

## LGPD E COMPLIANCE: A EFETIVAÇÃO DOS DIREITOS DA PERSONALIDADE NAS RELAÇÕES DE EMPREGO

LGPD AND COMPLIANCE: THE EFFECTIVENESS OF PERSONALITY RIGHTS IN EMPLOYMENT RELATIONS

Leda Maria Messias da Silva\*  
Nadine Girardi Alves\*\*

**Como citar:** DA SILVA, Leda Maria Messias; ALVES, Nadine Girardi. LGPD e *compliance*: a efetivação dos direitos da personalidade nas relações de emprego. *Scientia Iuris*, Londrina, v. 27, n. 2, p. 91-111, jul. 2023. DOI: 10.5433/2178-8189.2023v27n2p91-111. ISSN: 2178-8189.

\*Pós-doutora em Direito do Trabalho (Universidade de Lisboa – Ulisboa/PT).

Doutora em Direito do Trabalho (Pontifícia Universidade Católica de São Paulo - PUC/SP).

Mestre em Direito do Trabalho (Pontifícia Universidade Católica de São Paulo - PUC/SP).

E-mail: lemead@uol.com.br

ORCID: <https://orcid.org/0000-0003-0109-569X>

\*\*Mestranda em Direitos da Personalidade (Centro Universitário de Maringá – UNICESUMAR/PR). Bolsista pelo Instituto Cesumar de Ciência, Tecnologia e Inovação (ICETI).

Graduada em Direito (Pontifícia Universidade Católica do Paraná – PUC/PR).

E-mail: [nadinegirardialves@hotmail.com](mailto:nadinegirardialves@hotmail.com)

ORCID: <http://orcid.org/0000-0002-6423-6413>

**Resumo:** A conformidade com a Lei Geral de Proteção de Dados passou a ser requisito indispensável para a prática empresarial, inclusive no que diz respeito ao tratamento de dados dos empregados. Assim, valendo-se do método científico hipotético-dedutivo, a pesquisa se propôs a analisar o instituto do compliance de dados, voltado para o âmbito empregatício, como meio de efetivar a cultura de proteção de dados e assegurar os direitos da personalidade dos empregados, enquanto titulares, bem como verificar os principais aspectos a serem considerados na gestão dos contratos de emprego, relacionados à legislação de dados. Constatou-se, por fim, que a adoção de programas de compliance importam no desenvolvimento de um ambiente laboral mais digno e regulado, uma vez que promovem a conscientização acerca da temática, auxiliando na construção da cultura de proteção de dados de dentro para fora das organizações.

**Palavras-chave:** compliance trabalhista; contrato de emprego; proteção de dados pessoais; direitos da personalidade.

**Abstract:** Compliance with the General Data Protection Law has become an indispensable requirement for business practice, including with regard to the processing of employee data. Thus, using the hypothetical-deductive scientific method, this research aimed to analyze the institute of data compliance, focused on the employment environment, as a means of effecting the culture of data protection and ensuring the personality rights of employees as holders, as well as verifying the main aspects to be considered in the management of employment contracts, related to data

legislation. Finally, it appears that the adoption of compliance programs matter in the development of a more dignified and regulated work environment, since they promote awareness of the theme, assisting in the construction of the culture of data protection from the inside out of organizations.

**Keywords:** labor compliance; employment contract; protection of personal data; personality rights.

## INTRODUÇÃO

Após a vigência da Lei Geral de Proteção de Dados (BRASIL, 2018), particularidades passaram a compor as relações de emprego, ainda que implicitamente, como reflexo da intensa incorporação tecnológica ao ambiente laborativo, havendo a necessidade de adequação das práticas empresariais aos moldes da nova legislação.

Além da conformidade com as normas legais, fez-se necessário o implemento da cultura de proteção de dados, inclusive no ambiente interno das empresas, organizações, instituições, e demais agentes de tratamento de dados, empregadoras, a fim de difundir o conhecimento acerca da importância de proteger dados pessoais, bem como garantir os direitos da personalidade aos titulares, empregados, no bojo das relações empregatícias, de modo que o *compliance* figura como importante forma de realizar os anseios normativos e socioeconômicos a este respeito.

Diante disso, utilizando-se da metodologia científica hipotético-dedutiva, a presente pesquisa visa analisar o *compliance* de dados, voltado para o emprego, como meio de efetivação da cultura de proteção de dados, bem como de prevenção contra lesões aos direitos da personalidade dos empregados. Além disso, objetiva verificar os principais aspectos a serem observados na elaboração e execução do contrato de emprego, relacionados à Lei Geral de Proteção de Dados (BRASIL, 2018).

Em um primeiro momento, a pesquisa contextualiza as relações de emprego frente ao desenvolvimento tecnológico, e a intensificação do tratamento de dados das pessoas empregadas. Após, busca conceituar o *compliance* de forma geral, apontando benefícios advindos da adoção de programas de *compliance* voltado para a proteção de dados. Em seguida, o estudo adentra na efetivação do *compliance* de dados, no âmbito empregatício, através da análise das principais condições que devem ser verificadas na gestão dos contratos de emprego, perpassando pela questão educativa em relação à Lei Geral de Proteção de Dados (BRASIL, 2018).

O conhecimento acerca da necessidade de proteger os direitos da personalidade das pessoas nas suas relações de emprego, bem como de proteger os dados pessoais, não é difundido socialmente, ao contrário da prática de tratamento de dados dos indivíduos, cujo potencial valorativo não comporta desigualdades, ou seja, todo e qualquer indivíduo, em todas as suas relações, tem seus dados pessoais tratados e valorados economicamente. Ocorre que as relações de emprego são essenciais para o desenvolvimento da personalidade, e do aspecto relacional da pessoa, de modo que a presente pesquisa se justifica pela importância que a adoção do *compliance* trabalhista, voltado para a Lei Geral de Proteção de Dados (BRASIL, 2018), apresenta para promoção da cultura de proteção de dados, criando um ambiente de trabalho mais digno, com a salvaguarda de direitos da personalidade, além dos benefícios para os próprios empregadores, no caso, sujeitos ativos da lei.

## 1 DADOS NO ÂMBITO LABORAL E *COMPLIANCE*

O protagonismo dos dados pessoais é inerente à sociedade da informação e pode ser verificado nas mais diversas relações, uma vez que a partir dos dados ocorre a extração de um conhecimento extremamente rentável e valioso para o desenvolvimento socioeconômico, sendo certo que a informação passou a ser considerada “o (novo) elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial” (BIONI, 2021, p. 3).

Da mesma forma, o universo do trabalho se transformou substancialmente pelo avanço das tecnologias, do emprego de inteligência artificial, da robótica, e da virtualização do trabalho, de modo que houve, como consequência, a intensificação do tratamento de dados pessoais inclusive nestas relações. Significa dizer que em todas as fases do contrato de trabalho ocorre, indubitavelmente, a operacionalização de dados pessoais, seja do empregado, ou do candidato, pretense funcionário de determinada empresa, empregadora.

Diante disso, a vigência da Lei Geral de Proteção de Dados, Lei nº 13.709 (BRASIL, 2018), reflete a importância da matéria para o ordenamento jurídico, criando diretrizes e balizas para a atuação empresarial, e demais sujeitos ativos da lei, no que tange a proteção de dados de pessoas naturais, incluídos dos seus trabalhadores, além de seus clientes, haja vista o tratamento de dados geralmente corresponder à alguma atividade da empresa, dependendo dele para seu funcionamento e crescimento mercadológico.

Ainda que o acesso aos dados pessoais e sensíveis de empregados ocorra em decorrência da atividade laborativa, considera-se que estas informações possibilitam a formação de um perfil comportamental e traduzem a personalidade do indivíduo, de modo que “não revelam somente aptidões profissionais, mas também questões ligadas à privacidade e à intimidade do trabalhador” (REIS, 2020, p. 2), podendo-se vislumbrar riscos de violações de direitos no ambiente laboral, em casos de ocorrência de incidentes de segurança<sup>1</sup> com dados de seus titulares, nesse caso, os empregados.

De início, destaca-se que a Lei Geral de Proteção de Dados é uma legislação principiológica, que visa o empoderamento do indivíduo, titular de dados, acerca de suas próprias informações, por meio da proteção de direitos fundamentais e direitos da personalidade, tendo como alguns de seus fundamentos a autodeterminação informativa, o livre desenvolvimento da personalidade, o respeito à privacidade, a inviolabilidade da intimidade, da imagem e da honra, entre outros (BRASIL, 2018).

Todavia, não se olvida que referida lei se justifica também por possibilitar que realmente ocorra o fluxo informacional, uma vez que se trata do principal ativo de desenvolvimento socioeconômico atual, como dito anteriormente, ou seja, foi necessária uma regulação destas

---

<sup>1</sup> Incidente de segurança corresponde a diversas situações de violação de segurança dos dados pessoais, tais como, o uso inadequado ou ilícito, a ocorrência de vazamento, exposição, acesso desautorizado, transferência irregular, exclusão, perda, destruição, alteração de dados etc., havendo a necessidade de comunicar à autoridade nacional e ao titular, em casos de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, conforme o art. 48, da LGPD (BRASIL, 2018).

operações para que possam ocorrer de forma regrada, salvaguardando a dignidade da pessoa, em última análise. Trata-se da dupla função atribuída à Lei Geral de Proteção de Dados (LGPD), conceituada pelo estudioso Bruno Bioni (2021, p. 108):

O principal vetor para alcançar tal objetivo é franquear ao cidadão *controle* sobre seus dados pessoais. Essa estratégia vai além do consentimento do titular dos dados, pelo qual ele autorizaria o seu uso. Tão importante quanto esse elemento volitivo é assegurar que o fluxo informacional atenda às suas legítimas expectativas e, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade.

Desta maneira, infere-se que para o crescimento econômico, seja em empresas de pequeno e médio porte, seja em grandes conglomerados de empresas, instituições, e outros setores que realizam o tratamento de dados pessoais, passou a ser necessária a adequação e a observância das normas da Lei Geral de Proteção de Dados (BRASIL, 2018), até mesmo como estímulo à competitividade negocial, e buscando evitar ou minimizar as sanções administrativas pelo seu descumprimento. Em outras palavras, referida lei não deve se tornar letra morta, fazendo-se imprescindível que os sujeitos ativos estejam em conformidade com os ditames da nova legislação.

Importante salientar, ainda, que a aplicabilidade da Lei Geral de Proteção de Dados (BRASIL, 2018) se estende a pessoas naturais ou jurídicas que realizem o tratamento de dados por qualquer meio, seja físico, ou digital, sendo certo que a adequação às normas independe do tipo ou do faturamento empresarial, podendo se tratar de grandes *startups*, ou até mesmo de micro e pequenas empresas, independente do formato de atuação.

Sendo assim, convém que os controladores e operadores de dados empenhem boas práticas em suas atividades, tais como “estabelecer parâmetros claros e procedimentos adequados, fundamentar a coleta e o tratamento nas hipóteses legais e colher e tratar os dados com transparência” (SANKIEVICZ; PINHEIRO, 2021, p. 524). Neste sentido, a estudiosa Patrícia Peck Pinheiro (2021, p. 45) aponta que:

A instituição de medidas e regras de boas práticas e de governança é essencial para que todos os requisitos necessários à proteção dos dados pessoais sejam efetivados. Conforme os artigos 40, 41, 42 e 43, as medidas de boas práticas envolvem um sistema amplo e complexo de relações e previsões como instituição de mecanismos de educação e prevenção em face da segurança da informação, atuação de organismos de certificação e treinamento de equipes junto à atuação das autoridades supervisoras.

A Lei Geral de Proteção de Dados (BRASIL, 2018) incentiva a tomada dessas práticas a fim de alavancar a implementação e cumprimento da própria lei e estabelecer uma mudança e adequação de comportamento, sendo esperado que os agentes de tratamento atuem visando a orientação e a prevenção, através da ideia de *privacy by design*, e não só visando evitar punições administrativas ou judiciárias, ou seja, que adotem uma postura proativa, ao invés de reativa, acerca da formação uma cultura de proteção de dados pessoais (CARVALHO; MATTIUZZO;

PONCE, 2021, p. 371).

Para tanto, apesar da implementação da lei e de uma cultura de proteção de dados depender da atuação, principalmente, fiscalizatória e sancionatória da Autoridade Nacional de Proteção de Dados (ANPD), o *compliance* de dados no âmbito laboral figura como um importante mecanismo, para atender aos anseios de efetivação da proteção de dados trazida pela lei, bem como de proteger os direitos da personalidade das pessoas empregadas, tal qual será analisado oportunamente.

### 1.1 *Compliance* voltado para a Lei Geral de Proteção de Dados

A adoção de mecanismos de boas práticas e governança visam dar efetividade à lei, criando ou adequando procedimentos internos, autorregulatórios, que auxiliem no controle e na identificação de comportamentos contrários às regras e normas instituídas, contribuindo para a minimização de riscos, e facilitando, assim, a elaboração de soluções para eventuais problemas que possam surgir em virtude de inadequações (CARVALHO; MATTIUZZO; PONCE, 2021, p. 374).

De acordo com o artigo 50, da LGPD (BRASIL, 2018), a governança e boas práticas podem ser desempenhadas em associações ou individualmente, sendo que a última modalidade diz respeito aos programas de *compliance*, ou nomeados programas de integridade e conformidade, sendo certo que referido mecanismo contém “um elevado grau de detalhamento sobre a estrutura de governança interna da entidade” por serem realizadas “sob medida – endereçando todas as atividades de tratamento de dados pessoais realizadas pelo controlador ou operador em questão” (CARVALHO; MATTIUZZO; PONCE, 2021, p. 375).

Partindo da etimologia da palavra, o termo *compliance* deriva do inglês “*to comply*”, e significa “agir de acordo com uma regra, instrução interna, um comando ou um pedido. Quer dizer que atender ao *compliance* significa estar em conformidade com leis e regulamentos externos e internos” (HISSA; GALAMBA, 2019, p. 120).

Isso porque, considera-se *compliance*, um conjunto de medidas e procedimentos que podem ser utilizados pelas empresas, de forma autorregulatória, visando atingir, também, uma “mudança de cultura corporativa e do clima organizacional” (SILVA; PINHEIRO; BOMFIM, 2021, p. 51), e não só buscando estar em conformidade com legislações e políticas internas, por imposição.

Importante destacar, sobretudo, que a incorporação do *compliance* nos mais diversos segmentos empresariais não é uma ferramenta inaugurada pelo advento da Lei Geral de Proteção de Dados (BRASIL, 2018), inserindo-se majoritariamente nas práticas corporativas a partir da Lei nº 12.846/2013 (BRASIL, 2013), nomeada como Lei Anticorrupção ou Lei da Empresa Limpa, “que trata da responsabilização civil e administrativa da pessoa jurídica pela prática de atos lesivos contra a administração pública e após os escândalos de corrupção política que enfrentamos nos últimos anos” (CARLOTO, 2020, p. 22).

Apesar disso, é possível, e até mesmo recomendável, que o *compliance* seja adotado para as diferentes finalidades e demandas organizacionais, conforme Fabrício Lima Silva, Iuri Pinheiro

e Vólia Bomfim (2021, p. 55) esclarecem:

[...] os programas de compliance não devem se restringir ao combate à corrupção. Tais programas, para manterem lógica, consistência e coerência, devem versar sobre todas as esferas da empresa, envolvendo questões fiscais, contábeis, trabalhistas, financeiras, ambientais, jurídicas, previdenciárias, éticas, dentre outras.

Sendo assim, ambas as legislações possuem incentivos à prática de *compliance*, além de possuírem diversas semelhanças, dentre as quais se podem mencionar: a necessidade de capacitação de colaboradores, o monitoramento e aperfeiçoamento/revisão das normas instituídas, a criação de uma figura específica para intermediar a relação (o *Data Protection Officer*, no caso da LGPD, e o *Chief Compliance Officer*, no caso da Lei Anticorrupção), bem como estimulam a prática de mecanismos de *compliance* por meio da atenuação de sanções, entre outras similitudes (HISSA; GALEMBA, 2019, p. 124-126).

Indubitavelmente, a incorporação de um sistema de *compliance*, ou ainda a adequação de mecanismos já existentes para a conformidade com a Lei Geral de Proteção de Dados (BRASIL, 2018), bem como com a Lei Anticorrupção (BRASIL, 2013), promovem uma modificação nas gestões corporativas e nos modelos éticos das organizações, passando a ser inserida “na rotina das atividades empresariais para o crescimento sustentável e atualmente é indispensável reconhecer todos os esforços de compliance nas empresas” (CARLOTO, 2020, p. 24), seja para fruir de benefícios, seja para salvaguardar os direitos dos titulares de dados, em especial, dos empregados e demais pessoas trabalhadoras das empresas.

Portanto, a adoção de um programa de *compliance* relacionado à Lei Geral de Proteção de Dados representa um importante mecanismo interno para que a empresa realize o tratamento de dados de acordo com as perspectivas legais, ao passo que viabiliza que os empregadores, enquanto controladores e/ou operadores de dados, se mantenham em conformidade com os princípios e normas da lei, e exercitem as boas práticas e a governança.

Além disso, trata-se de aderir a práticas que estimulam o implemento de uma cultura consciente de proteção de dados, de privacidade, e garantia dos demais direitos relacionados, por vias de regramentos organizacionais que estejam em conformidade com as diretrizes dispostas na Lei Geral de Proteção de Dados (BRASIL, 2018), incluídos os direitos dos empregados.

## 1.2 BENEFÍCIOS DA ADOÇÃO DO *COMPLIANCE* RELACIONADO À LEI GERAL DE PROTEÇÃO DE DADOS

Com efeito, desenvolver um programa de *compliance*, para regular a atuação interna da empresa, no que tange à proteção de dados, inclusive de seus próprios colaboradores, importa em fatores positivos e vantajosos para estes agentes de tratamento, que muitas vezes dependem da operacionalização de informações pessoais para o exercício de suas atividades, e que, por sua vez, podem sofrer consequências indesejadas em caso de infração à lei:

Uma das principais vantagens de implementação de programa de compliance é a

viabilização da existência de mecanismos para a rápida identificação de violações à lei, com a possibilidade de pronta resposta pela organização, evitando-se que condutas lesivas sejam perpetuadas e que os prejuízos assumam proporções maiores. A conscientização promovida pelos programas de compliance tende a evitar ou a diminuir os riscos de que práticas indesejáveis venham ocorrer. Além disso, a adoção de programas de governança corporativa e compliance tem um grande impacto no fortalecimento da imagem e reputação da empresa, que passa a demonstrar maior credibilidade e segurança, agregando valor ao negócio (SILVA; PINHEIRO; BOMFIM, 2021, p. 60).

Nesse ponto, ressalta-se que, na atualidade, é crescente a preocupação das empresas com suas reputações e imagem, até pela identificação que os consumidores buscam ao adquirir um produto ou um serviço, sendo comuns as avaliações em aplicativos e sítios eletrônicos. Além disso, as redes sociais se destacam como importantes “portas de entrada” para muitos negócios, e são essenciais para a captação e fidelização de público e, até mesmo, funcionam como canal de divulgação de processos seletivos de recrutamento e contratação.

Embora todas essas estratégias implementadas pelo avanço das tecnologias da informação e comunicação sejam favoráveis à atividade empresarial, é fato que as empresas e *e-commerce* estão em maior visibilidade do que há tempos, de modo que a ocorrência de uma situação de vazamento de dados, ou qualquer outro tipo de incidente de segurança representa riscos potenciais à sua reputação e à atração de consumidores, parceiros, investidores etc.

Ademais, além de possíveis responsabilizações judiciais, há que se mencionar as sanções administrativas que podem ser aplicadas em caso de infração às normas legais, as quais passaram a vigorar desde primeiro de agosto do ano de 2021 e podem acarretar prejuízos financeiros de expressiva monta, posto que vão desde advertência, com prazo para tomada de medidas corretivas à multa no valor de até 2% do faturamento da empresa, limitada a R\$ 50.000.000,00, por infração.

Em vista disso, programas de *compliance* se mostram fundamentais para a atividade empresarial, uma vez que são eficazes para prevenir e conter danos que possam ser causados aos titulares de dados, empregados ou consumidores, em situações como a exemplificada, sem que se mencione, ainda, a publicização que pode ser imposta, levando a empresa a enfrentar prejuízos em múltiplos aspectos, inclusive de cunho reputacional.

Portanto, adotar o *compliance* como mecanismo de segurança no tratamento de dados pessoais importa em uma vantagem e em um diferencial competitivo que uma empresa pode possuir em relação à outra, eis que há a valorização pela credibilidade com consumidores, além de ser importante para a ampliação e manutenção da atividade em compasso com mercados internacionais, e demais fornecedores e parceiros comerciais, em âmbito nacional.

Ainda, insta salientar que a utilização reiterada de boas práticas e governança, tais como o *compliance*, são alguns dos critérios considerados para a aplicação de punições, após processo administrativo em que seja assegurada a ampla defesa, funcionando como “atenuante para aplicação da pena” (HISSA, GALAMBA, 2019, p. 124), conforme dispõe os incisos VIII e IX, do parágrafo 1º, do artigo 52, da Lei Geral de Proteção de Dados:

Art. 52 [...] § 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; [...] (BRASIL, 2018).

Em suma, além da conformidade com os ditames legais, os programas de *compliance* demonstram ser eficientes para a prevenção e identificação de riscos e inadequações que possam ocorrer, possibilitando a criação mais eficiente de soluções, ou a minimização de eventuais danos, bem como a redução de custos para as empresas, empregadoras.

Além dos benefícios verificados, destaca-se, sobretudo, que a adoção do *compliance* contribui para alavancar o desenvolvimento da cultura de proteção de dados nos ambientes laborativos, por meio de ferramentas de conscientização, como palestras, treinamentos e cursos promovidos para o pessoal interno. Isso porque, o conhecimento acerca da importância de proteger dados pessoais, e seu valor social e econômico, não é difundida igualmente entre os indivíduos que compõe a sociedade, dificultando o entendimento das pessoas sobre os seus direitos e os riscos aos quais estão expostas, inclusive nas relações de emprego, tornando essencial que o empregador, agente de tratamento de dados, promova, através do *compliance*, ações educativas e conscientizadoras sobre a temática.

Conclui-se, por fim, que os programas de *compliance* voltados para a LGPD são essenciais para o *enforcement* da legislação, bem como para a implementação da cultura de proteção de dados e privacidade, promovendo a conscientização e incorporação das noções trazidas pela Lei Geral de Proteção de Dados em favor das pessoas naturais, tanto empregados e colaboradores, quanto demais titulares de dados.

## 2 COMPLIANCE TRABALHISTA E O CONTRATO DE EMPREGO

O cenário atual, de supervalorização das informações pessoais e de avanço tecnológico, fez emergir inúmeros debates sobre a necessidade de proteção de dados pessoais e da autodeterminação informativa, para além da proteção da privacidade e da intimidade.

Evidencia-se, portanto, a ocorrência de significativa mudança de percepção que os indivíduos passaram a ter acerca da disponibilização de seus atributos de personalidade em meio digitais, bem como nas mais diversas relações sociais. Contudo, não se olvida que a conscientização social acerca do tema é muito singela em comparação ao conhecimento altamente rentável que pode ser extraído do tratamento de dados pessoais, como apontado anteriormente. Segundo ensinam estudiosos:

[...] a LGPD representa a consolidação de relevante paradigma: atribuir a titularidade dos dados à pessoa natural a eles referente, conferindo-lhe extensa miríade de direitos para empreender efetivo controle sobre as suas informações. A LGPD implica novo marco regulatório – a ponto de se estruturar agência reguladora própria, a ANPD. Apesar da existência de normas anteriores que contemplavam perspectiva similar, a prática em matéria de proteção de dados pessoais no Brasil ainda é muito distante dos comandos da nova lei (FRAZÃO; OLIVA; ABILIO, 2019, p. 693-694).

Diante disso, revela-se essencial a construção de uma cultura de proteção de dados, com o progresso das bases principiológicas e normativas trazidas pela Lei Geral de Proteção de Dados (BRASIL, 2018). Vislumbra-se, então, a necessidade de difundir ainda mais as questões atinentes ao tratamento de dados pessoais e sensíveis, em especial, relacionadas ao tratamento havido no bojo das relações laborais. Isso porque, as relações de trabalho, de forma geral, são permeadas de operações envolvendo dados pessoais, tais como a coleta, acesso, classificação, armazenamento, processamento, transferência de dados das pessoas trabalhadoras, enquanto que, de forma específica, a relação de emprego, apresenta particularidades ainda mais contundentes a este respeito, seja pela necessidade de alterações contratuais, seja pela subordinação do empregado e o exercício do poder diretivo dos empregadores, possibilitando o monitoramento e a fiscalização das atividades desempenhadas no ambiente laboral.

Fato é que a concretização de uma cultura de proteção de dados pessoais, inclusive no âmbito empregatício, precisa ser edificada “de dentro para fora”, com a incorporação deste viés à identidade de organizações e ambientes corporativos.

A vigência da Lei Geral de Proteção de Dados (BRASIL, 2018) representa uma diretriz geral de comportamento, sendo certo que a efetiva realização e valorização da proteção de dados depende da atuação interna das corporações, empresas, instituições, e demais sujeitos ativos do tratamento de dados, por meio da elaboração de programas de *compliance*, que por sua vez “podem contribuir para o estabelecimento de critérios adequados à cada hipótese, para além de traduzir os preceitos legais em ações concretas a serem tomadas pelos agentes econômicos” (FRAZÃO; OLIVA; ABILIO, 2019, p. 697).

Ou seja, muito mais efetiva a existência de uma ferramenta de controle interna que incentive práticas de respeito à esta proteção, com a conscientização dos titulares, empregados, acerca da defesa de seus direitos, e reforce os ditames legais.

Em outras palavras, as relações estabelecidas entre os empregadores, considerados controladores e/ou operadores de dados, e os empregados, titulares de dados, precisam ser reguladas de forma específica, de modo que um *compliance* trabalhista eficiente depende de um projeto que considere as especificidades e a natureza dos negócios desenvolvidos por cada entidade empregadora, bem como pela necessidade de tratamento de dados, caso a caso.

De todo modo, a adoção de um *compliance* trabalhista, voltado para a proteção de dados pessoais depende da inserção das boas práticas à identidade da organização, para que a vivência em determinado ambiente de trabalho seja voltada para o respeito aos padrões éticos de

comportamento estabelecidos, havendo a conscientização dos empregados, em todos os níveis hierárquicos, para a incorporação desses valores aos ideais corporativos.

Diante disso, é fundamental que os programas de *compliance* sejam executados efetivamente, e que não sejam somente controles internos e documentos inutilizados, sem a concreta prática corporativa, cuja conduta pode gerar prejuízos e responsabilização às organizações, além de gerar eventuais danos aos empregados e titulares de dados. Ou seja, urge que as empresas atuem com coerência entre a vivência prática e os regramentos internos.

Estudiosos nomeiam referido descompasso como “*bluwashing*”, que se caracterizaria pelos casos em empresas atuam por meio de “‘compliance de fachada’ ou ‘compliance de papel’ [...] apresentam-se como observadoras da legislação trabalhista e socialmente responsáveis, mas, na realidade, descumprem reiteradamente os preceitos que dizem observar” (SILVA; PINHEIRO; BOMFIM, 2021, p. 51).

De um lado, há que se considerar que não só voltado para a proteção de dados, o *compliance* trabalhista demonstra ser indispensável para as práticas empresariais atualmente, uma vez que representa importante mecanismo executivo de legislações da seara do trabalho, como pontuam Fabrício Lima Silva, Iuri Pinheiro e Vólia Bomfim (2021, p. 79, grifo dos autores):

O compliance trabalhista é uma ferramenta essencial para prevenção e gestão de riscos na área trabalhista, cuidando de garantir o cumprimento de normas trabalhistas (**função de cumprimento**), evitando que os riscos previstos ocorram (**função de prevenção**) e estimulando a adoção de boas práticas destinadas à valorização do capital humanos das empresas (**função de excelência laboral**) [...] com a adoção de medidas de detecção, prevenção e correção de erros, combater práticas que possam violar a legislação e elevar índices de satisfação com o clima organizacional da empresa, com reflexos positivos em seus resultados.

Ainda, a adoção de um programa de *compliance* trabalhista resulta em benefícios às empresas e instituições empregadoras, uma vez que contribuem para “reduzir a judicialização entre empregado e empregador, além de evitar multas e outras indenizações, manter a ética, a integridade, a idoneidade, a transparência da empresa” (CARLOTO, 2020, p. 25).

De fato, a prevenção e a redução de passivo com ações trabalhistas individuais e coletivas, ou ainda com punições administrativas, pelo descumprimento da legislação do trabalho ou da própria Lei Geral de Proteção de Dados é fator almejado pelas organizações, sendo importante para a formação de boa reputação empresarial, além de auxiliar na gestão de pessoas, e proteger os direitos dos empregados.

Por sua vez, o estabelecimento de uma cultura de proteção de dados, inserindo-a nos modelos éticos das empresas, por meio de adequações de comportamento e do cumprimento voluntário das normas de controle internos, em compasso com legislações trabalhistas e, inclusive, com a Lei Geral de Proteção de Dados (BRASIL, 2018), tem o condão de prevenir a ocorrência de lesões aos direitos da personalidade dos empregados, relacionados à privacidade, intimidade, autodeterminação informativa, livre desenvolvimento da personalidade, entre outros, além de

garantir melhores condições dos empregados exercerem suas atividades laborativas, por meio da criação de um meio ambiente de trabalho digno.

Acerca da valorização do trabalho humano e da garantia aos direitos da personalidade dos trabalhadores e, conseqüentemente, dos empregados, as estudiosas Leda Maria Messias da Silva, Ana Paula Baptista Marques e Maria Aparecida Alkimim (2021, p. 75) ensinam que:

[...] deve-se dar atenção à dimensão humana do trabalho, relacionando-o à dignidade e à própria subsistência da pessoa, tal como à dimensão patrimonial do trabalho, cuja finalidade é a retribuição pecuniária. Pelo abrigo dado ao trabalho pelo ordenamento jurídico brasileiro, regulado pela dignidade da pessoa humana e pelo valor social do trabalho, ressaltam-se tais direitos como garantidores de mínimo existencial necessário a uma vida digna, pelos valores constitucionalmente assegurados, que versam sobre a necessária proteção do trabalhador e seus direitos da personalidade.

Assim, destaca-se que o *compliance* trabalhista, voltado para a proteção de dados, com o emprego de algumas ferramentas próprias, são capazes de proteger os empregados de situações inadequadas no ambiente laborativo, posto que o *compliance* favorece a prevenção, a detecção e a punição dos responsáveis por condutas contrárias às normas e regulações internas, que possam levar a lesões aos direitos fundamentais e da personalidade dos empregados.

Selma Carlotto (2020, p. 32, grifo do autor) indica, em suma, que as principais ferramentas que podem ser aderidas são:

Os programas de treinamento e palestras, consultivo, regulamentos empresariais trabalhistas, os códigos de ética e de conduta, política de advertências, os canais de denúncia, registros do cumprimento da lei, os relatórios e avaliações de desempenho [...] o relatório de impacto à proteção de dados pessoais.

Dessa forma, a inserção de referidos mecanismos no ambiente laboral, por meio do *compliance* trabalhista, remodela os modelos éticos empresariais para uma cultura de proteção de dados, com respeito aos valores sociais do trabalho, efetivando as garantias constitucionais e protegendo os direitos da personalidade dos empregados, sendo exigida, ainda, a observância dos preceitos legais da Lei Geral de Proteção de Dados na gestão dos contratos de empregos, cujos principais aspectos serão abordados adiante.

## **2.1 PRINCIPAIS ASPECTOS DA GESTÃO DO CONTRATO DE EMPREGO FRENTE À LEI GERAL DE PROTEÇÃO DE DADOS**

No que tange ao contrato de emprego, indubitavelmente os empregadores devem tomar precauções com o cumprimento dos preceitos advindos da Lei Geral de Proteção de Dados (BRASIL, 2018), considerando a transversalidade legislativa, que engloba qualquer atividade de tratamento de dados, exceto aquelas realizadas para fins exclusivamente particulares e não econômicos, embora a lei não disponha expressamente sobre sua aplicação ao contexto do trabalho.

Fato é que o tratamento de dados ocorre constantemente nessas relações, como dito alhures, sendo certo que o empregador deve empenhar o *compliance* de dados, e a adequação aos ditames legais, também voltado aos contratos de emprego com seus funcionários, ao longo de toda a relação empregatícia, ou seja, desde o momento anterior à contratação, durante todo o lapso da vigência contratual e, até mesmo, após a rescisão de referido contrato.

É crucial, então, enfatizar o quão importante são os cuidados que devem ser feitos nesse momento que, de envolvimento tão basilar, pode ser visto equivocadamente como menos sujeito à aplicação da Lei de dados ou das consequências de sua não observância (MARCOLINO; SILVEIRA, 2020, p. 213).

A operacionalização de dados pessoais, tais como coleta e avaliação, ocorre antes mesmo da relação empregatícia ter início, quando dos processos seletivos de contratação e recrutamento, análise de currículos etc., encontrando respaldo legal nas disposições do artigo 7º, inciso V, da Lei Geral de proteção de dados, uma vez que é permitido o tratamento de dados “quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato” (BRASIL, 2018).

Ainda assim, mesmo que não haja uma relação jurídica formalizada, os princípios e normas legais devem ser observados, sendo imprescindível o expresso consentimento do candidato autorizando o tratamento de seus dados, nos limites da finalidade, necessidade e adequação que devem lhe ser informados, de forma precisa e clara, em observância ao princípio da transparência, conforme dispõe o artigo 6º, da Lei Geral de Proteção de Dados (BRASIL, 2018).

No momento pré-contratual, exige-se cautelas também relacionadas ao uso de técnicas automatizadas, algoritmos e operações tecnológicas nos processos seletivos de contratação. Embora muito comuns na atualidade, o emprego inadequado de mecanismos digitais pode reforçar práticas discriminatórias e inadequadas, tendo em vista que “informações equivocadas obtidas a partir de bancos de dados podem deturpar o processo de escolha e privar candidatos aptos de boas oportunidades” (SANKIEVICZ; PINHEIRO, 2021, p. 514).

Além disso, o uso de referidas técnicas deve ser comunicado de forma clara, até mesmo para que o titular de dados possa exercer seu direito de revisão, disposto pela LGPD<sup>2</sup>, e visando assegurar o princípio da não discriminação, sendo expressamente vedada pela legislação de dados e pela Lei nº 9.029/1995 (BRASIL, 1995), e contrárias à boa-fé esperada neste tipo de relações.

No que diz respeito ao período de vigência do contrato de emprego, também devem ser observadas nuances normativas em relação ao tratamento de dados dos empregados, especialmente no que tange à elaboração contratual, bem como ao dia a dia do empregado e seu relacionamento com o ambiente de trabalho, posto que ocorrem operações de dados, seja para o acesso ao estabelecimento, seja para o controle de jornada e monitoração das atividades laborais, servindo

---

2 De acordo com o artigo 20, da LGPD: “Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade” (BRASIL, 2018).

tanto para empregos realizados presencial ou no formato remoto, seja para conferir licenças e atestados de saúde, entre outras situações decorrentes do emprego.

Precipuamente, vislumbra-se a necessidade implícita de adequação dos contratos de emprego que já se encontravam em execução antes da vigência da Lei Geral de Proteção de dados, sendo certo que “é válida e preventiva a reanálise dos documentos e contratos de relações de trabalho existentes, eis que a falta de cautela pode ensejar problemas vindouros” (MARCOLINO; SILVEIRA, 2020, p. 216), assim como dos contratos a serem firmados a partir disso.

É importante ressaltar que o direito do trabalho é, ainda, muito deficitário no que se refere à proteção de dados das pessoas que trabalham, frente aos seus empregadores e tomadores de serviços. Isso porque, as modificações legislativas atuais pouco vêm albergando proteção e garantias aos trabalhadores, sendo omissa, a Lei Geral de Proteção de Dados (BRASIL, 2018), neste ponto específico. Sendo assim, a tutela dos direitos dos trabalhadores, em especial, em relação à proteção de dados e da privacidade depende, muito embora, de interpretações feitas pelos estudiosos, operadores do direito, dos tribunais e da vivência prática das relações laborativas. De toda forma, convém que os empregadores se atentem aos ditames da Lei Geral de Proteção de Dados (BRASIL, 2018) na elaboração e execução dos contratos de emprego.

Assim, as principais particularidades que podem ser observadas na gestão do contrato de emprego se referem às cláusulas contratuais e à informação que deve constar das mesmas, sendo pacífico entre os estudiosos que as cláusulas relacionadas ao tratamento de dados dos empregados devem ser destacadas das demais, sendo recomendável que as assinaturas se deem em local específico para tanto (SILVA; PINHEIRO; BOMFIM, 2021, p. 751).

Ainda, fundamental que a principiologia da lei seja inserida em referidos documentos, antecipando a adequação de comportamentos práticos esperados tanto do empregador, quanto dos empregados, com o cumprimento dos princípios da finalidade, da transparência, da necessidade e da adequação.

Em outras palavras, o tratamento de dados dos empregados pode ocorrer de acordo com a necessidade das informações para a prestação laborativa, de forma informada, respeitando a finalidade e o legítimo interesse dos empregadores, sempre resguardando os direitos dos titulares empregados, os quais também devem ser comunicados, possibilitando o direito de revisão mencionado anteriormente.

Dentre as obrigações e responsabilidades dos agentes de tratamento de dados, empregadores, em relação aos empregados, pode-se vislumbrar o dever de informar a finalidade e as hipóteses legais que amparam o tratamento de dados, o qual ocorrerá por qual lapso temporal e em qual extensão, além de comunicar quais são os destinatários e quem é o encarregado.

Outro relevante aspecto da gestão do contrato de emprego frente à Lei Geral de Proteção de Dados (BRASIL, 2018) e a adoção de programas de *compliance*, reside no consentimento e na disparidade entre as partes desta relação, sendo certa a hipossuficiência do empregado em relação ao empregador, mesmo nos casos de empregados chamados pela Lei 13.467/17 (BRASIL, 2017), “hipersuficientes”. Estes seriam os que auferem duas vezes o maior benefício da previdência

e possuem diploma de curso superior, o que, certamente, com tantos encargos sobre o salário, possuem uma relevante dependência econômica, pelo que, nada possuem de “hipersuficientes”<sup>3</sup>.

Uma vez que a lei abarca diversas situações que justificam o tratamento de dados, apontase o consentimento e o legítimo interesse como bases legais que merecem cautela, uma vez que podem ser contestados com maior facilidade, justamente em razão da mencionada disparidade entre as partes, seja pela necessidade econômica que o emprego representa para a subsistência da pessoa, seja pela subordinação, diante do exercício do poder diretivo, do poder fiscalizatório e disciplinar por parte do empregador, seja pelo maior conhecimento técnico sobre a implementação tecnológica no ambiente empregatício.

A pessoa empregada precisa acatar e se submeter às imposições empregatícias, sem grandes margens para debates e ponderações, até mesmo como condição para a manutenção do emprego, portanto, em se tratando de uso abusivo ou irregular de dados dos empregados, o consentimento pode não ter sido externado de forma livre, inequívoca e informada, como determina a LGPD<sup>4</sup>, enquanto o tratamento de dados pode extrapolar os limites da finalidade que justifique o legítimo interesse do empregador, acarretando lesões aos direitos da personalidade e liberdades dos empregados, situações também desfavoráveis ao empregador.

Embora o tratamento de dados dos empregados em decorrência de obrigatoriedade legal ou regulatória, pelo controlador, dispense o consentimento, nos termos do artigo 7º, inciso II, da Lei Geral de Proteção de Dados (BRASIL, 2018), o empregador não fica desobrigado da observância das demais imposições legais, conforme expressamente dispõe o parágrafo 6º do mesmo artigo<sup>5</sup>, sendo “necessário, portanto, cuidados com o expresse consentimento do trabalhador, bem assim com suas finalidades, mesmos nos casos que não demandam consentimento, pois as demais proteções continuam valendo” (MARCOLINO; SILVEIRA, 2020, p. 216).

Além disso, é importante destacar que a legislação de dados veda a obtenção de consentimento de forma generalista, de modo que as finalidades devem ser determinadas caso a caso, e indicadas de forma específica para que sua externalização seja válida, pelo que se justifica a importância de destacar, no contrato de emprego, as cláusulas relacionadas ao tratamento de dados, ou por meio aditivo ou, até mesmo, por documento a parte. Portanto, de acordo com Fabrício Lima Silva, Iuri Pinheiro e Vólia Bomfim (2021, p. 751):

[...] quando estivermos diante da pretensão de tratamento de diversos dados, deve ser assegurado ao titular dos dados a indicação pontual e específica de quais dados ele deseja consentir e para qual finalidade específica, em detrimento da prática de mercado

3 De acordo com o parágrafo único do artigo 444, da CLT: “A livre estipulação a que se refere o caput deste artigo aplica-se às hipóteses previstas no art. 611-A desta Consolidação, com a mesma eficácia legal e preponderância sobre os instrumentos coletivos, no caso de empregado portador de diploma de nível superior e que perceba salário mensal igual ou superior a duas vezes o limite máximo dos benefícios do Regime Geral de Previdência Social” (BRASIL, 1943).

4 Segundo o artigo 5º, inciso XII, da Lei Geral de Proteção de Dados, o consentimento pode ser considerado como a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;” (BRASIL, 2018).

5 De acordo com o artigo 7º, § 6º, da Lei Geral de Proteção de Dados: “A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular” (BRASIL, 2018).

materializada pelo “all or nothing”.

Diante da hipossuficiência e da facilidade de invalidação do consentimento, revela-se viável que o tratamento de dados dos empregados, realizado no âmbito da relação empregatícia, tenha amparo em mais de uma hipótese legal, até mesmo para que se efetive o cumprimento das bases principiológicas da legislação. Aqui, novamente, vale ressaltar que o desenvolvimento da cultura de proteção de dados no ambiente de trabalho é fundamental para que sua prática seja consciente por parte de ambos os sujeitos da relação empregatícia e de tratamento de dados, iniciando-se pela transparência na elaboração dos contratos de emprego.

Outra questão relacionada ao consentimento para o tratamento de dados durante o exercício das atividades empregatícias pode ser levantada, em especial, no que se refere à utilização de dados sensíveis, como dados biométricos, para fins de identificar os empregados, bem como para controlar jornadas, intervalos, afastamentos e licenças médicas. Isso porque, o tratamento de dados sensíveis possui alto grau de intromissão na vida privada da pessoa empregada, potencializando riscos aos seus direitos da personalidade, liberdades e garantias fundamentais, asseguradas constitucionalmente.

Os estudiosos Alexandre Sankievicz e Guilherme Pereira Pinheiro (2021, p. 517) sintetizam ilustremente as razões que inviabilizam o emprego do consentimento como única hipótese legitimadora para o tratamento de dados sensíveis, da seguinte forma:

[...] a mera obtenção desse consentimento não é algo a garantir, por si só, a segurança jurídica ao tratamento pelo empregador. Primeiro, porque o consentimento pode ser retirado a qualquer momento pelo empregado sem que, desse fato, possa haver qualquer prejuízo a outros direitos. Segundo, porque, tendo em vista o desequilíbrio de poder existente nas relações de trabalho, sempre se poderá questionar judicialmente a livre manifestação de vontade do subordinado no momento do consentimento para o fornecimento de dados biométricos.

Não se olvida que mesmo após a rescisão do contrato de emprego cabe a observância das diretrizes trazidas pela Lei Geral de Proteção de Dados (BRASIL, 2018), uma vez que o encerramento contratual não representa, necessariamente, o término do tratamento de dados.

A obrigatoriedade de retenção de alguns documentos para fins fiscalizatórios, ou ainda para produção probatória em pretensões trabalhistas ou previdenciárias, encontra amparo no artigo 16, inciso I, da Lei Geral de Proteção de Dados, o qual dispõe sobre a possibilidade de conservação de dados pessoais para o “cumprimento de obrigação legal ou regulatória pelo controlador” (BRASIL, 2018).

No entanto, o armazenamento, a transferência ou qualquer operação de tratamento realizada no período pós-contratual pode, eventualmente, gerar lesões aos direitos dos titulares de dados, de modo que se mantém vedada a utilização abusiva, inadequada e irregular de informações pessoais, ou ainda a “divulgação de ‘listas negras’, sejam aquelas que apontam empregados que entraram com ações trabalhistas ou as relativas àqueles que possuem atuação sindical

significativa” (BELLINETTI; SOUZA, 2019, p. 233), até mesmo por contrariar os modelos éticos organizacionais e a cultura de proteção de dados a ser implementada no âmbito das relações de emprego. Acrescente-se a isso, especialmente em relação à atuação sindical, quando motive a rescisão sem justa causa do contrato de emprego, o direito à reintegração do empregado, em face à dispensa arbitrária e aos danos morais decorrentes da lesão aos direitos da personalidade do empregado.

A adoção de medidas de *compliance* trabalhista voltado para a proteção de dados, com influência na gestão dos contratos de emprego revela-se, portanto, fundamental para a criação da cultura de proteção de dados nos ambientes laborativos, uma vez que, além de manter os agentes de tratamento em conformidade com a lei, promovem a educação e conscientização acerca da necessidade de proteger dados, conhecimento pouco difundido, nas mais diversas camadas sociais, embora o intenso tratamento de dados ocorra na sociedade contemporânea atingindo sobremaneira todos os indivíduos.

O *compliance*, por fim, representa importante mecanismo de orientação e adequação de comportamentos nos ambientes organizacionais, representando, principalmente, ferramenta de defesa dos direitos da personalidade por meio da conscientização individual a respeito das garantias legais e normativas advindas da Lei geral de Proteção de Dados, e pouco ensinadas e incorporadas ao ambiente empregatício.

## CONCLUSÃO

O avanço tecnológico provocou modificações significantes nas relações de emprego, proporcionando uma intensificação da coleta e do tratamento de dados das pessoas empregadas, assim como ocorreu nas demais relações sociais da atualidade.

Pela essencialidade dos dados para o desenvolvimento socioeconômico, a Lei Geral de Proteção de Dados figura, no ordenamento jurídico brasileiro, como um marco legislativo em busca do empoderamento dos titulares de dados, visando proteger seus direitos, ao passo que proporciona a regulação do fluxo informacional.

Sendo assim, os sujeitos ativos no tratamento de dados devem estar em conformidade com as normas e princípios advindos da Lei Geral de Proteção de Dados, em prol da implementação da cultura protetiva de dados, a qual deve estar inserida internamente nas práticas empresariais, de modo a abranger as relações entre empregadores e empregados, enquanto agentes de tratamento e titulares de dados, respectivamente.

Em vista disso, a presente pesquisa se propôs a analisar o instituto do *compliance* de dados no âmbito do emprego como meio de efetivar a proteção de dados e garantir direitos da personalidade dos empregados, bem como verificar os principais aspectos considerados na gestão do contrato de emprego, relacionados à Lei Geral de Proteção de Dados (BRASIL, 2018).

Para tanto, observa-se que a adoção do *compliance* trabalhista, voltado para a legislação de dados, representa uma importante prática para concretizar a proteção de informações pessoais

nos ambientes internos das organizações, bem como para proteger direitos dos empregados, inclusive direitos da personalidade.

Dentre as boas práticas e governança estimuladas pelas disposições do artigo 50, da Lei Geral de Proteção de Dados, percebe-se que o *compliance* pode ser considerado uma forma mais específica de adequar a prática empresarial aos normativos legais, consistindo na elaboração de procedimentos e regramentos internos, os quais possibilitam a identificação e responsabilização por eventuais inadequações.

Além da conformidade com a legislação, outros benefícios aos empregadores (e agentes de tratamento de dados) decorrem da adoção do *compliance* trabalhista relacionado à nova lei, tais como, benefícios reputacionais e de imagem, aumento de valor e credibilidade ao negócio, consistindo em uma vantagem, um diferencial competitivo no mercado. Ainda, a demonstração do emprego de boas práticas, como o *compliance*, funciona como atenuante em casos de sanções administrativas, que podem ser aplicadas pelos órgãos fiscalizadores.

Além disso, pontua-se que as ferramentas de *compliance* contribuem para uma mudança nos modelos éticos e nas gestões empresariais, ou seja, além de possibilitarem a conformidade com as legislações trabalhistas, e demais normas, em especial com a LGPD, implementam a cultura de proteção de dados no ambiente interno das organizações, mostrando-se fundamental para prevenir e minimizar lesões aos direitos da personalidade dos empregados e demais colaboradores, propiciando um ambiente de trabalho digno.

Ademais, a promoção de ações conscientizadoras e educativas, como treinamentos, cursos e palestras, demonstram ser essenciais para difundir a cultura de proteção de dados, inclusive no âmbito do emprego, uma vez que ensinam sobre a proteção de dados, a importância de proteger suas próprias informações pessoais, bem como sobre os direitos da personalidade intrínsecos ao tratamento de dados, que podem sofrer lesões e ofensas pelo manejo inadequado, nas relações empregatícias.

De fato, o conhecimento acerca da proteção de dados não é difundido para todos os indivíduos, igualmente, embora não haja referida disparidade quando se trata de operar dados pela sua valoração socioeconômica, o qual pode ser fomentado nas relações empregatícias e nos ambientes laborativos, criando a cultura de proteger dados, primeiramente, no âmbito interno, de modo que tais diretrizes sejam incorporadas à identidade das organizações e demais agentes de tratamento de dados, empregadoras.

No que tange ao contrato de emprego, ressalta-se que a observância das normas trazidas pela Lei Geral de Proteção de Dados (BRASIL, 2018) deve ocorrer desde o momento pré-contratual, durante o período contratual, e após o término da relação empregatícia, tendo em vista que o tratamento de dados se tornou inerente à própria atividade de trabalho.

Dessa forma, a principiologia, as faculdades jurídicas e as normas trazida pela lei devem ser estritamente observadas, no que cabível, tanto na elaboração quanto na execução do contrato de emprego, por exemplo, com destaque para cláusulas contratuais que versem sobre o tratamento de dados dos empregados, e ainda, devem ser aderidas ao dia a dia do emprego, havendo o zelo pela

transparência na comunicação das decisões e práticas que envolvem dados, com a observância da finalidade e da adequação.

Inferem-se que algumas particularidades legais merecem maior atenção quando se trata da relação de emprego, como a informação sobre o uso de técnicas automatizadas, a utilização de biometria e de dados sensíveis na prática e no meio ambiente laborativo, além de precauções com o tratamento de dados baseado, somente, no consentimento.

Por fim, conclui-se, que o *compliance* trabalhista de dados apresenta, portanto, importantes ferramentas para atingir a finalidade maior da Lei Geral de Proteção de Dados (BRASIL, 2018), que corresponde à proteção dos titulares de dados, inclusive nas relações empregatícias e na gestão dos contratos de emprego, no que tange aos direitos da personalidade dos empregados, enquanto estimula a conscientização individual sobre a importância e os direitos relacionados ao tratamento de dados, incorporando, também, a cultura de proteger dados no ambiente laborativo.

## REFERÊNCIAS

BELLINETTI, Luiz Fernando; SOUZA, Raíssa Fabris de. *Compliance* trabalhista: uma análise a partir da função social da propriedade e da responsabilidade socioambiental da empresa. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 13, n. 40, p. 221-238, 2019. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/741/955>. Acesso em: 20 dez. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. Advocacia-Geral da União. Lei nº 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, ano 150, n. 148, p. 1, 02 ago. 2013. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/lei/112846.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/112846.htm). Acesso em: 20 dez. 2022.

BRASIL. Ministério da Ciência, Tecnologia, Inovação e Comunicações – MCTIC. Lei nº 13.709, de 14 agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, ano 155, n. 157, p. 59, 15 ago. 2018. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 20 dez. 2022.

BRASIL. Ministério do Trabalho. Decreto-lei nº 5.452, de 1º de maio de 1943. Aprova a Consolidação das Leis do Trabalho. **Diário Oficial da União**: seção 1, Brasília, ano 82, n. 184, p. 11937, 1 maio 1943. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/decreto-lei/del5452.htm](https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm). Acesso em: 20 dez. 2022.

BRASIL. Ministério do Trabalho. Lei nº 13.467, de 13 de julho de 2017. Altera a Consolidação das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, e as Leis nº 6.019, de 3 de janeiro de 1974, 8.036, de 11 de maio de 1990, e 8.212, de 24 de julho de 1991, a fim de adequar a legislação às novas relações de trabalho. **Diário Oficial da União**: seção 1, Brasília, ano 154, n. 134, p. 1, 14 jul. 2017. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2017/lei/113467.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/113467.htm). Acesso em: 20 dez. 2022.

BRASIL. Ministério do Trabalho. Lei nº 9.029, de 13 de abril de 1995. Proíbe a exigência de atestados de gravidez e esterilização, e outras práticas discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho, e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, p. 5361, 17 abr. 1995. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/19029.htm](https://www.planalto.gov.br/ccivil_03/leis/19029.htm). Acesso em: 20 dez. 2022.

CARLOTO, Selma. **Compliance Trabalhista**. 2. ed. São Paulo: LTr, 2020.

CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 371-384.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thompson Reuters, 2019. p. 677-715.

HISSA, Carmina Bezerra; GALAMBA, Priscilla Hissa do N. O impacto da LGPD na aplicação das normas de compliance. In: LIMA, Ana Paula Canto de; HISSA, Carmina Bezerra; SALDANHA, Paloma Mendes (coord.). **Direito digital: debates contemporâneos**. São Paulo: Revista dos Tribunais, 2019. p. 117-128.

MARCOLINO, Beatriz Aparecida; SILVEIRA, Daniel Barile da. A lei geral de proteção de dados e as relações de trabalho: o compliance como alternativa. **Revista Juris Unitoledo**, Araçatuba, SP, v. 05, n. 04, p. 206-224, 2020. Disponível em: <http://ojs.toledo.br/index.php/direito/article/view/3725/654>. Acesso em: 20 dez. 2022.

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

REIS, Beatriz de Felipe. 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, 2020. Disponível em: <https://hdl.handle.net/20.500.12178/180571>. Acesso em: 20 dez. 2022.

SANKIEVICZ, Alexandre; PINHEIRO, Guilherme Pereira. Aspectos da proteção de dados nas relações de trabalho. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 511-526.

SILVA, Fabrício Lima; PINHEIRO, Iuri; BOMFIM, Vólia. **Manual do compliance trabalhista: teoria e prática**. 2. ed. Salvador: Editora Juspodivm, 2021.

SILVA, Leda Maria Messias da; MARQUES, Ana Paula Baptista; ALKIMIM, Maria Aparecida. **Inteligência artificial e a dignidade do trabalhador no meio ambiente de trabalho: um difícil convívio?**. São Paulo: Editora LTr, 2021.

**Como citar:** DA SILVA, Leda Maria Messias; ALVES, Nadine Girardi. LGPD e *compliance*: a efetivação dos direitos da personalidade nas relações de emprego. **Scientia Iuris**, Londrina, v. 27, n. 2, p. 91-111, jul. 2023. DOI: 10.5433/2178-8189.2023v27n2p91-111. ISSN: 2178-8189.

Recebido em: 03/12/2021.

Aprovado em: 14/12/2022.