UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
BACHARELADO EM CIÊNCIAS JURÍDICAS E SOCIAIS

Aline Dal Bó Correa

COMPLIANCE DIGITAL NO DIREITO DO TRABALHO:

A Lei Geral de Proteção de Dados nas relações de trabalho

Porto Alegre
2022

Aline Dal Bó Correa

COMPLIANCE DIGITAL NO DIREITO DO TRABALHO:

A Lei Geral de Proteção de Dados nas relações de trabalho

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de bacharela em Ciências Jurídicas e Sociais da Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Orientadora: Luciane Cardoso Barzotto

Porto Alegre

2022

CIP - Catalogação na Publicação

Correa , Aline Dal Bó
Compliance Digital no Direito do Trabalho: A Lei Geral de Proteção de Dados nas relações de trabalho / Aline Dal Bó Correa . -- 2022.
53 f.
Orientadora: Luciane Cardoso Barzotto.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Direito, Curso de Ciências Jurídicas e Sociais, Porto Alegre, BR-RS, 2022.

1. Compliance . 2. Compliance Trabalhista . 3. Lei Geral de Proteção de Dados . 4. Direito do Trabalho . I. Cardoso Barzotto, Luciane, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

Aline Dal Bó Correa

COMPLIANCE DIGITAL NO DIREITO DO TRABALHO:

A Lei Geral de Proteção de Dados nas relações de trabalho

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de bacharela em Ciências Jurídicas e Sociais da Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Orientadora: Luciane Cardoso Barzotto

Aprovada em: Porto Alegre, 09 de agosto de 2022.

BANCA EXAMINADORA:

Professora Doutora Luciane Cardoso Barzotto, Orientadora
Universidade Federal do Rio Grande do Sul

Professor Doutor Fabiano Menke
Universidade Federal do Rio Grande do Sul

Professora Doutora Lenara Giron de Freitas
Universidade do Vale do Rio dos Sinos

Professora Mestra Rosana Kim Jobim
Universidade Federal do Rio Grande do Sul

Dedico este trabalho à Gladis, Olinda e Wally.
Minhas flores.

AGRADECIMENTOS

Este trabalho é a construção de 21 anos de trabalho árduo, anseios e sonhos. Portanto, devo agradecer àqueles que estiveram comigo neste processo:

Primeiramente à Deus e seu Filho, que com a civilização do amor fazem sentir que sei que sou um tanto bem maior.

À minha mãe, Adriane, por ser a melhor professora da vida que eu poderia pedir. E ao meu pai, Edmilson, por ser meu maior apoiador.

Às minhas avós, Olinda e Wally (*in memoriam*), por todo o carinho depositado. E aos meus avôs, Nilo (*in memoriam*) e Clóvis (*in memoriam*) por terem me ensinado valores éticos e inesquecíveis.

À minha avó do coração, Gladis, por todo o incentivo e apoio nesses 21 anos.

Ao meu companheiro, Gabriel, por ser meu porto seguro.

Aos meus dindos, Maria Andrea e Claudio, e Amanda, por serem tão amáveis e gentis comigo.

Aos meus amigos Glenda, Geórgia, Daniele e Murilo: Obrigada por ficarem até aqui. Amigos do Panela Velha, gratidão pela paciência. Aos da DPE Partenon: Obrigada por me ensinarem tanto. À MALUQ: Obrigada por me acolherem tão bem.

Agradeço à minha segunda família da faculdade: o Grupo de Debates e Oratória. Vocês me ajudaram tanto a ser quem eu sou e a evoluir como pessoa. Levo vocês para a vida inteira.

A todos os professores que passaram por mim, sem vocês eu não seria o que sou, em especial: Elivelto Machado, Rodrigo Luz Peixoto e Gerson Branco. Obrigada por pautarem meu caminho.

Aos meus colegas dos estágios que passei: Leonardo e Marina, DPE Partenon, TRT4, CMT Advogados. Obrigada por tudo que me ensinaram.

Por último, mas não menos importante, à minha orientadora, Luciane Cardoso Barzotto. Você é muito especial. Obrigada por tudo que me ensinastes nestes quatro anos de faculdade, por todos os projetos, empreitadas, trabalhos, artigos e por ser alguém com que eu posso contar.

“São os passos que fazem os caminhos.”

(Mário Quintana)

RESUMO

Através desta monografia, pretende-se verificar a aplicação de um programa de Compliance Data para que seja implementada a Lei Geral de Proteção de Dados no âmbito trabalhista. Como objetivos específicos, tem-se: a) proceder uma revisão bibliográfica a respeito do tema; b) identificar a legislação a respeito do tema escolhido; c) proceder análise da legislação com o estandarte da doutrina; d) fazer uma análise de riscos e benefícios de uma implementação sincrônica e diacrônica de um programa de Compliance Data; e) verificar as Etapas da implementação de um programa de Compliance para adequação à Lei Geral de Proteção de Dados; e f) elencar os Direitos dos Trabalhadores tutelados pela Lei Geral de Proteção de Dados. Pretende-se utilizar nesta pesquisa o método dedutivo. Através da análise da legislação atual e doutrina constrói-se a interpretação quanto à existência de um programa de Compliance Data. A análise de doutrina se dará pela revisão sistemática de literatura e de legislação atual por interpretação dogmática.

Palavras-chave: Compliance Trabalhista. Lei Geral de Proteção de Dados. Direito do Trabalho.

ABSTRACT

Through this monograph, it is intended to verify the thesis that it is possible to apply a Compliance Data program to implement the General Data Protection Law in the labor field. As specific objectives of this monograph, we have: a) carry out a bibliographic review on the subject; b) identify the legislation on the chosen subject; c) to carry out an analysis of the legislation with the banner of the doctrine; d) to make an analysis of risks and benefits of a chronic and diachronic implementation of a Compliance Data program; e) verify the stages of the implementation of a Compliance program to adapt to the General Data Protection Law; f) list the Rights of Workers protected by the General Data Protection Law. The deductive method is intended to be used in this research. Through the analysis of current legislation and doctrine, the interpretation of the existence of a Compliance Data program is constructed. The analysis of doctrine will take place by systematic review of literature and current legislation by dogmatic interpretation.

Keywords: Labour Compliance. General Law of Data Protection. Labour Law.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIAÇÕES

ADI	–	Ação Direta de Inconstitucionalidade
ANPD	–	Autoridade Nacional de Proteção de Dados
CC	–	Código Civil Brasileiro
CDC	–	Código de Defesa do Consumidor
CF	–	Constituição Federal
CLT	–	Consolidação das Leis do Trabalho
COSO	–	Committee of Sponsoring Organizations of the Treadway Commission
DPIA	–	Data Protection Impact Assessments
DPO	–	Data Protection Officer
GDPR	–	General Data Protection Regulation
ISSO	–	International Organization for Standardization
LGPD	–	Lei Geral de Proteção de Dados
MPT	–	Ministério Público do Trabalho
OIT	–	Organização Internacional do Trabalho
ONU	–	Organização das Nações Unidas
PIA	–	Privacy Impact Assessment
STF	–	Supremo Tribunal Federal

SUMÁRIO

1 INTRODUÇÃO

É notório que vem ocorrendo uma transformação digital, que está mudando o modo que se vive e, por consequência, a maneira que se trabalha. Essa transformação acarreta diversas mudanças positivas, como democratização do acesso à informação, qualidade de vida e facilidade no uso de serviços e produtos. Por outro lado, se pode notar a precarização das relações de trabalho, a extinção de postos de trabalho, a exposição ao estresse e a falta de proteção social aos trabalhadores.

Os dados, nesta transformação digital, têm grande valor econômico, sendo considerados o principal insumo da sociedade contemporânea. Pode-se afirmar, portanto, que se vive em uma economia movida por dados (*data driven economy*). É por esta razão que a proteção de dados virou pauta em diversos países, de maneira a garantir o seu uso correto.

O Conselho da Europa disciplina o tratamento de dados pessoais desde 1973, por meio da Resolução nº 22/1973 e da Resolução nº 29/1974, ambas versando sobre princípios para a proteção de informações pessoais em bancos de dados automatizados, no setor público e privado. Entretanto, o tratamento mais abrangente da matéria, no âmbito da União Europeia, foi realizado pela Diretiva nº 46/1995, sucedida pelo Regulamento Geral da Proteção de Dados (GDPR), o qual entrou em vigor em 25 de maio de 2018.

No Brasil, vive-se um grande período de indefinição legislativa a respeito das normas infralegais sobre o tema, o que não tem o mesmo significado que desproteção, pois a privacidade e a intimidade são valores declarados como direitos fundamentais na Constituição Federal (art. 5º, X, CF/88). Além disso, existem outras manifestações infraconstitucionais, a exemplo do Código de Defesa do Consumidor (arts. 43 a 45 do CDC); Lei nº 9.507, de 12.11.1997 (Habeas Data); Lei nº 12.414, de 9.06.2011 (Cadastro Positivo); Lei nº 12.527, de 18.11.2011 (Lei do Acesso à Informação); e Lei nº 12.965, de 23.04.2014 (Marco Civil da Internet).

Contudo, apenas em 15 de agosto de 2018, com a publicação da Lei Geral de Proteção de Dados (LGPD), o Brasil recebeu a confiança da comunidade internacional a respeito da confiabilidade do compartilhamento de dados.

A Lei Geral de Proteção de Dados trouxe diversos aspectos inovadores para o ordenamento jurídico brasileiro, entre estes o poder de consentimento do titular dos dados pessoais que serão coletados, o princípio da autodeterminação informativa, o qual confere ao titular dos dados protagonismo no tratamento de suas informações pessoais. Apesar de as disposições da LGPD não se destinarem, em princípio, às relações de trabalho, elas abrangem a relação entre empregado e empregador, visto que tanto na fase pré-contratual, quanto durante a relação laboral e até mesmo após a extinção do vínculo, está presente o fluxo de dados pessoais daquele trabalhador.

Justamente por não existir regulamentação específica na LGPD que trate da relação entre empregados e empregadores, torna-se necessária uma análise cuidadosa acerca de sua aplicação, ou seja, dos riscos de não estarem delimitadas as orientações de comportamento, de conformidade, e de não reconhecer os trabalhadores como portadores do direito à proteção de dados pessoais e as consequências práticas para o empregador e o trabalhador.

Portanto, mesmo que a legislação brasileira não tenha especificado na LGPD a aplicação da proteção de dados nas relações de trabalho, é necessário elencar a necessidade de armazenamento de dados, bem como as causas legitimadoras do seu tratamento. Cabe um olhar atento dos profissionais da área trabalhista para que estejam preparados em um sistema de gestão de riscos e exigências da proteção de dados.

Neste trabalho, pretende-se responder a seguinte pergunta: “É possível implementar um programa de Compliance para adequar as empresas à Lei Geral de Proteção de Dados com relação aos seus empregados?”

Através do problema de pesquisa, chega-se à seguinte hipótese: É possível a implementação da Lei Geral de Proteção de Dados por conta de uma obrigação legal das empresas com seus empregados, o que pode ser feito através de um programa de Compliance Data.

Através desta monografia, pretende-se verificar a tese de que é possível a aplicação de um programa de Compliance Data para que seja implementada a Lei Geral de Proteção de Dados no âmbito trabalhista. São objetivos específicos desta monografia: a) proceder uma revisão bibliográfica a respeito do tema; b) identificar a legislação a respeito do tema escolhido; c) proceder análise da legislação com o

estandarte da doutrina; d) fazer uma análise de riscos e benefícios de uma implementação sincrônica e diacrônica de um programa de Compliance Data, de acordo com o tópico 4.1; e) verificar as etapas da implementação de um programa de Compliance para adequação à Lei Geral de Proteção de Dados; e f) elencar os Direitos dos Trabalhadores tutelados pela Lei Geral de Proteção de Dados.

Na primeira parte do trabalho, pretende-se traçar um panorama geral da Lei Geral de Proteção de Dados, comparando-a com o Regulamento Geral de Proteção de Dados Pessoais Europeu (GDPR), frisando aspectos gerais da lei e sua incidência nas relações de trabalho. Na segunda parte, abordar-se-á o conceito de compliance e suas ferramentas, bem como as etapas de implementação de um programa de compliance. Por último, serão apresentados os riscos e os benefícios de uma implementação sincrônica e diacrônica da LGPD, por conseguinte, compliance de dados do empregador e a proteção de dados do trabalhador como direitos fundamentais.

Pretende-se utilizar nesta pesquisa o método dedutivo. Através da análise da legislação atual e doutrina, construir-se-á a interpretação quanto à existência de um programa de Compliance Data. A análise de doutrina se dará por revisão sistemática de literatura e de legislação atual por interpretação dogmática.

2 LEI GERAL DE PROTEÇÃO DE DADOS CONCEPÇÕES, FUNDAMENTOS E LEI 13709 DE 2018

A Sociedade Informacional trouxe uma significativa mudança em às relações, dentre as quais, se pode destacar, a maneira como se resolvem os conflitos. Contudo, ainda não se chegou a um consenso de como tratar os direitos do ambiente digital (ou seja, do conjunto de dados) a partir do princípio da dignidade da pessoa humana ou até mesmo dos direitos humanos fundamentais. Em razão disso, surge a necessidade de meios para garantir os direitos e deveres internos e externos ao ambiente digital.

Para melhor compreender as delimitações do ambiente digital, é necessário explicitar os conceitos de dado pessoal e dado sensível:

> Dados pessoais são todas as informações de caráter personalíssimo caracterizadas pela identificabilidade e pela determinabilidade do seu titular, enquanto os dados sensíveis são aqueles que tratam sobre a origem racial e étnica, as convicções políticas, ideológicas, religiosas, as preferências sexuais, os dados sobre a saúde, os dados genéticos e os biométricos. (SARLET; TRINDADE; MELGARÉ, 2021, p. 19-20).

Considerando que as informações podem ser utilizadas para fins políticos e econômicos, que posteriormente podem ser fonte para ferramentas de controle social, pode-se dizer que a proteção de dados é a proteção da pessoa humana. Dessa forma, no âmbito jurídico, a proteção de dados é convocada a ser regulada.

Nesse contexto, a proteção jurídica de dados pessoais iniciou-se no limiar da década de 1970, com o reconhecimento da proteção dos dados pessoais como um direito humano e fundamental, à exemplo da Constituição da República Portuguesa de 1976 e da Constituição Espanhola de 1978.

No caso do Brasil, a Constituição Federal de 1988 (CF) não contemplou no seu texto um direito fundamental autônomo à proteção de dados pessoais. Direito este que veio a ser reconhecido, como implicitamente positivo, pelo Supremo Tribunal Federal (STF) somente em maio de 2020, por ocasião do julgamento do mérito da Ação Direta de Inconstitucionalidade ADI 6387-DF, relatada pela ministra Rosa Weber.

Em 27 de abril de 2016, foi promulgado o Regulamento Geral de Proteção de Dados Pessoais Europeu (GDPR), com o objetivo de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses

dados. Esse evento fez com que vários outros países se atentassem à importância da proteção de dados, visto que a União Europeia passou a exigir que os demais países, com quem realizassem transações comerciais mútuas, dispusessem de regulamento semelhante.

Em 15 de agosto de 2018, foi publicada a Lei nº. 13.709, nomeada de Lei Geral de Proteção de Dados Brasileira (LGPD). Dividida em 10 Capítulos e com 65 artigos, comparativamente, a LGPD é menor que a sua referência europeia (GDPR), que possui 11 Capítulos, com 99 artigos. A versão mais enxuta deixa margem para maior interpretação, o que traz certa insegurança jurídica. Um exemplo disso ocorre em relação à determinação de prazos: enquanto o GDPR prevê prazos exatos, como de 72 horas, a LGPD prevê “prazo razoável”. Segundo Pinheiro (2021), ambas as legislações têm como objetivo o regramento do tratamento de dados pessoais, buscando em si a defesa dos direitos fundamentais das pessoas naturais, como se pode observar no Quadro 1, a seguir.

Quadro 1 - Proteção De Dados Pessoais

ITEM DE CONFORMIDADE	REGIME BRASILEIRO (LGPD)	REGIME EUROPEU (GDPR)
Definição e distinção do que são dados pessoais e dados sensíveis. Tal conceituação busca delimitar os direitos e as informações protegidas pelo ordenamento jurídico	Define que dado pessoal é qualquer informação que identifique ou torne identificável a pessoa natural; já dados sensíveis são dados pessoais sobre etnia, raça, crenças religiosas, opiniões políticas, dados genéticos/biométricos, além de informações sobre filiações a organizações quaisquer da pessoa natural.	Adota os mesmos princípios e conceitos para realizar a distinção e delimitação dos direitos relativos aos dados pessoais e dados sensíveis, e ainda pontua considerações acerca dos dados genéticos, biométricos e os relativos à saúde.
Obrigatoriedade do consentimento do usuário para a coleta de informações e limitação do tratamento do dado conforme finalidade	A coleta e o tratamento de dados só poderão ser realizados se o usuário (dono dos dados ou responsável legal no caso de menores legais) der consentimento. Todo agente deve apontar finalidade certa, garantida e justificável ao tratamento do dado. Além disso, deve garantir que ele será utilizado somente para tal finalidade.	Prevê a necessidade de uso do dado conforme a finalidade apontada. Traz exceções de tratamento por motivo de interesse público, segurança e saúde.
Distinção entre titularidade e responsabilidade sobre os dados, assim como delimitação das funções e responsabilidades assumidas no tratamento de dados	Titular é a pessoa natural a quem se referem os dados que são objeto de tratamento; por outro lado, o responsável é a pessoa física ou jurídica, de direito público ou privado, que realiza decisões sobre o tratamento de dados. São definidos dois agentes de tratamento: o responsável – cuja competência é decidir sobre o tratamento dos dados – e o operador – a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados. Ambos os agentes são juridicamente responsáveis pela segurança e privacidade dos dados.	Há a mesma distinção entre titularidade e agentes, mas os agentes são divididos em controlador e processador de dados. O controlador é quem realiza as decisões acerca do tratamento de dados; o processador, quem efetua o tratamento dos dados. Ambos são responsáveis pelo tratamento dos dados.
Indicação de um encarregado pela comunicação entre os agentes, titulares e órgãos competentes	Além dos agentes, aponta-se a necessidade da indicação de um encarregado – pessoa natural – pela comunicação de qualquer informação ou fato relevante em relação ao tratamento dos dados. Ele deve atuar como um canal entre os agentes, titulares e órgãos competentes e deve ser indicado pela organização responsável pelo tratamento (Agente de Proteção de Dados).	Aponta que o controlador deve ter uma pessoa responsável por tudo que seja relacionado à proteção de dados (DPO).
Aplicação de mecanismos e práticas pautadas no livre acesso à informação e na transparência entre os usuários e as organizações	Do consentimento ao fornecimento de dados ao término do tratamento dos dados, as informações acerca do processo devem ser claras, acessíveis e adequadas à linguagem e compreensão do usuário, de forma que o seu consentimento possa ser revogado a qualquer momento. O consentimento do usuário deve ser realizado por escrito ou de qualquer outro modo que demonstre a sua livre manifestação da vontade.	Os titulares também têm direito a informações claras e acessíveis do início ao fim do tratamento do dado, podendo revogar o consentimento a qualquer momento.
Aplicação de medidas de segurança e dever de reportar	Da mesma forma que as organizações são responsáveis no caso de incidentes – como vazamentos – no tratamento dos dados, devem aplicar medidas de prevenção e proteção à segurança dos dados que manuseiam, como anonimização e encriptação das informações. Ainda assim, no caso de qualquer incidente é obrigação da organização notificar as autoridades imediatamente.	Também aponta que as empresas devem criar medidas – como pseudoanonimização e encriptação de dados – para garantir a segurança de forma preventiva. No caso de qualquer incidente, a notificação às autoridades deve ser imediata.
Possibilidade de alteração e exclusão do dado pessoal	O titular do dado pode alterar ou excluir seu dado pessoal a qualquer momento,	Os titulares dos dados também podem alterar ou excluir seus dados.
Possibilidade de alteração e exclusão do dado pessoal	exceto nas hipóteses previstas na lei, como fins fiscais, por exemplo. Da mesma forma, assim que o tratamento de dados chegar ao final – seja porque cumpriu sua finalidade, seja porque o usuário revogou seu consentimento –, as informações devem ser eliminadas.	
Aplicação de sanções no caso do descumprimento das regras	As punições variam entre advertências, aplicação de multas, suspensão e até mesmo proibição das atividades relacionadas ao tratamento de dados. Essas punições variam de forma gradativa de acordo com cada caso, conforme a gravidade do dano, a condição econômica do infrator, a reincidência, a boa-fé do infrator etc., e devem ser investigadas por meio de um processo administrativo que assegura o contraditório, a ampla defesa e o direito de recurso. As multas podem ser simples ou diárias, com valor relativo a 2% do faturamento da organização privada, limitadas a um total de R$ 50 milhões por infração.	Também prevê a aplicação de sanções gradativas e multas administrativas, que podem chegar a 20 milhões de euros ou a 4% do faturamento anual da empresa.
Criação de um órgão competente para fiscalizar e zelar pela proteção de dados pessoais e da privacidade	Criada a Autoridade Nacional de Proteção de Dados Pessoais (ANPD).	Possui um Órgão de Controle e Fiscalização de Proteção de Dados Pessoais por Estado (28) e aplica o princípio do Balcão único.

Fonte: Pinheiro (2021).

A LGPD, portanto, se aplica a todos aqueles que realizam o tratamento de dados pessoais, sejam organizações públicas ou privadas, pessoas físicas ou jurídicas, que realizam qualquer operação de tratamento de dados pessoais, independentemente do meio, que possa envolver pelo menos um dos seguintes elementos: (i) ocorrer em território nacional; (ii) que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; (iii) em que os dados tenham sido coletados no território nacional. Sendo assim, a LGPD não está relacionada à cidadania ou à nacionalidade dos dados pessoais, tampouco à residência do indivíduo titular.

Importante ressaltar que as regulamentações de proteção de dados têm caráter principiológico, ou seja, trazem um rol de princípios que precisam ser atendidos. A melhor metodologia de análise da lei encontrada pelo legislador é pela verificação da conformidade dos itens de controle, ou seja, se o controle não está presente, aplicado e implementado, logo, o princípio não está atendido. De acordo com Pinheiro (2021, p. 18), “a legislação visa fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico”.

O art. 6º da Lei ressalta a boa-fé, assim como os princípios da (i) finalidade; (ii) adequação; (iii) limitação do tratamento de dados ao mínimo necessário para a realização de suas finalidades; (iv) garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; (v) qualidade dos dados (garantia de exatidão, clareza, relevância e atualização dos dados); (vi) transparência; (vii) segurança; (viii) adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; (ix) impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e (x) responsabilização e prestação de contas, ou seja, o agente precisa demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Frisa-se que da boa-fé e da segurança decorrem os demais princípios que deverão guiar o comportamento das empresas que coletam e tratam, de qualquer forma, dados pessoais. No caso, destacam-se: (i) minimização dos dados: os princípios da Lei impõem que sejam coletados apenas dados mínimos para a

finalidade do serviço a ser prestado ou produto. Esse conceito deve ser incorporado desde a concepção do serviço ou produto a ser ofertado (*Privacy by Design*), devendo o controlador sempre efetuar a pergunta “é preciso coletar esse dado? Para qual finalidade”? na medida em que, inexistindo finalidade clara e adequação, o tratamento poderá ser considerado abusivo; (ii) adequação do tratamento dos dados à finalidade para os quais foram coletados: o tratamento não pode estar dissociado daquilo que o titular razoavelmente espera ao fornecê-lo.

Ainda, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), com a finalidade de executar as adequações necessárias para que a legislação tenha uma aderência maior com a realidade social e econômica. A ANPD tem papel primário como elo entre diversas partes interessadas que deverão continuar a compreender a temática da dinâmica dos dados pessoais em um contexto não apenas nacional, mas principalmente internacional para que o Brasil saiba se posicionar no mercado digital global.

Contudo, a análise desses princípios permite concluir que a sua simples observação não chega a garantir uma efetiva proteção de dados, pois apenas uma interpretação sistemática e complementar alcançará o objetivo pretendido com a lei geral. Pode se verificar, também, que os princípios são direcionados a todos os atores que, de alguma forma, trabalhem com a operação de coleta de dados.

2.1 ASPECTOS GERAIS E INCIDÊNCIA NAS RELAÇÕES DE TRABALHO

A Lei Geral de Proteção de Dados se destina às relações jurídicas em geral, e, consequentemente, as relações de trabalho, em termos normativos, são, também, por ela afetadas. Ao contrário do GDPR (art. 25), que versa que:

> 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
>
> 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That

> obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.[1]

A LGPD não prevê de forma expressa em seu texto este tema, entretanto, ela se aplica ao tratamento dos dados pessoais dos empregados pelos empregadores, que são os controladores destes dados. Ou seja, trabalhadores são os titulares dos dados, enquanto empregadores são os controladores dos dados.

> Art. 5º Para os fins desta lei, considera-se:
> [...] 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; (BRASIL, 2018).

O acesso aos dados pessoais pelo empregador (controlador) configura obrigação de cumprimento legal, conforme ordena a própria LGPD, no seu art. 7º, V e IX, pois visa a atender aos legítimos interesses do empregador para execução do contrato de trabalho em benefício do próprio empregado.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses
> [...] V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato;
> [...] 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. (BRASIL, 2018).

A adequação à LGPD, portanto, deve começar desde o recrutamento de novos empregados, sendo solicitados apenas os dados essenciais à vaga, sempre atentando a ideia de o mínimo necessário para a finalidade. Ainda, não se pode utilizar esses dados para discriminar um candidato em seleção, ou seja, não pode ocorrer

[1] Em tradução livre: 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados. 2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

coleta de dados com intuito discriminatório. Calcini e Andrade (2021, p. 1-2) examinam a questão da seguinte forma:

> A fase pré-contratual é a etapa do primeiro contato do candidato com o potencial empregador e geralmente é realizada por terceiros (recrutador, departamento pessoal, empresas especializadas etc.). Nessa fase há disponibilização da vaga, análise do currículo, entrevistas e posterior escolha do candidato selecionado. Naturalmente, os procedimentos preliminares a um contrato de trabalho legitimam o acesso aos dados pessoais do candidato logo a partir do anúncio de um emprego, devendo o empregador se ater ao estritamente necessário para o exercício da função a ser contratada. Em outras palavras, o empregador pode solicitar ao empregado o nome completo, a data de nascimento, estado civil, escolaridade, o número do CPF, filiação, a numeração do RG, o endereço de domicílio, o contato telefônico, e-mail pessoal ou corporativo, IP do computador etc. Ainda na fase preliminar, é proibida a coleta de dados sensíveis que possam gerar qualquer critério discriminatório entre os candidatos. De modo que é de suma importância que o empregador avalie quais serão os dados requeridos ao candidato para que não haja descumprimento das normas legais.

Como salientado, mesmo na fase anterior à vigência do contrato de trabalho, a LGPD já possui efeitos. Isso porque, nessa fase, de acordo com os fundamentos e princípios da LGPD, é proibida a coleta de dados que possam representar qualquer critério discriminatório entre os candidatos, como solicitação de exames de gravidez, toxicológico ou de sangue; atestado de antecedentes criminais ou análise de crédito. A demanda desse tipo de documentos representaria inefável violação à Lei nº. 9.029/95 e aos artigos 5º, *caput* e 7º, XXX, da CF/88, que vedam qualquer forma de discriminação nas relações em geral e trabalhistas no Brasil. Sobre essa vedação às práticas discriminatórias na fase pré-contratual, Reani (2018, p. 3-4) traz a seguinte ponderação:

> Um dos princípios basilares de LGPD é o da não discriminação. Ele determina que uma pessoa não pode ser discriminada, de modo que a prejudique, com base nos seus dados pessoais. Ainda, a LGPD confere ao titular — a pessoa física a quem os dados se referem —, o direito de ter acesso a todos os dados que uma entidade, privada ou pública, tem sobre ela. Assim, o cidadão poderia verificar realmente quais dados sobre ele a empresa tinha em mãos e o que fez com tais dados após o uso dos mesmos. A LGPD, de forma objetiva, reforça, por exemplo, o que o direito trabalhista já consolidou na Consolidação das Leis do Trabalho, no capítulo específico para proteção do trabalho da mulher, onde consta expressamente a vedação da discriminação.

É importante mencionar que a empresa deve elaborar um documento pelo qual o candidato ao emprego indique o seu consentimento expresso com a coleta e a utilização dos seus dados pela possível contratante. Desse modo, a empresa seguramente mitigará significativamente o risco de realizar a coleta indevida de dados pessoais dos candidatos.

Não obstante, a empresa deverá informar claramente aos candidatos não selecionados a política de utilização dos dados fornecidos, além do destino dos dados e documentos daqueles que não foram selecionados. Assim, uma vez rejeitado o candidato ao emprego, a empresa deve desfazer-se daqueles dados, pois entende-se por cessada a finalidade do seu tratamento, nos termos do art. 15 da LGPD; salvo se existente a possibilidade de contratação futura, ainda que não formalizada de imediato, fato que deve ser devidamente informado ao candidato.

Ainda que o consentimento seja exceção, deve-se ter ainda mais cautela com os dados, para não ferir a privacidade do trabalhador. As violações previstas poderão ser objeto de reclamação trabalhista e denunciadas ao Ministério Público do Trabalho (MPT), bem como sujeitas à fiscalização da Autoridade Nacional de Proteção de Dados (ANPD), com sanções disciplinares previstas no art. 52 da LGPD.

Mesmo na fase pós-contratual, a LGPD demanda cautela por parte da empresa, pois o tratamento de dados do antigo empregado deve ser realizado de acordo com os seus preceitos. Isso se dá pelo fato de que a LGPD, expressamente, estipula ser necessária a informação de finalização do uso de dados, seja por determinação legal, seja por solicitação do titular do direito. Ocorre que, no caso das relações trabalhistas, há obrigações de guarda de documentos que decorrem de imposição legal, o que afasta a possibilidade de eliminação imediata dos dados do empregado, ainda que haja solicitação expressa de sua parte. Por conseguinte, a empresa pode manter os dados pessoais gerais do empregado sob guarda pelo prazo prescricional de até dois anos após a ruptura contratual (CF, art. 7º, XXIX), para eventual utilização em reclamação trabalhista futura.

Por conseguinte, na seara laboral é fundamental valer-se dos princípios e diretrizes da LGPD para se impor limites a uma possível invasão de dados pessoais dos empregados, impondo às empresas o dever de tratar esses dados de forma prudente e cautelosa, sob pena de responsabilização, inclusive por meio de eventual indenização por danos morais causados aos trabalhadores.

2.2 DIREITOS DOS TRABALHADORES TUTELADOS PELA LEI GERAL DE PROTEÇÃO DE DADOS

O Direito do Trabalho, no entendimento de Delgado (2007), consolidou-se como o patamar fundamental de afirmação da cidadania social da maior parte das pessoas que participavam do sistema econômico. Nessa linha, pode-se dizer que a proteção dos direitos da personalidade só se concretizará quando estiver efetivamente adequado às diversas classes sociais e minorias.

Como exposto, a LGPD deve garantir aos trabalhadores o respeito do uso de seus dados pessoais com base na privacidade, intimidade e liberdade. Portanto, direito à proteção de dados pessoais deve ser visto não apenas como um novo direito da personalidade, mas também como mais uma forma de tutela dos direitos fundamentais do empregado, intuito que deve ser primordial ao Direito do Trabalho.

Além de ser um direito autônomo, a proteção de dados pessoais é um direito fundamental, merecendo toda atenção do legislador infraconstitucional e dos aplicadores do Direito. A fim de manter sempre atual a LGPD, sua base é essencialmente principiológica, tendo como fundamento os princípios listados anteriormente.

Ainda, importante ressaltar as bases de tratamento dos dados pessoais sensíveis, constantes no art. 11 da LGPD, que abaixo se transcreve:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for Estudos sobre LGPD - Lei 13.709/2018 392 indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2018).

O titular dos dados detém de diversos direitos em relação aos seus dados, a iniciar pela liberdade, privacidade e livre desenvolvimento da sua personalidade (art. 1º), além dos elencados no art. 18, direitos estes que poderiam ser explicitados por normas coletivas, a fim de que correspondam à principiologia legal do art. 6º da LGPD e respondam ao titular algumas perguntas: para que fim são guardados os dados, em que contexto e etc. Nesses termos, cumpre referir que os direitos do titular dos dados correspondem aos princípios fixados na Lei, como didaticamente indica Barzotto (2022):

Quadro 2 - Direitos do titular dos dados

PRINCÍPIOS	PERGUNTAS SOBRE DADOS	DIREITOS DO TITULAR
I – Finalidade	Para que fim	Informação – art. 9º
II – Adequação	Em que contexto	Portabilidade – art. 18, V
III – Necessidade	Por que é preciso	Negativa – art. 18, VII
IV – Livre acesso	Onde	Acesso – art. 9º
V – Qualidade dos dados	Como	Correção – art. 7, § 6º
VI – Transparência	Qual modo	Confirmação – art. 8º, 37
VII – Segurança	Com que medidas	Eliminação – art. 16
VIII – Prevenção	Em vista de que	Anonimização – art 11, §, c
IX – Não-discriminação	Para que não	Revisão – art. 20
X – Responsabilização e prestação	Quem responde	Revogação – art. 8, § 5º

Fonte: Barzotto (p. 392, 2022).

Para corroborar a aplicação dos princípios da LGPD no Direito do Trabalho, a Organização Internacional do Trabalho (OIT), em Declaração publicada por ocasião do seu centenário (OIT, 2019), menciona a necessidade de que o trabalhador tenha garantida a proteção de seus dados pessoais e privacidade por meio do reforço das instituições. Essa proteção para o futuro do trabalho – proteção de dados –, deve se dar de forma individual e mesmo de modo coletivo, com a participação de empregadores e empregados, para que se chegue à plena defesa dos direitos dos trabalhadores. [2]

[2] A OIT volta a tratar do tema em 2020, no guia prático “Teletrabalho durante e após a pandemia da COVID-19”.

3 COMPLIANCE TRABALHISTA: UMA ABORDAGEM GERAL LABORAL

A LGPD versa sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, de direito público ou privado, e tem por fim máximo a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Tem como fundamento, no seu art. 2º, V, valores como a garantia do desenvolvimento econômico e tecnológico, bem como a inovação. Como já abordado neste trabalho, a Lei trouxe uma grande necessidade de adaptação quando relacionada ao tema privacidade e proteção de dados pessoais, por esta razão, deve-se tratar do tema Compliance Trabalhista.

O primeiro conceito fundamental para se entender a extensão do escopo de aplicação da LGPD é o conceito de Dado Pessoal. Nos termos do artigo 5º, I, Dado Pessoal é qualquer "Informação relacionada a pessoa natural identificada ou identificável". De acordo com Palhares, Prado e Vidigal (2021):

> No campo prático, o conceito de dado pessoal vai além daqueles dados comumente utilizados em cadastros (como nome, endereço, profissão, documento de identidade) e, na maioria das vezes, inclui qualquer tipo de informação que possa ser útil à individualização de uma pessoa natural (física), como conjunto de hábitos, comportamentos, preferências, registros eletrônicos (inclusive dados de acesso e uso de internet). Trata-se, portanto, de um conceito aberto, sendo praticamente impossível cravar se determinado dado é ou não pessoal sem a análise do contexto em que se insere.

Da mesma forma, a LGPD define "titular de dados" como a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (art. 5º, V). O titular é o "dono" do dado pessoal, atributo que não cabe a pessoas jurídicas, ainda que em sua posse existam bases de dados que incluam dados de pessoais naturais (titulares). Nesse sentido, a pessoa jurídica, no limite, trata dados pessoais de acordo com as regras aplicáveis, mas não é titular deles, ainda que tenha investido para sua coleta e manutenção.

Compliance, em tradução literal, significa estar em conformidade. Esse estado de conformidade exige orientação de comportamento, a qual vem a se tornar norma jurídica, que varia conforme a área do Direito. Esse estado de conformidade mencionado diz respeito a organização de um Sistema de Gestão de Compliance. A expressão Sistema de Gestão de Compliance (*Compliance Managment System*) foi cunhada pela *International Organization for Standardization* (ISO, 2014), por meio da

norma ISO 19600. A proteção de dados e a tão difundida necessidade de “adequação à LGPD” são, portanto, um elemento desse sistema mais amplo de gestão de compliance. Esse ponto já está sedimentado na doutrina, na legislação pátria, nos manuais internacionais de certificação e na própria ISO.

Entretanto, a noção de compliance é mais do que o mero cumprimento da legislação. O compliance também tem por objetivo criar, difundir e consolidar uma cultura e uma prática de respeito às normas jurídicas e éticas, razão pela qual comumente é baseado em códigos de ética ou princípios, cuja finalidade é mostrar como os objetivos empresariais de cada agente econômico podem e devem ser buscados de forma compatível com a preservação dos valores defendidos pela organização.

Vale ressaltar que o compliance de dados e, também, o compliance de dados trabalhista, lida diretamente com um complexo sistema, no qual, a lei, os contratos, a conduta dos agentes e de seus empregados, precisam estar em conformidade com os mecanismos de políticas, de controles internos, de código de ética e de conduta. Nesse sentido, pontua Saavedra (2021):

> Nesse sentido, um dos problemas do compliance é o de que ele lida com fenômenos diversos de autorregulação, desde a autorregulação tradicional à chamada “autorregulação regulada”. Trata-se de normas de orientação de comportamento que não têm natureza jurídica estrita, mas que passam a ter “relevância jurídica” ou por força de contrato (por meio das conhecidas “cláusulas contratuais de compliance”) ou por força de lei (como a Lei Anticorrupção, que atribui explicitamente consequências jurídicas para aquelas empresas que tiverem Códigos de Ética e Códigos de Conduta, ou seja, deixa claro que a existência dessas normas internas passa a ter impacto na forma como será aplicada a pena no caso concreto), Portanto, compliance consiste em um estado dinâmico de conformidade a uma orientação normativa de comportamento com relevância jurídica por força de contrato ou lei, caracterizado pelo compromisso com a criação de um sistema complexo de políticas, de controles internos e de procedimentos, que demonstrem que a empresa está buscando "garantir", que se mantenha em um estado de compliance." (SAAVEDRA, 2021, p. 729-730);
>
> [...] não há dúvida de que a proteção de dados e a tão difundida necessidade de "adequação à LGPD" nada mais são do que um elemento desse sistema mais amplo de gestão de compliance." (SAAVEDRA, 2021, p. 730).

Já o compliance trabalhista pode ser todo o procedimento ou qualquer procedimento para evitar as ações trabalhistas e a responsabilização da empresa. Piza e Mendes (2019) discorrem sobre os pilares do compliance trabalhista, assinalando que:

> [...] pretende estabelecer na empresa programa voltado para a obediência a critérios legais de contratações de funcionários, demissões, relação interpessoal entre funcionários, normas de saúde e segurança do trabalho, terceirização de serviços entre outros.

As autoras apontam 10 pilares do compliance trabalhista, a saber: 1. Suporte da alta administração – assessoramento direto aos proprietários da empresa. 2. Avaliação de riscos – procedimento prévio e com antecedência para evitar a ocorrência do evento danoso. 3. Código de conduta, regulamento interno, políticas da empresa – elaboração de um guia com princípios e valores da empresa. 4. Controles internos – meios de prevenir e corrigir problemas. 5. Treinamentos – atualização periódica de todos (patrões e empregados). 6. Canais de denúncia – adoção de instrumentos para coibir assédio e abuso. 7. Investigação interna – procedimentos para avaliar denúncias. 8. Due diligence – com relação a terceirizados quando houver, para ter conhecimento efetivo da sua realidade. 9. Auditoria e monitoramento – avaliação constante (monitoramento) e auditoria para detectar irregularidades e produtividade. 10. Ouvidoria – veículo de contato direto com o usuário dos serviços prestados pela empresa, para elogiar, criticar, incentivar e apresentar sugestões acerca dos empregados e das atividades que desenvolve (PIZA; MENDES, 2019).

O compliance é recomendado pela OIT desde o final do século XX. Dentre as atividades que podem ser desenvolvidas no compliance trabalhista, destacam-se as tarefas necessárias ao bom funcionamento patronal. Nesse rol exemplificativo, de acordo com Franco Filho (2021), estão:

> (1) a análise criteriosa dos riscos operacionais;
> (2) o controle interno da organização (que o Chief Compliance Officer deverá executar), inclusive para detectar fraudes e procedimentos irregulares;
> (3) o monitoramento das atividades da empresa, com a equipe de tecnologia da informação (que também deve ser avaliada);
> (4) a realização de auditorias e avaliação de políticas de recursos humanos, a fim de melhorar os serviços e adequar às normas técnicas e de saúde e segurança do trabalho;
> (5) o controle e aplicação da legislação existente para que sejam cumpridas as obrigações sociais da empresa, enquanto empregador.

Nesse aspecto, embora não direcionada ao compliance, deve ser dado especial realce à Agenda 2030 para o Desenvolvimento Sustentável, adotada em setembro de 2015 pela Organização das Nações Unidas (ONU), a qual traça um plano de ação para erradicar a pobreza, proteger o planeta e garantir que as pessoas alcancem a paz e a prosperidade.

No objetivo 17 da agenda, podemos dividir as metas relacionadas ao desenvolvimento sustentável em cinco eixos quais sejam: finanças, tecnologia, capacitação, comércio e questões sistêmicas. O eixo finanças tem o intuito de estimular a mobilização de recursos financeiros, com o fim de auxiliar os países em desenvolvimento. Além de propiciar o regime de promoção de investimentos para os países menos desenvolvidos, um dos mecanismos utilizados é a chamada assistência oficial ao desenvolvimento, que define percentuais mínimos da renda nacional bruta dos países desenvolvidos economicamente a serem direcionados para esta finalidade.

O eixo da tecnologia por sua vez trata-se da promoção do desenvolvimento, transferência, disseminação e difusão de tecnologias entre os países em condições favoráveis e inclusivas. O terceiro eixo, referente à capacitação visa implementar eficazmente em países em desenvolvimento, apoiando os planos nacionais para concretizar os objetivos de desenvolvimento sustentável, em seus diferentes setores. O eixo do comércio concerne à promoção de um sistema multilateral de comércio, mais equitativo, aberto e com maior participação dos países menos desenvolvidos sob o manto da Organização Mundial do Comércio (OMC). O último eixo trata das questões sistêmicas.

Neste sentido, o compliance permite um monitoramento e verificação de irregularidades ou descumprimento dos critérios legais, onde se admite mecanismos de coleta de informações, a fim de evitar riscos e promover a transparência dentro da organização. As informações importantes podem ser colhidas através de inspeção no local. Acompanhar sistematicamente o compliance é essencial para que se possa chegar a uma efetividade do mesmo.

Portanto, é necessária a realização de inspeções ou outras formas de fiscalização com o fim de se evitar eventuais processos judiciais, penalidades e consequências danosas a sociedade decorrente do descumprimento do ordenamento coorporativo ou legal.

3.1 COMPLIANCE TRABALHISTA: CONCEITOS E FERRAMENTAS

Como elucidado por Silva, Lima e Pinheiro (2022), um programa de compliance trabalhista é pontuado pela formação de medidas relativas aos controles internos da

organização, sempre prevendo os mecanismos de padronização e controle. Não existe um modelo único de compliance e cada empresário deverá desenvolver um programa adequado ao seu negócio. A doutrina costuma elencar nove ferramentas de implementação de um compliance trabalhista (ANDRADE; FERREIRA, 2017).

Vale ressaltar que o compliance de dados e, também, o compliance de dados trabalhista, lida diretamente com um complexo sistema, no qual, a lei, os contratos, a conduta dos agentes e de seus empregados, precisam estar em conformidade com os mecanismos de políticas, de controles internos, de código de ética e de conduta.

A primeira diz respeito ao comprometimento da alta administração da companhia ao programa a ser implementado, pois, quando estes não se comprometem, corre-se o risco de ocorrer o chamado *paper compliance*, ou seja, o compliance que existe apenas na teoria, não na prática. Essa ferramenta pode ser identificada no Código de Conduta como o conjunto de valores elencados pelos líderes da organização.

A segunda ferramenta se refere à gestão de riscos, que consiste em uma avaliação completa dos processos da organização, com a posterior classificação dos riscos e o estabelecimento de ordem de prioridade, avaliando o impacto e a probabilidade de eles ocorrerem. Um exemplo de matriz para mapear os processos e riscos é a matriz Gravidade X Urgência X Tendência, onde se atribuem valores de 1 a 5 para cada um dos elementos, que se multiplicam e geram um valor final para definir a prioridade de lidar com o impasse. O quadro 3 traz um exemplo de Matriz de avaliação de riscos:

Quadro 3 – Avaliação de riscos

Problema	Gravidade	Urgência	Tendência	Resultado GxUxT	Ordem de Priorização
Falta de controle no estoque	3	1	3	9	4º
Atraso na entrega do fornecedor	4	3	3	36	3º
Baixo índice de compra dos clientes	4	4	4	64	1º
Atraso na entrega de mercadorias	4	3	4	48	2º

Fonte: Elaborado pela Autora (2022).

No presente exemplo, pela multiplicação Gravidade X Urgência X Tendência, se vê que o problema “Baixo índice de compra dos clientes” está na ordem de prioridades desta empresa.

A terceira ferramenta são os códigos de conduta, que são definidos pelo Instituto Brasileiro de Ética nos Negócios (2019, p. 3) como:

> A declaração do conjunto de direitos, deveres e responsabilidades empresariais para com os *Stakeholders*, refletindo a cultura, os princípios e os valores, a atuação socioambiental e o conjunto das normas de conduta para dirigentes, executivos e colaboradores bem como para as empresas integrantes da cadeia produtiva, mediante os quais atuam as premissas que enriquecem os processos decisórios da empresa e orientam o seu comportamento. Além disto, deve ser o principal instrumento da Governança Corporativa e da gestão estratégica para se tornar um aliado das empresas no caminho que levará ao Desenvolvimento Sustentável.

Em quarto lugar, estão elencados os treinamentos e comunicações que têm como propósito o processo de conscientização sobre o programa de compliance da empresa também fazem parte das ferramentas, bem como em os Canais de Denúncias, quinto princípio, que devem seguir princípios como a neutralidade e o anonimato, servem para detecção de fraudes e assédios.

Além disso, o sexto princípio diz respeito as investigações internas podem apurar inconformidades, devendo sempre respeitar o sigilo e presunção de inocência, para que não seja ferida a imagem do trabalhador. Sétimo, a auditoria, vinculada aos fatos, documentos e situações passadas, e o monitoramento, vinculado ao momento presente da empresa, também configuram como ferramentas. Por último, a respeito de avaliação de fornecedores, o *Due Dilligence* se estabelece como ferramenta de verificação da existência do programa de compliance na empresa parceira. E em nono, a presença da ouvidoria.

Quanto às ferramentas, Jobim (2020) menciona que se apresentam “como uma colcha de retalhos que devem estar bem atados uns aos outros para que se transforme em um verdadeiro programa de compliance”.

3.2 ETAPAS DA IMPLEMENTAÇÃO DE UM PROGRAMA DE COMPLIANCE PARA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS

Como já explicitado anteriormente neste trabalho, há na relação de emprego a coleta de inúmeros dados do trabalhador, incluindo dados sensíveis. Essas informações não são apenas para a execução do contrato, mas para a firmação de obrigações legais. A respeito do assunto, Sanden (2014, p. 17) destaca que:

> As relações empregatícias são um importante palco para a realização de objetivos diversos, como a inclusão de determinados grupos no mercado de trabalho, o cumprimento de padrões no atendimento ao consumidor, a gestão da saúde ocupacional dos empregados e o pagamento de benefícios previdenciários a empregados ou a seus familiares. Normalmente, o empregador funciona como estação de trânsito das informações necessárias para a realização desses misteres. E, em ambiente marcado pelo uso das tecnologias da informação e da comunicação, todas essas informações, mesmo que fragmentárias, formam uma base de dados multifuncional que, por meio das operações de processamento, propiciam a exploração de acordo com as expectativas e as políticas empresariais e trazem o risco de fragilizar a posição do empregado e de prejudicá-lo.

O advento da tecnologia veio para facilitar a coleta de dados e o armazenamento dos mesmos. O respeito à LGPD não deve ser procurado pelas empresas apenas para evitar sanções, mas para preservar a imagem da companhia frente ao público geral. Ainda, a conformidade com a Lei possibilita e, por vezes, condiciona a celebração de negócios com empresas estrangeiras localizadas em países que possuem legislação de dados e exigem padrões mínimos de privacidade e proteção de dados pessoais para a transferência internacional, o que, consequentemente, aumenta o valor de mercado das organizações.

Um programa de implementação de compliance deve ser adequado ao porte da empresa, mas certos elementos devem estar sempre presentes: O programa de implementação inicia-se com uma mobilização das pessoas que serão envolvidas: pessoal interno, externo ou a contratação de novos profissionais para a viabilização da adoção das novas medidas. Uma figura importante no grupo de trabalho inicialmente formado para a implementação da LGPD é o Encarregado de Dados Pessoais, chamado de “DPO” (*Data Protection Officer*).

A norma o conceitua como sendo o “[...] canal de comunicação entre o controlador, titulares e a Autoridade Nacional de Proteção de Dados.” (art. 5º, VIII), ou

seja, o “elo de ligação” entre controlador[3], titulares e órgão regulatório, do qual deve-se realizar a sua indicação, podendo ser pessoa física ou jurídica, tendo em vista a inexistência de vedação legal para tanto, admitindo-se, inclusive, que tal função seja desempenhada de forma terceirizada ou por empregado, podendo, inclusive, que um mesmo encarregado atue para diferentes organizações. Não é demais ressaltar, de acordo com o art. 23, III, da LGPD, a figura do encarregado tem aplicação tanto para pessoas jurídicas de direito privado como para as de direito público, devendo os dados e a forma de contato deste sujeito de tratamento ser divulgadas publicamente e de maneira clara e objetiva, respeitando, assim, as determinações constantes do art. 41, §1º, da LGPD.

Alexandre Prata, citando o guia *DP&P Strategies Policies and Plans – Data Protection ad Privacy Guide,* de Kyrazoglou, propõe um ponto de partida para as tarefas do Encarregado:

> [...] desenvolver e manter políticas, normas e procedimentos; cuidar do cotidiano do programa de proteção de dados e privacidade; desenvolver e manter padrões de conduta relacionados a privacidade de dados; colaborar com comitês internos (ex: privacidade) e departamentos da empresa (gestão de risco, auditoria interna, RH etc.) para investigação e resolução de incidentes; interagir com o jurídico para resolução de questões legais relacionadas a privacidade de dados; investigar violações de privacidade de dados; monitorar iniciativas do negócio, tendências, vulnerabilidades, riscos etc.; comunicar com agências reguladoras e partes interessadas.

A fase inicial é de extrema relevância, porque é um momento em que deve ser introduzida uma mudança de cultura na companhia, sendo imprescindível que a alta gestão esteja envolvida e engajada com o projeto para que, de fato, isso ocorra. É importante que todos os setores da empresa estejam alinhados estrategicamente com essa nova política de compliance que está a ser implementada. Para isso, devem ser realizados treinamentos, *workshops* e palestras a respeito do tema, inclusive, trazendo casos internos da empresa, para que todo o processo se torne entendível e palpável. Neste caso, o encarregado deve alinhar as premissas com a alta administração, e supervisionar a aplicação do projeto.

Feita a avaliação inicial, é necessário analisar todo o conjunto de leis que deverá ser observado no tratamento dos dados pessoais, considerando que estar “de

[3] É um dos agentes de tratamento de dados, definido pela legislação como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

acordo” com a Lei Geral de Proteção de Dados” não significa cumpri-la, apenas, mas cumprir também outras normas setoriais, por exemplo: a Constituição Federal, a Consolidação das Leis Trabalhistas, as Convenções da Organização Internacional do Trabalho, as Normas Regulamentadoras expedidas pelas autoridades competentes, entre outras.

Após a mobilização, finda a fase de conscientização e avaliação inicial, passa-se à próxima fase: o mapeamento de dados. Deve ser feito o inventário de dados, chamado de “*data mapping*”, para que sejam mapeados todo os dados que são tratados na empresa. Concluídas as etapas iniciais de mobilização e mapeamento de dados, deve ser elaborado um plano de ação para a implementação do programa, de acordo com a realidade encontrada na fase inicial anteriormente descrita. O Comitê Executivo de Privacidade e Proteção dos Dados Pessoais deve acompanhar esse plano, de forma a avaliá-lo e adequá-lo periodicamente. É importante que as ações sejam documentadas para que, em eventual fiscalização, a empresa possa demonstrar as medidas adotadas para cumprir a LGPD.

A importância da documentação de todas as etapas de implementação do programa não é destacada apenas para que o Comitê tenha esse controle, mas também porque a Autoridade Nacional de Proteção de Dados Pessoais pode exigir que o controlador apresente o Relatório de Impacto de Proteção de Dados, com o objetivo de avaliar o cumprimento da lei.

As empresas de pequeno e médio porte nem sempre irão conseguir implementar um programa completo de Compliance, porém, dentro das suas possibilidades, devem adotar medidas no sentido de inserir a cultura de privacidade e o cumprimento da Lei Geral de Proteção de Dados Pessoais nas suas atividades.

4 COMPLIANCE TRABALHISTA E A ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS

Como visto, uma das inovações trazida pela adoção de legislações de proteção de dados foi a conexão de institutos legais internos com práticas de compliance. O sistema de gestão de compliance de dados aparece na legislação como expressão do princípio da *accountability* e como meio de proteção dos direitos subjetivos/fundamentais de dados. No âmbito da legislação comparada, se tem a *General Data Protection Regulation* (GDPR) da União Europeia. No caso do Brasil, se está falando da Lei Geral de Proteção de Dados (LGPD), Lei nº. 13.709, de 14 de agosto de 2018. De acordo com Saavedra (2020):

> Compliance consiste em um estado dinâmico de conformidade a uma orientação normativa de comportamento com relevância jurídica por força de contrato ou lei, caracterizado pelo compromisso com a criação de um sistema complexo de políticas, de controles internos e de procedimentos, que demonstrem que a empresa está buscando “garantir”, que se mantenha em um estado de compliance.

Segundo o autor, para garantir esse estado de compliance deve ser realizado um Sistema de Gestão de Compliance, que é composto de *Data Assessments*, sendo que a doutrina lista quatro principais: 1) *Risk Assessment* (Análise de riscos); 2) *Data mapping*: Inventário e registro de dados; 3) *Privacy Impact Assessment* (PIA); e 4) *Data Protection Impact Assessments* (DPIA). Esses *assessments* têm papel fundamental na implantação de um Sistema de Gestão de Compliance de Dados.

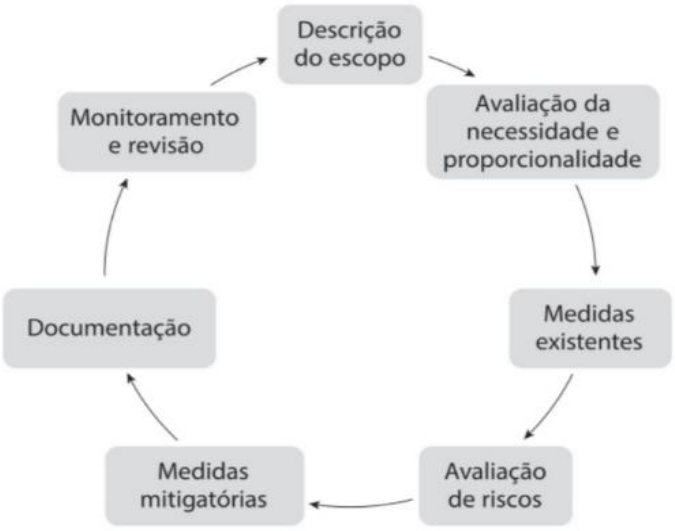
A avaliação de riscos é elemento essencial de qualquer sistema de gestão de compliance, pois o compliance tem, na verdade, o risco como seu objeto de análise. Analisar e gerenciar riscos é a razão de existência de sistemas de gestão de compliance. De maneira geral, existem, basicamente, duas metodologias aceitas mundialmente como referência de melhores práticas de gestão de riscos: 1) COSO *Enterprise Risk Management* (COSO-ERM), criada pelo *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) e 2) a ISO 31.000.

As referidas metodologias são constituídas de algumas etapas fundamentais: 1) conhecer a empresa; 2) conhecer seu ambiente legal e suas obrigações de compliance; 3) realizar entrevistas e análise de documentos; 4) fazer testes e checagem dos dados levantados; 5) identificar riscos e fatores de risco; 6) realizar

avaliação de probabilidade; 7) desenvolver matriz de riscos; 8) realizar monitoramento.

Já o *data mapping* tem por função principal identificar os dados que transpassam vários sistemas e, em função disso, serve para indicar como os dados estão compartilhados, organizados e onde eles estão localizados. Um PIA (*Privacy Impact Assessment*) é uma análise dos riscos de privacidade e proteção de dados associada ao "processamento de informação pessoal em relação a um projeto, produto ou serviço." (DENSMORE, 2019, p. 69). Por último, o DPIA (*Data Protection Impact Assessments*) descreve "o processo designado para identificar riscos, que surgem do processamento de dados pessoais e para minimizar esses riscos o máximo e o mais rápido possível" (SAAVEDRA, 2020). No caso da GDPR, não estar em conformidade com as exigências da DPIA pode levar à aplicação de multas, que serão impostas à autoridade de dados da empresa ou organização. No esquema apresentado na Figura 1, Saavedra (2020) exemplifica o ciclo DPIA:

Figura 1 – Ciclo DPIA



Fonte: Bioni (2020).

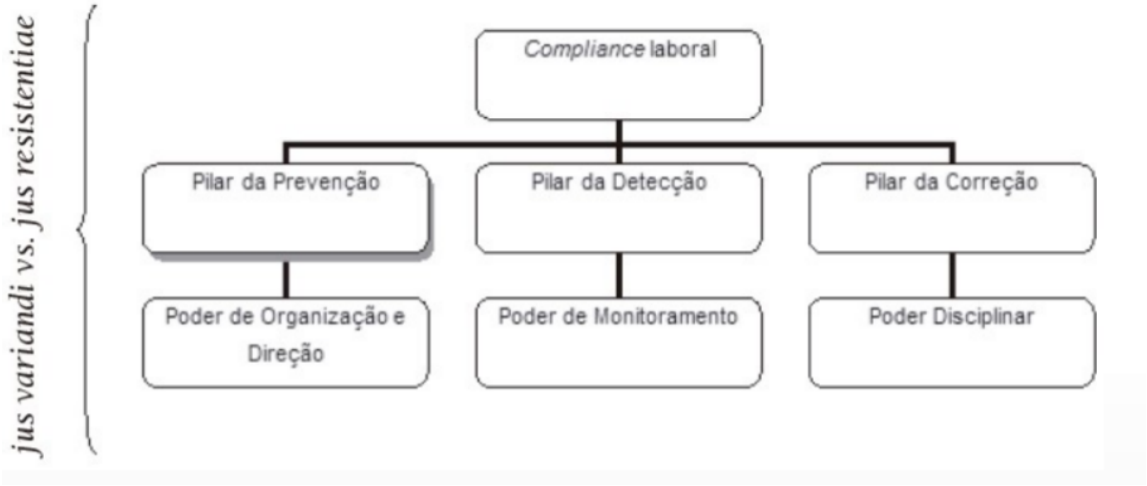
O Sistema de Gestão de Compliance de Dados é construído a partir das metodologias referidas no capítulo anterior: após a realização de uma avaliação de risco de dados, do *data mapping*, do PIA e do DPIA, passa-se a ter informações suficientes para elaborar um projeto de implementação de Compliance de Dados. As legislações exigem, porém, que uma determinada metodologia seja aplicada no

momento da implementação do Compliance de Dados: o *Privacy by Design* (PbD). Segundo Saavedra (2020):

> O Privacy by Design framework reza que privacidade e proteção de dados estão intrinsecamente ligadas com todo o ciclo de vida das tecnologias, do desenho inicial até o seu lançamento no mercado. O seu conceito fundamental implica que as organizações devem sempre criar produtos e serviços, que, desde o início, estejam de acordo com as diretrizes de um sistema de gestão de compliance digital ou de dados, bem como das melhores práticas de Compliance de dados e que essas medidas sejam aplicadas diretamente nas tecnologias, nos sistemas e nas práticas vinculadas a todo o ciclo de vida dos produtos e serviços das organizações e empresas.

Conforme estabelece Jobim (2018), o compliance possui três pilares: prevenção, detecção e correção. A autora ainda destaca que é possível fazer um paralelo entre os pilares que orientam a aplicação de programas de compliance e os três poderes abrangidos pelo poder diretivo, que são o poder de organização e direção; poder de monitoramento e poder disciplinar, conforme ilustrado na Figura 2.

Figura 2 – Pilares do Compliance



Fonte: Jobim (2018).

O compliance, na legislação trabalhista, visa cumprir com a função social da empresa, que, de acordo com Silva, Pinheiro e Bonfim (2021), resulta na observância aos percentuais estabelecidos em lei, voltados para a inclusão social, na urbanidade ao tratar com os funcionários, na garantia de condições salubres e na diminuição dos riscos inerentes ao trabalho, respeitando os direitos trabalhistas e jamais atuando de forma discriminatória.

O *caput*, do art. 2º, da Consolidação das Leis Trabalhistas dispõe que “considera-se empregador a empresa, individual ou coletiva, que, assumindo os riscos

da atividade econômica, admite, assalaria e dirige a prestação pessoal de serviço.” (BRASIL, 1948). Além do conceito de empresa, extrai-se do dispositivo a premissa de que o empregador é responsável pelos riscos do negócio, o que também fundamenta o poder diretivo do empregador. Considerando esta premissa, o compliance é uma forma de garantir o cumprimento das normas trabalhistas e, também, pode ser utilizado para demonstrar em Juízo cometimento de falta grave e dos procedimentos adotados.

A legislação trabalhista brasileira dispõe, basicamente, três tipos de sanções em caso de cometimento de ato faltoso pelo empregado: advertência, suspensão disciplinar e ruptura do contrato de trabalho por justa causa. Especificamente quanto à justa causa, cumpre frisar que se trata de medida extrema que macula a vida profissional do trabalhador, pelo estigma que carrega essa ruptura e pelo grau de desonra que a justa causa costuma envolver, razão pela qual, acertadamente, os Tribunais entendem que é ônus do empregador comprovar de prova robusta o cometimento de falta grave pelo empregado despedido, no teor do artigo 818 da CLT. Sendo do empregador o ônus *probandi*, novamente o compliance se demonstra como ferramenta necessária não apenas para evitar o cometimento do próprio ato faltoso pelo empregado, uma vez que implica em fornecimento de informações e treinamentos visando à observância aos princípios e procedimentos da empresa, como pode ser utilizado para demonstrar em Juízo o cometimento de falta grave e dos procedimentos adotados. Relembra-se que algumas práticas ilegais que podem ser observadas no meio ambiente de trabalho, como atitudes discriminatórias, assédio moral e sexual, devem ser rechaçadas pela organização, sendo mister uma postura rígida com atitudes contrárias ao código de ética estabelecido pela empresa e direitos fundamentais dos trabalhadores.

A existência de um programa de compliance, que institua medidas correcionais efetivas, demonstra o comprometimento da empresa com o bem-estar da comunidade empresarial e valida, portanto, a aplicação de medida disciplinar proporcional à gravidade do ato cometido, coibindo a reiteração das condutas consideradas faltosas por parte dos demais empregados. Ao implantar um programa de compliance, também se faz necessário o detalhamento do procedimento disciplinar a ser utilizado pela empresa quando da apuração de ato contrário à legislação ou às normas internas da empresa, o que demonstra a observância ao critério de aplicação disciplinar de acordo

com os limites impostos pela doutrina (previsão legal, atualidade ou imediatidade da falta, nexo de causalidade entre a falta e a punição, proporcionalidade e gravidade da pena aplicada em relação ao ato faltoso). Ressalta-se que o detalhamento das condutas envolvidas no exercício do poder disciplinar é tão importante que a Controladoria-Geral da União editou o “Manual de Direito Disciplinar para as empresas estatais”.

Há uma tendência jurisdicional em aceitar justas causas baseadas em programas de compliance com detalhamento do procedimento disciplinar, que demonstrem o respeito do empregador pelo direito à intimidade, à privacidade, ao contraditório, à ampla defesa, entre outros direitos do empregado, legitimando a medida disciplinar aplicada. Nesse sentido, traz-se os seguintes julgados:

> JUSTA CAUSA. VIOLAÇÃO DO CÓDIGO DE ÉTICA DA RECLAMADA. Com efeito, a justa causa consiste em sanção de natureza gravíssima, que implica repercussões danosas ao trabalhador, de ordem pessoal, social e profissional, hábeis a macular de forma indelével a vida do trabalhador, causando-lhe dificuldades de reinserção no parco mercado de trabalho. Por essa razão, a sua aplicação pressupõe a prova da concorrência de requisitos inafastáveis, a saber: a previsão legal; a atualidade ou imediatidade da falta; o nexo de causalidade entre a falta e a punição; bem como a proporcionalidade e a gravidade da pena aplicada. Violado pelo empregado, por mais de uma vez, o Código de Ética da reclamada no que diz respeito ao recebimento de presentes, caracterizada a falta grave apta a justificar a penalidade. (TRT-17 – RO: 00011460620165170006, Relator: Gerson Fernando da Sylveira Novais, Data de Julgamento: 07.11.2017, Data de Publicação: 17.11.2017).

> JUSTA CAUSA. CONFIGURAÇÃO. Restando configurado nos autos que o empregado, não obstante esteja ciente das normas internas da empresa, deixa de cumpri-las e, em razão de tal fato advém prejuízos a empregadora, com a quebra da fidúcia inerente ao contrato de trabalho, há de ser mantida a justa causa aplicada pela empregadora. Recurso ordinário conhecido e provido” (TRT-16 00189376120165160023 0018937-61.2016.5.16.0023, Relator: Jose Evandro de Souza, Data de Publicação: 16.05.2019).

No aspecto, merece especial atenção a fundamentação do acórdão proferido nos autos do processo 0001146-06.2016.5.17.0006, que manteve a despedida por justa causa em razão da violação ao código de ética da empresa reclamada:

> No presente caso, é incontroverso que o reclamante recebeu de cliente da reclamada diversas recargas para seu celular pessoal, dentro da loja da reclamada. A controvérsia está apenas no motivo que teria levado o cliente da reclamada a recarregar o celular do autor. Fato é que a prática de aceitar presente de cliente fere o código de ética da reclamada, seja qual for o motivo do presente. A reclamada comprovou que o reclamante recebeu cópia de seu código de ética, em que consta: Brindes e gratificações Aceitar brindes e

> gratificações pode gerar um conflito ou aparentar um conflito entre interesses pessoais e responsabilidade profissional. A cultura do Walmart é de nunca aceitar brindes ou gratificações de qualquer fornecedor, fornecedor em potencial, representante do governo ou qualquer pessoa que o associado tenha motivos para crer que esteja buscando influenciar transações ou decisões de negócios. Os associados também não podem aceitar brindes ou gratificações de um cliente pelo trabalho realizado dentro das unidades do Walmart, exceto se houver tal exigência em alguma política local. Não podemos aceitar itens doados ao Walmart por fornecedores com o propósito de levantar fundos para caridade ou organizações não governamentais. Também nunca devemos pedir, aceitar ou aprovar doações de fornecedores em nome do Walmart. Além disso, os associados não devem fornecer listas de nossos fornecedores a organizações de caridade com o objetivo de arrecadação de fundos. Nossa cultura de recusar brindes e gratificações vem ao encontro dos nossos valores de transparência e objetividade e do nosso princípio de manter Custo baixo Todo Dia, já que tais brindes aumentam o custo de realizar negócios. Com essa postura, ajudamos nossos fornecedores a nos oferecer produtos a custos mais baixos, o que nos permite vender por menos para nossos clientes. Reconhecemos que, como uma empresa global, podemos nos deparar com situações em que as práticas locais devem ser levadas em consideração. O Departamento de Ética Local, em conjunto o Escritório Global de Ética, analisará essas situações caso a caso. Quando você estiver estabelecendo uma nova relação de negócios, garanta que todas as partes estejam cientes de nossa política de brindes e gratificações. Em alguns países onde a troca de presentes é um costume ou tradição, você deve explicar educadamente essa política a seus clientes e fornecedores, especialmente antes de datas comemorativas, quando a troca de presentes é tradicional, para deixar claro nosso posicionamento. DIGA APENAS... Não, obrigado. Portanto a reclamada possui um Código de Ética que é claro ao expressar a proibição de recebimento de qualquer tipo de brinde, presente ou gratificação de qualquer valor e o reclamante confessa que violou tal política por diversas vezes, tendo recebido de cliente diversas recargas de celular, sendo, portanto, irrelevante para a aplicação da justa causa o motivo do autor ter aceitado tais presentes. Em razão da reiterada atitude do reclamante, entendo que o critério da gradação da penalidade também foi aplicado no presente caso. [...] O autor tinha pleno conhecimento de toda a política descrita no código de ética da reclamada. Assim sendo comprovada que a atitude do reclamante se enquadra nas alíneas a e b do artigo 482 da CLT (LGL\1943\5 *apud* TRT-17 – RO: 00011460620165170006, Relator: Gerson Fernando da Sylveira Novais, Data de Julgamento: 07.11.2017, Data de Publicação: 17.11.2017).

O exame detalhado dos efeitos da LGPD no contrato de trabalho demonstra, de forma inegável, a sua relevância na seara laboral. Será necessário, por conseguinte, que se passe a adotar diversos ajustes no tratamento de informações dos empregados pelo empregador, para salvaguardar seus dados gerais e, especialmente, os sensíveis. Conclui-se, assim, que o descumprimento desse dever ensejará, inefavelmente, o direito do empregado a reparações variadas, em especial a indenização por danos morais, de acordo com os parâmetros contidos na própria LGPD, mais especificamente nos artigos 42 a 44.

Nos termos do artigo 42 da LGPD, 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. A fim de assegurar a efetiva indenização ao titular dos dados, 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 se equipara ao controlador.

Por sua vez, o art. 43 da LGPD estipula que os agentes de tratamento só não serão responsabilizados quando provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído; que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. Ademais, na forma do art. 44 da LGPD, o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: o modo pelo qual é realizado; o resultado e os riscos que razoavelmente dele se esperam; as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Responde, ainda, pelos danos decorrentes da violação da segurança dos dados, o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas na LGPD, der causa ao dano. Há, igualmente, previsão do trâmite da ação de reparação por danos, pelos §§ 2º a 4º, do art. 42, da LGPD, com possibilidade de inversão do ônus da prova a favor do titular dos dados, quando o juízo entender verossímil a alegação e houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

Urge destacar, por derradeiro, a existência de acalorada cizânia doutrinária acerca da modalidade de responsabilização da empresa pelo descumprimento das diretrizes da LGPD, se subjetiva ou objetiva. Silva, Pinheiro e Bomfim (2020, p. 19-20) analisam a questão da seguinte forma:

> Os artigos 42 a 45 da Lei 13.709/18 tratam da responsabilidade civil patrimonial e extrapatrimonial dos agentes de tratamento de dados (controlador e operador). Há forte tendência doutrinária em se adotar apenas a responsabilidade subjetiva, com culpa presumida e, via de consequência, em afastar o entendimento de responsabilidade civil objetiva do empregador, por aplicação do artigo 42 e incisos II e III do artigo 43 da LGPD, que expressamente isenta de responsabilidade aquele que não violou a lei. A

> exceção se faz às relações de consumo, pois excluídas pelo artigo 45 da Lei 13.709/18. 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. Entretanto, mesmo antes do Código Civil (parágrafo Doutrina e aplicabilidade no âmbito laboral 165 único do art. 927) a jurisprudência já vinha alargando o conceito de "culpa", cujo requisito é necessário para o dever de indenizar. A culpa presumida nasce da premissa do dever de que todos temos de não prejudicar ninguém e praticar atos com segurança. Ainda que não se confunda com a culpa presumida, a atividade de risco é mero desdobramento dessa tese, pois a pessoa que explora economicamente a atividade de risco deve ser responsabilizada pelos prejuízos materiais e morais daí decorrentes. Por isso e considerando que a LGPD (lei especial) não trouxe a culpa como elemento necessário para configuração de responsabilidade, defendemos que, em tese, é possível a aplicação da responsabilidade objetiva.

Na seara trabalhista, o compliance traz inúmeros benefícios, reduzindo problemas de assédio moral ou sexual, coibindo condutas inadequadas por parte dos empregados e impondo a todos os integrantes da corporação um código de conduta pautado na ética empresarial, evitando o ajuizamento de demandas trabalhistas, multas administrativas, entre outras situações que podem gerar custos ao empregador.

4.1 RISCOS E BENEFÍCIOS DE UMA IMPLEMENTAÇÃO SINCRÔNICA E DIACRÔNICA

O compliance, como ferramenta de aplicação da Lei Geral de Proteção de Dados, requer especialistas em cada uma das áreas do Direito (administrativo, penal, tributário, trabalhista e etc.). No âmbito trabalhista, principalmente devido a sua função social e de tutela, exige uma equipe extremamente especializada. Conforme já explicitado neste trabalho, embora cada programa de compliance tenha a sua especificidade, sempre terão a mesma forma.

Montoya Melgar (2018) defende a autonomia do Direito do Trabalho, pois que atendidas as condições necessárias, quais sejam: 1) o objeto ou a matéria social sobre os quais versa a regulamentação desta área jurídica seja um de conteúdo particular bem definido; e 2) que seja, ao mesmo tempo, um objeto relevante o bastante para exigir um Direito próprio e que essa matéria social seja disciplinada por um verdadeiro sistema normativo, com princípios peculiares e instituições especialmente adaptadas ao objeto regulado, princípios e instituições que nenhum outro ramo do Direito possa incorporar.

Este trabalho se propõe a responder um questionamento: “Como o compliance trabalhista abarca o compliance digital no que diz respeito à proteção de dados?”. Ora, deve-se lembrar que grande parte dos dados de uma empresa diz respeito a seus trabalhadores. Ainda, a LGPD está causando uma grande mudança no conceito de direitos fundamentais, transformando o sistema jurídico brasileiro. Defende-se, portanto, que o programa de adequação à LGPD, no âmbito trabalhista, diz respeito principalmente aos dados dos trabalhadores.

4.2 COMPLIANCE DE DADOS DOS EMPREGADOS E O COMPLIANCE TRABALHISTA

A LGPD prevê, em seu art. 5º, I, que dado pessoal é a informação relacionada à pessoa natural identificada ou identificável. A Lei ainda difere o dado pessoal em uma subespécie: dado pessoal sensível, que consiste no dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou 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. Pode-se considerar que dados são fatos brutos que, quando processados e organizados, convertem-se em algo inteligível, podendo ser deles extraída uma informação (DONEDA, 2019, p. 152).

A coleta de dados por si só não teria nenhuma relevância social ou econômica, se não fossem extraídas dali informações pertinentes, como, por exemplo, dados do E-Social, vínculos empregatícios, contribuições previdenciárias, folha de pagamento, comunicações de acidente de trabalho, aviso prévio, escriturações fiscais, informações sobre o FGTS, entre outros. Importante ressaltar que o banco de dados, no âmbito trabalhista, perdura em todas as fases do contrato, pré e pós contratual.

O tratamento de dados de empregados pode ser utilizado para fins diversos, desde o cumprimento de serviços legais até mapeamento de perfil. Quando se reúne esse arcabouço de informações, forma-se um verdadeiro dossiê de empregados e familiares e quando se pensa na facilidade com que essas informações podem ser compartilhadas lícita ou ilicitamente, é indispensável que medidas sejam adotadas para restringir o acesso a esses dados.

O art. 6º da Lei Geral de Proteção de Dados trata dos princípios que deverão ser observados no tocante à proteção de dados, sendo eles o da finalidade, da adequação, da necessidade, do livre acesso, da qualidade, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização. Os princípios ali dispostos visam tutelar a liberdade, a privacidade e a autodeterminação informativa, princípios esses presentes na Carta Magna de 1988, que declara como direitos fundamentais do cidadão a inviolabilidade de sua privacidade, a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.

Em análise mais profunda dos princípios que norteiam o ordenamento brasileiro, se pode observar os direitos da personalidade enumerados no Código Civil (CC), como direito ao nome, à imagem, à liberdade, à honra, à integridade física e etc. Vale ressaltar que não se limitam àquelas situações previstas no CC, sendo o seu rol *numerus apertus* (rol aberto), ou seja, eles não se exaurem naquelas espécies enumeradas nos arts. 11 a 21 do CC.

No ordenamento justrabalhista, encontram-se diversas normas protetoras do direito à identidade do empregado. Com bem ressalta Delgado (1999, p. 5), o “dano moral decorrente da violação da intimidade, vida privada, honra e imagem das pessoas – e sua respectiva indenização reparadora – são situações claramente passíveis de ocorrência no âmbito empregatício”.

Parece, sem dúvida, que a noção de consentimento, entendido como uma manifestação de vontade livre, específica e informada, é um conceito de difícil concretização e de difícil preenchimento no contexto de uma relação de trabalho. Na verdade, não se pode esquecer que o Direito do Trabalho surgiu como um ramo do Direito que pretendia proteger os trabalhadores perante os arbítrios do empregador, sendo que a história laboral do Direito é, em boa medida, a dos limites aos poderes dos empregadores com o fim de proteger socialmente os trabalhadores. A sua autonomização alicerça-se na tentativa de superar as insuficiências da aplicação do Direito Civil às relações contratuais laborais, onde a igualdade das partes era meramente formal. E se, inicialmente, a resposta passou pela consagração de determinados direitos coletivos, máxime, a liberdade sindical, ligada à ideia da despersonalização que acompanhou o trabalho na Revolução Industrial, rapidamente se começou a entender que os direitos dos trabalhadores poderiam ser ameaçados

através de outras formas e meios, nomeadamente através da violação dos direitos de que era titular enquanto pessoa.

A relação laboral assenta, como é comumente aceite, na ideia de que as partes envolvidas não se encontram em pé de igualdade, apresentando-se o empregador como a parte contratual mais forte, dotada de um poder de conformação da prestação a que o trabalhador está submetido. Este, quando celebra um contrato de trabalho, aliena uma parte da sua autonomia e da sua liberdade, sendo colocado numa situação de dependência perante o empregador, que não se configura somente na ótica jurídica, mas também, quase sempre, na perspectiva econômica.

Em primeiro lugar, tem-se, desde logo, o fato de que surgiram e continuam a surgir novas tecnologias extremamente invasoras da privacidade das pessoas, em geral, e dos trabalhadores, em especial. Além disso, surgem, a todo o momento, tecnologias de seguimento dos trabalhadores e das suas comunicações eletrônicas que podem violar sua privacidade. Esse monitoramento pode infringir os direitos de privacidade dos trabalhadores, independentemente dele ocorrer de forma sistemática ou ocasional. O risco não se limita à análise do conteúdo das comunicações. A análise de metadados sobre uma pessoa pode permitir um monitoramento detalhado, igualmente invasivo da privacidade, da vida e até dos padrões de comportamento de um trabalhador.

Outro aspecto extremamente relevante é a granularidade do consentimento, que se aplica na hipótese de coleta de diversos documentos com finalidades distintas. Ainda que sem essa denominação expressa na LGPD, a granularidade é um atributo aplicável nas situações de coleta de vários dados com finalidades distintas e é capaz de garantir a efetiva liberdade do consentimento (art. 5º, XII). A granularidade do consentimento pressupõe a indicação pontual, tanto dos dados aos quais se consente o tratamento, quanto ao fim específico desse tratamento, o que se opõe ao consentimento generalista (art. 8º, 4º). Com isso, inibem-se práticas “tudo ou nada”, que conduzem o titular dos dados a permissões além das quais seriam necessárias e ferem, inclusive, o Princípio da Necessidade (art. 6º, III).

A empresa deve observar, também, que a obtenção do consentimento não lhe permite compartilhar dados com outros controladores sem a obtenção de consentimento específico para tanto, conforme teor do art. 7º, § 5º, da LGPD. Esse destaque é de extrema importância para o âmbito das relações de trabalho, porque

muitos dados são compartilhados pelo empregador com planos de saúde, previdência privada e empresas terceirizadas.

Portanto, imprescindível a implementação de mecanismos de boas práticas, que envolve uma (re)organização interna, além da criação de novos procedimentos internos, com a consequente elaboração de documentos em conformidade com a Lei Geral de Proteção de Dados.

4.3 O COMPLIANCE TRABALHISTA COMO INSTRUMENTO PARA A PROTEÇÃO DE DADOS PESSOAIS DO TRABALHADOR

Os dados pessoais e sensíveis refletem múltiplas expressões da personalidade do trabalhador, eles têm valor e definem os rumos da atividade empresarial e laboral. Para que os dados pessoais e sensíveis do trabalhador não sejam utilizados indevidamente como ferramenta de fiscalização pelo empregador, ultrapassando a esfera profissional e atingindo a esfera da personalidade do trabalhador, potencialmente maculando seus direitos de proteção à vida privada, é necessária a reafirmação da privacidade como direito fundamental da pessoa trabalhadora. Conforme ensina Doneda (2019):

> Se hoje a privacidade e a proteção dos dados pessoais são assuntos na pauta cotidiana do jurista, isto se deve a uma orientação estrutural do ordenamento jurídico com vistas à atuação dos direitos fundamentais, tendo como pano de fundo o papel do desenvolvimento tecnológico na definição de novos espaços submetidos à regulação jurídica.

Com a evolução da tecnologia e a internet cada dia mais presente na vida das pessoas, novas questões surgem ao mundo do Direito, não sendo exceção ao Direito do Trabalho. Nesse sentido, Dacheri e Feuser (2019) ponderam:

> Juntamente com toda a evolução desencadeada com a intersecção trabalho e tecnologia, importantes questionamentos circundam a matéria que baliza as relações sociais e laborais, atuais e principalmente futuras, ao ponto de se indagar se todo esse avanço estaria fazendo bem para a saúde psicológica do ser humano trabalhador, enquanto detentor de direitos sociais, bem como se isso vem respeitando a dignidade humana ou se, novamente, há mitigação de direitos fundamentais trabalhistas.

A CLT prevê normas expressas sobre direitos de personalidade, como verifica-se nos arts. 482, alínea “j”, e 483, alínea “e”, que consideram motivo justo para resolução do contrato de trabalho a lesão à honra e à boa fama.

Uma das dificuldades que pode surgir a partir da vigência da LGPD, em agosto de 2020, é sair do âmbito da teoria e aplicar, no cotidiano da empresa, as disposições legislativas inseridas pela Lei, bem como se adequar aos princípios nela previstos. Para tanto, a empregadora pode se valer de programas de compliance, cujo objetivo é justamente a prevenção, a mitigação de problemas, a partir da análise de riscos e da adequação à legislação pátria e estrangeira.

A entrada em vigor da LGPD, além de conferir maior segurança jurídica no tratamento de dados pessoais, também é uma inovação jurídica na maneira como a própria sociedade lida com esses dados, resultando no surgimento de novos desafios. O compliance trabalhista, portanto, é um instrumento apto a proteger os dados pessoais do trabalhador, pois limita a atuação dos dirigentes e responsáveis aos códigos de ética e conduta, que, por sua vez, estabelecem limites para a coleta e tratamento desses dados na contratação, no curso e no término do contrato de trabalho.

Conforme exposto, o compliance está intrinsecamente ligado ao gerenciamento do risco da atividade, na medida em que este é mitigado por meio de programas de prevenção, observância a códigos de condutas e aos procedimentos de uma corporação. Os pilares do compliance (prevenção, detecção e correção) aproximam-se do poder diretivo, na medida em que este é constituído pelo poder de organização e direção, poder de monitoramento e poder disciplinar. Nesse contexto, a mitigação dos riscos do negócio é efetivada com a implementação de um programa de compliance, devendo a empresa ter especial cuidado no que tange ao exercício do poder disciplinar.

A aplicação do compliance como parte do poder de organização e direção de uma empresa é pacífica e se relaciona com o cumprimento da função social da empresa, comprometimento com as normas de saúde e segurança do empregado, entre outros aspectos inerentes à administração empresarial. Quando se aplica o pilar da detecção enquanto poder de monitoramento, há de se ter um cuidado para não violar os direitos de personalidade do trabalhador, em especial a privacidade e a intimidade, o que pode ocorrer mesmo na fase pré-contratual, por meio de perguntas abusivas numa entrevista de emprego. No entanto, é no exercício do poder disciplinar que, muitas vezes, as empresas, mesmo agindo de acordo com a legislação, têm seus atos invalidados perante a Justiça do Trabalho em razão do seu caráter mais, o que

poderia ser evitado, contudo, com a demonstração de um forte programa de compliance.

O Brasil experimenta um incremento legislativo a partir da aprovação do direito fundamental à proteção dos dados pessoais. Tal visa imprimir maior vigor à LGPD. Na seara trabalhista é muito importante que sejam respeitados os direitos do trabalhador, pois os dados laborais, identitários, sindicais e, por vezes, dados de saúde, também são considerados sensíveis e, caso vazem, poderão causar situações de discriminação. Por tal motivo, é importante que as empresas promovam a sua adequação à LGPD. A prevenção é extremamente positiva, pois assinala o compromisso com as boas práticas, o que é levado em conta tanto no âmbito administrativo como no judiciário, caso haja algum revés.

5 CONSIDERAÇÕES FINAIS

Como visto, a recente vigência da LGPD e a tutela de proteção de dados pessoais tem gerado muitas discussões no ordenamento jurídico pátrio, incluindo o questionamento acerca da incidência da LGPD nas relações de trabalho para a proteção dos dados pessoais dos trabalhadores e o instrumento mais adequado para concretizar e efetivar esse direito. Levando em consideração a existência de um fluxo informacional na relação trabalhista, desde a contratação até a extinção do contrato de trabalho, e a importância dos direitos e princípios veiculados.

A LGPD traz a necessidade de uma mudança de cultura, na era digital em que se vive no século XXI: a invasão da privacidade, com publicização e comercialização dos dados pessoais de terceiros, sem o consentimento ou sequer a ciência delas, tornou-se prática generalizada neste mundo virtual. É fundamental, por conseguinte, valer-se dos princípios e diretrizes da LGPD para se impor, na seara laboral, objeto do presente estudo, limites a essa possível invasão de dados pessoais dos empregados, impondo às empresas o dever de tratar esses dados de forma prudente e cautelosa, sob pena de responsabilização, inclusive, por meio de eventual indenização por danos morais causados aos trabalhadores.

Neste trabalho, pretende-se responder a seguinte pergunta: “É possível implementar um programa de Compliance para adequar as empresas à Lei Geral de Proteção de Dados com relação aos seus empregados?”

Através do problema de pesquisa, chega-se à seguinte hipótese: É possível a implementação da Lei Geral de Proteção de Dados por conta de uma obrigação legal das empresas com seus empregados, o que pode ser feito através de um programa de Compliance Data.

Através deste trabalho, verificou-se que é possível a aplicação de um programa de Compliance Data para que seja implementada a Lei Geral de Proteção de Dados no âmbito trabalhista.

Na primeira parte do trabalho, traçou-se um panorama geral da Lei Geral de Proteção de Dados, comparando-a com o Regulamento Geral de Proteção de Dados Pessoais Europeu (GDPR), frisando aspectos gerais da lei e sua incidência nas relações de trabalho. Na segunda parte, abordou-se o conceito de compliance e suas

ferramentas, bem como as etapas de implementação de um programa de compliance. Por último, foram apresentados os riscos e benefícios de uma implementação sincrônica e diacrônica da LGPD, por conseguinte, compliance de dados do empregador e a proteção de dados do trabalhador como direito fundamental.

REFERÊNCIAS

BARZOTTO, Luciane Cardoso. Negociação coletiva e LGPD. *In:* BARZOTTO, Luciane Cardoso; COSTA, Ricardo H. Martins (Orgs.). **Estudos sobre LGPD – Lei Geral de Proteção de Dados – Lei nº 13.709/2018**: Doutrina e aplicabilidade no âmbito laboral. Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4ª Região, 2022.

BIONI, Bruno. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Grupo Gen, 2020. *E-book.* Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 29 jun. 2022.

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

BRASIL. (CLT [1948]). **Decreto-Lei nº 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 05 jun. 2022.

BRASIL. (Constituição [1988]). **Constituição da República Federativa do Brasil.** Brasília, DF, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 jul. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l3709.htm. Acesso em: 06 jun. 2022.

CALCINI, Ricardo; ANDRADE, Dino Araújo de. Impactos da LGPD nas relações de trabalho. **Consultor Jurídico,** São Paulo, 11 fev. 2021. Disponível em: https://www.conjur.com.br/2021-fev-11/pratica-trabalhista-impactos-lgpd-relacoes-trabalho. Acesso em: 04 jul. 2022.

DACHERI, Emanueli.; FEUSER, Marja Mariane. O teletrabalho e as principais críticas diante da reforma trabalhista. *In:* CONGRESSO NACIONAL DO CONPEDI, 27. **Anais...** Porto Alegre, 2019.

DELGADO, Maurício Godinho. Direitos da personalidade (intelectuais e morais) e contrato de emprego. **Revista Síntese Trabalhista,** Porto Alegre, n. 125, p. 5-12, nov. 1999.

DELGADO, Mauricio Godinho. Direitos fundamentais na relação de trabalho. **Revista de Direitos e Garantias Fundamentais**, São Paulo, n. 2, p. 13-14, 2007. Disponível em: http://sisbib.emnuvens.com.br/direitosegarantias/article/view/40. Acesso em: 11 maio 2022.

DENSMORE, Russell. **Privacy program management:** Tools for managing privacy within your organization. Portsmouth: Hyde Park Publishing Services/IAPP, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006.

FRANCO FILHO, Georgeonor de Sousa. **Direito do trabalho no STF**: N. 23/24**.** São Paulo: LTr, 2021.

INSTITUTO BRASILEIRO DE ÉTICA NOS NEGÓCIOS. **Programa de integridade e conduta.** Campinas, 2019. Disponível em: http://eticanosnegocios.org.br/wp-content/uploads/2019/02/Apresentacao-PIC-Programa-de-Integridade-de-Conduta.pdf. Acesso em: 02 jun. 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION – ISO. **Norma nº 19600: sistemas de gestão de compliance**. rio de janeiro: abnt, 2014.

JOBIM, Rosana Kim. **Compliance e trabalho**: entre o poder diretivo do empregador e os direitos inespecíficos do empregado. Rio de janeiro: Tirant lo Blanch, 2018.

JOBIM, Rosana Kim. Regulamentação do procedimento disciplinar na efetivação do compliance: uma necessidade na proteção do empregador. In: NASCIMENTO, Juliana Oliveira; CRESPO, Liana Irani Affonso Cunha (org.). **Mulheres em compliance**: desde o programa de Compliance até os seus impactos na sociedade. Curitiba: Ithala, 2020.

MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no direito e no processo do trabalho**. São Paulo: Revista dos Tribunais, 2022. *E-book.* Disponível em: Https://proview.thomsonreuters.com/launchapp/title/rt/monografias/252498744/v2/page/v. Acesso em: 06 jun. 2022.

MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no direito e no processo do trabalho.** São Paulo: Revista dos Tribunais, 2022. *E-book.* Disponível em: Https://proview.thomsonreuters.com/launchapp/title/rt/monografias/252498744/v2/page/v. Acesso em: 06 jun. 2022.

MONTOYA MELGAR, Antonio. **Derecho del trabajo.** 39. ed. Madrid: Tecnos, 2018.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO – OIT. **Conferência Internacional do Trabalho.** Genebra, 21 jun. 2019. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-lisbon/documents/publication/wcms_749807.pdf. Acesso em: 06 jul. 2022.

PALHARES , Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. **Compliance digital e lGPD.** São Paulo: Thomson Reuters Brasil, 2021. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/262297688/v1/page/rb-6.1. Acesso em: 06 jun. 2022.

PINHEIRO, Patrícia P. **Proteção de dados pessoais**: comentários à lei n. 13.709/2018 (LGPD). São Paulo: saraiva, 2021. *E-book.* Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555595123/. Acesso em: 29 jun. 2022.

PIZA, Bruna; MENDES, Larissa. Os pilares do compliance trabalhista. **JusBrasil,** [s.l.], 2019. Disponível em: https://ieadireito.jusbrasil.com.br/artigos/722168931/os-pilares-do-compliance-trabalhista?ref=topic_feed. Acesso em: 02 jul. 2022.

REANI, Valéria. O impacto da Lei de Proteção de Dados brasileira nas relações de trabalho. **Consultor Jurídico,** São Paulo, 21 set. 2018. Disponível em: https://www.conjur.com.br/2018-set-21/valeria-reani-alei-protecao-dados-relacoes-trabalho. Acesso em: 04 jul. 2022.

SAAVEDRA, Giovani Agostini. Compliance de dados. *In:* BIONI, Bruno. **Dados pessoais.** São Paulo: Revista dos Tribunais, 2020.

SANDEN, Ana Francisca Moreira de Souza. **A proteção de dados pessoais do empregado no direito brasileiro**: um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado. São Paulo : LTr, 2014.

SARLET, Gabriell Bezerra; TRINDADE, Manoel Gustavo; MELGARÉ, Plínio. **Proteção de dados:** temas controvertidos. Rio de Janeiro: Foco, 2021.

SILVA, Fabrício Lima; PINHEIRO, Iuri; BOMFIM, Vólia. **Manual do compliance trabalhista:** teoria e prática. Salvador: Juspodvm, 2020.