de Dados (LGPD) e o Direito do Trabalho. **Revista Síntese Trabalhista e Previdenciária**, São Paulo, v. 31, n. 377, p. 205-217, nov. 2020.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

CRESPO, Danilo Leme; RIBEIRO FILHO, Dalmo Ribeiro. A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da Lei Geral de Proteção de Dados Pessoais. **Revista de Direito Privado**, São Paulo, v. 20, n. 98, p. 161-186, mar./abr. 2019.

DELGADO, Mauricio Godinho. Curso de direito do trabalho. 17. ed. rev. ampl. São Paulo: LTr, 2018. 176 pg

DINIZ, Danielle Alheiros. A impossibilidade de responsabilização civil dos pais por abandono afetivo. *In:* JUS.COM, [s.l.], 24 jun. 2009. Disponível em: https://jus.com.br/artigos/12987/a-impossibilidade-de-responsabilizacao-civil-dos-pais-por-abandono-afetivo#. Acesso em: 31 ago. 2018.

DINIZ, Maria Helena. **Curso de Direito Civil brasileiro**: Responsabilidade civil. 22. ed. São Paulo: Saraiva, 2007. v. 7.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**: Responsabilidade Civil. 26. ed. São Paulo: Saraiva. 2012. v. 7.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Revista dos Tribunais, 2021.

DONEDA, Danilo; MENDES, Laura Schertei; CUEVA, Ricardo Villas Bôas. **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade**: contribuições para a implementação da LGPD. São Paulo: Revista dos Tribunais, 2020.

EUROPEAN UNION. **General Data Protection Regulation (GDPR)**. May 25, 2018. Disponível em: https://gdpr-info.eu/art-12-gdpr/. Acesso em: 12 abr. 2022.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de Direito Civil:** Responsabilidade Civil. 10. ed. São Paulo: Saraiva. 2012. v. 3.

JUSTEN FILHO, Marçal. **Curso de Direito Administrativo**. 12. ed. São Paulo: Revista dos Tribunais, 2016.

KUCHLER, Hannah. Punição britânica ao Facebook abre precedentes. **Valor,** São Paulo, 12 jul. 2018. Disponível em: https://valor.globo.com/empresas/noticia/2018/07/12/punicao-britanica-ao-facebook-abre-precedentes.ghtml. Acesso em: 12 maio 2022.

LIMA, Ana Paula Moraes Canto de Lima; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. **LGPD Lei Geral de Proteção de Dados**: sua empresa está pronta?. São Paulo: Literare Books International, 2020.

LIRA, Wlademir Paes de. Responsabilidade civil nas relações familiares: O estado da arte no Brasil. **Revista da Faculdade de Direito da ULP,** Porto, v. 6, n. 6, p. 168-209, fev. 2016. Disponível em: https://revistas.ulusofona.pt/index.php/rfdulp/article/view/5352. Acesso em: 31 ago. 2018.

MAIA, Daniel de Oliveira. As Hipóteses Autorizativas de Tratamento de Dados Pessoais nas Relações de Trabalho Sob a Ótica da LGPD e do GDPR. *In:* MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2021. *E-book* (não paginado).

MALDONADO, Viviane Nóbrega; BLUM, Renato (coord.). **Comentários ao GDPR**: Regulamento Geral de Proteção de Dados da União Europeia. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 201-202.

MARTINS, Ives Gandra da Silva. **Comentários ao Código Tributário Nacional**. São Paulo: Saraiva, 1998.

MARTINS, Sergio Pinto. **Direito Processual do Trabalho.** 41. ed. São Paulo: Saraiva Jur, 2019.

MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2021.

NASCIMENTO, Amauri Mascaro; NASCIMENTO, Sônia Mascaro; **Curso de Direito do Trabalho.** 29. ed. São Paulo: Saraiva, 2014. *E-book.*

NEGRÃO, Antônio Carlos. Economia digital, proteção de dados e competitividade. *In:* DONEDA, Danilo; MENDES, Laura Schertei; CUEVA, Ricardo Villas Bôas. **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade**: contribuições para a implementação da LGPD. São Paulo: Revista dos Tribunais, 2020.

NERY JUNIOR, Nelson. **Código Civil Comentado**. 14. ed. São Paulo: Revista dos Tribunais, 2022.

PALMA, Fernanda. Incidentes de segurança da informação: conceitos, exemplos e cases. *In:* PORTAL GSTI, 2014. Disponível em: https://www.portalgsti.com.br/2014/01/incidentes-de-

seguranca-da-informacao-conceito-exemplos-e-cases.html#:~:text=Segundo%20CERT.br%2C%20um%20incidente%20de%20seguran%C3%A7a%20pode%20ser,sob%20risco%20%C3%A9%20considerado%20um%20incidente%20de%20seguran%C3%A7a. Acesso em: 09 nov. 2020.

PECK PINHEIRO, Patrícia. **Segurança digital**: Proteção de dados nas empresas. São Paulo: Atlas, 2021.

PEREIRA, Caio Mário da Silva; TEPEDINO, Gustavo. **Responsabilidade civil**. 12. ed. Rio de Janeiro: Forense, 2018.

PERONGINI, Maria Fernanda Hosken. Efeitos da compliance na proteção de dados pessoais. *In:* MIGALHAS, São Paulo, 21 ago. 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI285967,21048-Efeitos+da+compliance+na+protecao+de+dados+pessoais. Acesso em: 13 jun. 2019.

PERREGIL, Fernanda; CALCINI, Ricardo (org.). **LGPD e *Compliance* trabalhista**: Os desafios atuais no Direito do Trabalho Empresarial. Leme, SP: Mizuno, 2021.

PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. *In:* MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (coord.). **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2021.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais comentários à Lei n. 13.709/2018 (LGPD)**. 3. ed. São Paulo: Saraiva Jur, 2021.

REIS, Beatriz de Felippe. A cultura de compliance em matéria de proteção de dados e sua adoção no âmbito laboral. **Revista de Direito do Trabalho e Seguridade Social**, São Paulo, v. 46, n. 214, p. 323-340, nov./dez. 2020.

RIBEIRO, Cinthya Imano Vicente. **Privacidade digital das instituições bancárias**. 2019. Dissertação (Mestrado em Direito Comercial) - Pontifícia Universidade Católica de São Paulo, São Paulo/SP, 2019. p. 71. Disponível em: https://tede2.pucsp.br/bitstream/handle/22990/2/Cinthya%20Imano%20Vicente%20Ribeiro.pdf. Acesso em: 04 maio 2022.

SANTOS, Camila Ferrão dos; SILVA, Jeniffer Gomes da; PADRÃO, Vinicius. Responsabilidade civil pelo tratamento de dados pessoais na Lei Geral de Proteção de Dados. **Revista Eletrônica da PGE RJ,** Rio de Janeiro, v. 4, n. 3, p. 1-31, set./dez. 2021. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/256. Acesso em: 11 fev. 2022.

SCHWARTZ, Matthew J. Marriott recebe multa de privacidade de US$ 24 milhões do GDPR por violação. *In:* BANK INFO SECURITY, [s.l.], 2 nov. 2020. Disponível em: https://www.bankinfosecurity.com/marriott-hit-24-million-gdpr-privacy-fine-over-breach-a-15288. Acesso em: 12 maio 2022.

SHEAD, Sam L. British Airways multada em £ 20 milhões por violação de dados que afetou mais de 400.000 clientes. *In:* CNBC, [s.l.], 16 out. 2020. Disponível em:

https://www.cnbc.com/2020/10/16/british-airways-fined-20-million-for-data-breach-by-ico.html. Acesso em: 12 maio 2022.

SISTEMA DE ADMINISTRAÇÃO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO (SISP). Tratamento de Incidentes. *In:* PORTAL SISP, 2019. Disponível em: https://www.gov.br/governodigital/pt-br/sisp. Acesso em: 09 nov. 2020.

SOUSA, Duarte Abrunhosa; GONÇALVES, Rui Coimbra. Da necessidade de conservação de dados pessoais dos trabalhadores no período pós-contratual. **Revista de Direito do Trabalho e Seguridade Social,** São Paulo, v. 212, v. 46, p. 119-145, jul./ago. 2020.

STOCO, Rui. **Tratado de responsabilidade civil**: doutrina e jurisprudência. 7. ed. São Paulo: Revista dos Tribunais, 2007.

STRICKLAND, Fernanda; ÍCARO, Pedro. Sanções da LGPD estão em vigor e instituições devem ficar atentas às novas normas. **Correio Braziliense,** Brasília, 1º ago. 2021. Disponível em: https://www.correiobraziliense.com.br/politica/2021/08/4941113-sancoes-da-lgpd-entram-em-vigor-e-instituicoes-devem-ficar-atentas-as-novas-normas.html. Acesso em: 11 fev. 2022.

TARTUCE, Flávio. **Direito Civil:** Direito das obrigações e responsabilidade civil. 8. ed. São Paulo: Método, 2013. v. 2.

TARTUCE, Flávio. **Direito Civil**: Lei de Introdução e parte geral. 9. ed. São Paulo: Método, 2016.

UGGERI, Karollyne. Compliance digital: os benefícios da implementação. *In:* MIGALHAS, São Paulo, 1º mar. 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI275349,51045Compliance+digital+os+beneficios+da+implementacao. Acesso em: 11 nov. 2020.

VAINZOF, Rony; LIMA, Caio César Carvalho; TAMER, Maurício Antonio. Compliance e LGPD: plano de adequação como ferramenta de mitigação de riscos legais. *In:* JOTA, [s.l.], 07 abr. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-adequacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019. Acesso em: 20 nov. 2020.

VENOSA, Sílvio de Salvo. **Direito Civil**: Responsabilidade civil. 5. ed. São Paulo: Atas, 2005. v. 4.

VENOSA, Silvio de Salvo. **Direito Civil:** Responsabilidade civil. 14. ed. São Paulo: Atlas, 2014. v. 4.

WITZEL, Ana Claudia Paes. Aspectos gerais da responsabilidade civil no direito de família. **Âmbito Jurídico**, Rio Grande, v. 16, n. 110, 2013. Disponível em: http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12958. Acesso em: 30 ago. 2018.