UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO DO RECIFE

CATARINA CARVALHO COELHO LUSTOSA

A APLICAÇÃO DA LGPD NAS RELAÇÕES TRABALHISTAS:

O Papel Estruturante do *Compliance* na Proteção de Dados do Empregado

Recife
2025

CATARINA CARVALHO COELHO LUSTOSA

A APLICAÇÃO DA LGPD NAS RELAÇÕES TRABALHISTAS:

O Papel Estruturante do *Compliance* na Proteção de Dados do Empregado

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, como requisito parcial para a obtenção do título de bacharel(a) em Direito.

Área de concentração: Direito do Trabalho e Direito Digital.

Orientador(a): Prof.º Dr. Carlo Benito Cosentino Filho

Recife

2025

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Lustosa, Catarina Carvalho Coelho.
A aplicação da LGPD nas relações trabalhistas: o papel estruturante do compliance na proteção de dados do empregado / Catarina Carvalho Coelho Lustosa. - Recife, 2025.
75

Orientador(a): Carlo Benito Cosentino Filho
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, Direito - Bacharelado, 2025.
9.
Inclui referências.

1. Direito do Trabalho. 2. Relações trabalhistas. 3. Lei Geral de Proteção de Dados (LGPD) . 4. Compliance. 5. Dados pessoais. 6. Proteção de dados do empregado. I. Cosentino Filho, Carlo Benito . (Orientação). II. Título.

340 CDD (22.ed.)

CATARINA CARVALHO COELHO LUSTOSA

A APLICAÇÃO DA LGPD NAS RELAÇÕES TRABALHISTAS:

O Papel Estruturante do *Compliance* na Proteção de Dados do Empregado

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, como requisito parcial para a obtenção do título de bacharel(a) em Direito.

Aprovado em: 05 / 08 / 2025

BANCA EXAMINADORA

_____

Prof.º Dr. Carlo Benito Cosentino Filho
Universidade Federal de Pernambuco

_____

Prof. Dr. Hugo Cavalcanti Melo Filho
Universidade Federal de Pernambuco

_____

Prof. Fydel Marcus Rolim Mota
Universidade Federal de Pernambuco

RESUMO

O presente trabalho analisa a aplicação da Lei Geral de Proteção de Dados (LGPD) nas relações trabalhistas, destacando o papel estruturante do *compliance* na proteção dos dados pessoais do empregado. Inicialmente, apresenta um panorama histórico e conceitual da proteção de dados no Brasil, ressaltando os fundamentos constitucionais e a inspiração advinda do GDPR europeu. Em seguida, discute a aplicabilidade da LGPD no âmbito laboral, identificando os sujeitos envolvidos, as bases legais adequadas para o tratamento de dados no ambiente de trabalho, a classificação dos dados do empregado e a responsabilidade das empresas em caso de tratamento irregular. Esse diálogo conduz à importância de proteção de dados do empregado-titular no âmbito das operações realizadas pelo empregador-controlador, reforçada pela natureza assimétrica da relação laboral. O estudo analisa a função essencial do *compliance* para implantação eficaz da LGPD nas relações de trabalho, desde a fase pré-contratual até a pós-contratual, identificando as principais ferramentas de conformidade, como políticas de privacidade, códigos de conduta, mapeamento de dados, treinamentos e sistemas de resposta a incidentes. Por fim, conclui que a aplicabilidade da LGPD às relações de trabalho exige uma abordagem multidisciplinar, integral e contínua, que pode e deve ser estruturada pelo *compliance*.

Palavras-chave: direito do trabalho; relações trabalhistas; LGPD; *Compliance*; dados pessoais; proteção de dados do empregado.

ABSTRACT

This paper examines the application of the General Data Protection Law (LGPD) in labor relations, highlighting the structuring role of compliance in safeguarding employee's personal data. It begins by providing a historical and conceptual overview of data protection in Brazil, emphasizing constitutional foundations and the influence of the European GDPR. The study then discusses the applicability of the LGPD in the labor context, identifying the involved parties, appropriate legal bases for data processing in the workplace, the classification of employee data, and corporate liability in cases of improper data handling. This discussion leads to the importance of protecting employee data within the operations carried out by the employer as a data controller, a concern heightened by the inherently asymmetric nature of labor relations. The paper analyzes the essential role of compliance in the effective implementation of the LGPD throughout all phases of the employment relationship–from pre-contractual to post-contractual stages–by identifying key compliance tools such as privacy policies, codes of conduct, data mapping, training, and incident response systems. Finally, it concludes that the application of the LGPD to labor relations requires a multidisciplinary, comprehensive, and continuous approach, which can and should be structured through compliance.

Keywords: labor law; labor relations; LGPD; compliance; personal data; employee data protection.

LISTA DE ABREVIAÇÕES E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
art.	artigo
arts.	artigos
ASO	Atestado de Saúde Ocupacional
cap.	capítulo
CC	Código Civil
CDC	Código de Defesa do Consumidor
CF/88	Constituição Federal de 1988
CLT	Consolidação das Leis do Trabalho
CPF	Cadastro de Pessoas Físicas
CTPS	Carteira de Trabalho e Previdência Social
DIRF	Declaração do Imposto sobre a Renda Retido na Fonte
DPO	*Data Protection Officer* (Encarregado)
EPI	Equipamento de Proteção Individual
FGTS	Fundo de Garantia do Tempo de Serviço
GDPR	*General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados – União Europeia)
LGPD	Lei Geral de Proteção de Dados
MPT	Ministério Público do Trabalho
NIT	Número de Identificação do Trabalhador
PIS	Programa de Integração Social
RBAC	*Role-Based Access Control* (Controle de Acesso Baseado em Papéis)
RH	Recursos Humanos
SEFIP	Sistema Empresa de Recolhimento do FGTS e Informações à Previdência Social
TI	Tecnologia da Informação
2FA	*Two-Factor Authentication* (Autenticação de Dois Fatores)

SUMÁRIO

1 INTRODUÇÃO

No século XX, Foucault propôs a teoria do panoptismo, descrevendo uma nova arquitetura de poder baseada na vigilância contínua, invisível e assimétrica, que se adapta aos diferentes cenários e induz comportamentos disciplinados. Transposta para o século XXI, essa lógica se potencializa: a vigilância pós-moderna se dá pelo controle de dados pessoais, que alavanca a economia informacional e ultrapassa limites físicos, exigindo uma regulamentação específica e interdisciplinar.

Nessa economia informacional, a valoração de dados pessoais gerou impactos em toda estrutura social, desde as relações privadas, pela inserção de informações pessoais nos *Smartphones*, até as relações contratuais externas, onde a difusão de dados é praticamente um requisito para a celebração e execução de contratos – inclusive de natureza laboral. Nas relações de trabalho, a crescente dependência de informações pessoais para a contratação, gestão e rescisão de vínculos empregatícios revela uma ameaça constante à privacidade dos trabalhadores.

A promulgação da Lei Geral de Proteção de Dados (LGPD) no Brasil ocorreu justamente numa era em que a vida se desdobra em fluxos incessantes de informações, tornando mais tênue a fronteira entre o público e o privado. Inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD estabeleceu parâmetros claros para o tratamento de dados no Brasil, orientando-se por princípios como a finalidade, necessidade, transparência e não discriminação.

Assim, a LGPD não apenas propôs um novo ecossistema de tutela de direitos, mas também, nos meandros desse ecossistema, ressoou profundamente nas relações laborais, onde o tratamento de dados pessoais do empregado – parte tradicionalmente vulnerável e subordinada ao poder patronal – reveste-se de especificidades, exigindo ainda maior cautela por parte das empresas e empregadores.

Entretanto, o microcosmo trabalhista apresenta desafios próprios à implementação da LGPD. Se, por um lado, o direito à proteção de dados pessoais se irradia a toda sociedade, inclusive nas relações laborais, por outro, a LGPD não dispõe expressamente sobre a aplicação de seus dispositivos aos contratos de trabalho.

O objetivo desta pesquisa consiste, portanto, em analisar de forma crítica e detalhada a aplicabilidade da LGPD no contexto das relações de trabalho, investigando

a efetiva operacionalização de seus dispositivos para assegurar a proteção dos dados pessoais dos empregados ao longo de todas as fases do processo contratual, especialmente mediante o uso de ferramentas de *compliance*.

Para tanto, após a introdução, o segundo capítulo esclarece sobre o núcleo teórico da LGPD, criando substrato para o desenvolvimento da pesquisa. Esse capítulo apresenta os conceitos, princípios, sujeitos e bases legais do tratamento de dados dispostos na lei, além de abordar a questão da responsabilização administrativa e civil pelo tratamento irregular de dados.

No início do terceiro capítulo, demonstra-se a aplicabilidade da LGPD no microssistema laboral, a partir de fundamentos doutrinários e legais. Ao longo do capítulo, superado o tema da aplicabilidade, o estudo busca estabelecer um diálogo eficiente entre a LGPD e a CLT, identificando os sujeitos e as bases legais de tratamento de dados nas relações de trabalho, além de tratar da responsabilização do empregador pelo tratamento irregular de dados do empregado.

Em sequência, o quarto capítulo direciona-se a aspectos práticos, analisando o papel estruturante do *compliance* nas empresas para garantia da conformidade contínua e integral com os preceitos da LGPD. Neste ponto, são apresentadas as principais ferramentas de *compliance* para implementação da LGPD na seara trabalhista – com foco na tutela de dados do empregado-titular – como as políticas de privacidade, regulamentos internos, bancos de dados, além de treinamentos e canais de denúncia.

Ademais, também no quarto capítulo, a perspectiva de integralidade e continuidade do *compliance* é explorada a partir das diversas fases do processo contratual trabalhista, condensando os principais momentos de tratamento de dados, como a coleta de currículos na fase pré-contratual, a vigilância digital por meio de câmeras na fase contratual e o armazenamento de dados após a rescisão contratual.

Destarte, o presente estudo se propõe a adentrar nas nuances das relações trabalhistas sob o escopo da Lei Geral de Proteção de Dados (LGPD), demonstrando o papel estruturante do *compliance* para proteção de dados pessoais de empregados.

2 LEI DE PROTEÇÃO DE DADOS

A proteção de dados no Brasil tem raízes que antecedem a própria legislação específica sobre o tema. Inicialmente, o debate girava em torno dos direitos fundamentais à privacidade e à intimidade – consolidados na Constituição Federal de 1988, no artigo 5º, incisos X e XII (Brasil, 1988) – e, durante muito tempo, a interpretação dessas normas constitucionais serviu de amparo a decisões judiciais sobre proteção de dados.

Ademais, mesmo que indiretamente, havia leis infraconstitucionais que dialogavam com a tutela de dados – cada uma em seu respectivo microssistema –, como o Código de Processo Penal (Brasil, 1941), no art. 157, o Código de Defesa do Consumidor (Brasil, 1990), nos arts. 43, 72 e 73, o Código Civil (Brasil, 2002), nos arts. 12 e 20, a Lei de Acesso à Informação (Brasil, 2011), no art. 31 e, especialmente, o Marco Civil da Internet (Brasil, 2014).

Não obstante, é evidente que a promulgação da LGPD inovou o ordenamento jurídico, por constituir um regulamento unificado e específico, de importância multifatorial. Além de estabelecer parâmetros e princípios claros para o tratamento de dados pessoais no Brasil – protegendo direitos fundamentais – a nova lei elevou o patamar do país perante o cenário internacional em matéria de proteção de dados.

A promulgação da LGPD se deu em 2018, vindo a entrar em vigor apenas em setembro de 2020, período este justificado pelo caráter inovador e impositivo da nova legislação, que exigiu das empresas (e ainda exige) adequação de seus procedimentos às novas obrigações legais.

Em 2022, consolidando a tutela de dados no Brasil, foi aprovada a Emenda Constitucional nº 115, de 8 de fevereiro de 2022, que incluiu expressamente a proteção de dados no rol de direitos e garantias fundamentais do art. 5º da CF/88 (Brasil, 2022). Assim, o direito à proteção de dados deixou de ser implícito – derivado de outros princípios – e ganhou natureza de direito fundamental autônomo, atraindo maior relevância jurídica e política para a LGPD.

A LGPD é dividida em 10 capítulos: em "Disposições Preliminares" (cap. I) são descritos os princípios e diretrizes da lei, seu objeto e conceitos essenciais; em "Do Tratamento dos Dados Pessoais" (cap. II), são indicadas as bases legais do tratamento

de dados, outros requisitos e obrigações; em "Dos Direitos do Titular" (cap. III), apresentam-se os direitos do titular de dados, como o de confirmação, eliminação e correção.

Os últimos capítulos são essenciais para a integração da LGPD às políticas de *compliance*: o cap. VII, "Da Segurança e das Boas Práticas", oferece diretrizes para programas de proteção de dados; o cap. VIII, “Da Fiscalização”, esclarece a aplicação de sanções administrativas decorrentes do descumprimento da LGPD.

2.1 Aspectos gerais

No artigo 1°, caput, o legislador define o objeto da lei, qual seja, o tratamento de dados pessoais, inclusive nos meios digitais, realizado por pessoa natural ou pessoa jurídica. O propósito da LGPD, nos termos do seu art. 1º, é a proteção dos direitos fundamentais à liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

Isto posto, três são as principais interpretações decorrentes do dispositivo: (i) a lei protege apenas dados pessoais da pessoa natural, não abrangendo informações de pessoas jurídicas, como segredos industriais e estratégias de negócio; (ii) a lei se aplica ao tratamento realizado por qualquer pessoa física ou jurídica, sejam empresas privadas ou instituições e órgãos públicos; (iii) a lei abrange o tratamento efetuado por meio físico e material, como em arquivos de papel, e em meio digital e virtual, como em bases de dados, nuvens e softwares.

O art. 2º acrescenta à base principiológica da legislação ao indicar fundamentos adicionais para o tratamento de dados pessoais, tais como o respeito à privacidade, autodeterminação informativa, liberdade de expressão, inviolabilidade da intimidade e da imagem e o desenvolvimento econômico e tecnológico. Esses fundamentos buscam equilibrar a tutela de direitos fundamentais com a promoção da inovação e a fluidez das informações na sociedade contemporânea.

Já o art. 3º delimita o âmbito de aplicação da LGPD, estabelecendo de forma abrangente que qualquer operação de tratamento de dados pessoais que envolva a coleta, armazenamento ou processamento de dados realizados no território nacional ou direcionados a pessoas localizadas no Brasil estará sujeita à lei.

2.2 Conceitos

O art. 5º da LGPD define conceitos-chave que orientam a aplicação da lei: dados pessoais, sensíveis e anonimizados; banco de dados; sujeitos e agentes do tratamento; operações de tratamento, bloqueio, eliminação, transferência e compartilhamento de dados; consentimento do titular; a figura da Autoridade Nacional de Proteção de Dados; e o relatório de impacto à proteção de dados pessoais (Brasil, 2018).

Entre os conceitos fundamentais para a LGPD e para o desenvolvimento deste estudo, destaca-se o termo "dado pessoal", que consiste em qualquer informação sobre uma pessoa natural que possibilita sua identificação direta ou indiretamente, como nome e sobrenome, CPF, RG, endereço residencial, telefone e e-mail (art. 5º, I).

Dentre esses dados pessoais, há uma categoria especial designada como “dados sensíveis”, que inclui informações sobre origem racial ou étnica, convicções religiosas, opiniões políticas, saúde, vida sexual (art. 5º, II). Esses dados carregam informações íntimas que podem ser utilizadas para fins discriminatórios e, por isso, seu tratamento representa um maior risco para os direitos do titular.

Tal distinção corresponde a um dos pilares da proteção de dados no Brasil, na medida em que a LGPD impõe aos agentes de tratamento de dados um especial dever de cautela quando estiverem em posse de dados pessoais sensíveis, com requisitos específicos, obrigações extras e penalidades mais gravosas.

A LGPD se propõe a proteger o titular durante todo ciclo de dados – desde a coleta até a eliminação – sem restringir-se a fases e momentos pontuais. Nesse sentido, o art. 5º, X, define o tratamento como toda operação realizada com dados pessoais, como a coleta, utilização, armazenamento, eliminação, transferência e outras. Trata-se de rol exemplificativo, logo, operações não indicadas no artigo também podem configurar tratamento de dados, atraindo a aplicação da lei (Miziara, 2022, p. 173).

No que concerne aos atores envolvidos, o art. 5º, incisos V a VIII, identifica o titular, o controlador, o operador e o encarregado: o titular é a pessoa natural a quem se referem os dados pessoais; o controlador é quem toma as decisões referentes ao tratamento de dados, enquanto o operador executa esse tratamento em nome do controlador – sendo ambos os “agentes de tratamento”; o encarregado, também

conhecido como Data Protection Officer (DPO), atua como intermediário entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD).

Por fim, o art. 5º, XIX, define a Autoridade Nacional de Proteção de Dados (ANPD) como órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional. Ao longo de sua redação, especialmente no Capítulo IX, Seção I ("Da Autoridade Nacional de Proteção de Dados), a LGPD detalha a função da ANPD, incluindo atividades de cunho social e cultural, direcionadas para conscientização da sociedade sobre a proteção de dados e demais temas pertinentes.

Além dos conceitos já abordados, termos como anonimização, banco de dados e relatório de impacto serão examinados com mais profundidade no decorrer do estudo, na medida de dialogarem com o tema, garantindo sejam apresentados de forma contextualizada.

2.3 Princípios gerais da LGPD

A LGPD estabelece em seu artigo 6º dez princípios fundamentais que devem nortear todas as atividades de tratamento de dados pessoais no Brasil (Brasil, 2018). Estes princípios dialogam diretamente com os direitos do titular e com os deveres dos agentes de tratamento, formando a base ética e jurídica para a proteção dos dados.

À luz dos ensinamentos de Bomfim e Pinheiro, os princípios "são premissas estruturantes que informam, conformam e orientam a aplicação das outras normas, sendo, por isso mesmo, considerados os alicerces ou as vigas-mestras do edifício jurídico" (Pinheiro; Bomfim, 2022, p. 40).

Os princípios da finalidade e adequação focam na compatibilidade e nos propósitos do tratamento: o primeiro (finalidade), determina que o tratamento deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular; o segundo (adequação), prevê que o tratamento deve ser compatível com as finalidades informadas ao titular, assegurando uma relação de confiança entre as partes.

Por sua vez, os princípios da necessidade e qualidade dão ênfase à quantidade e à precisão dos dados: o primeiro (necessidade), limita o tratamento ao mínimo necessário para a realização das finalidades almejadas, abrangendo apenas os dados pertinentes, proporcionais e não excessivos; o segundo (qualidade), busca assegurar

que os dados sejam exatos, claros e atualizados, ou seja, trata-se de garantia de qualidade.

Inclusive, dentre os princípios normativos, Bomfim e Pinheiro (2022, p. 40) dão especial destaque aos princípios da finalidade, adequação e necessidade, colocando-os como “tripé do núcleo duro de legitimação do tratamento de dados”. Explica-se:

> Os três primeiros princípios acima indicados formam um tripé do núcleo duro de legitimação do tratamento de dados, eis que sempre será preciso ponderar criteriosamente se a operação realizada está se restringindo à finalidade específica que justifica o seu uso; se é adequado ao fim pretendido e se está sendo realizado sem excessos, limitando apenas ao necessário (Pinheiro; Bomfim, 2022, p. 40).

Em sequência, tem-se o princípio da transparência e do livre acesso, que são direcionados à proteção dos direitos do titular – tema que será abordado em tópico específico. Adiante-se que o princípio da transparência assegura ao titular informações claras, precisas e facilmente acessíveis sobre a realização do tratamento, enquanto o princípio do livre acesso garante ao titular a consulta facilitada e gratuita sobre a forma, duração e agentes de tratamento de dados.

Os princípios da segurança e prevenção dispõe sobre o dever da organização em proteger os dados coletados e prevenir danos: o primeiro (segurança) exige da empresa a utilização de medidas técnicas para evitar acessos não autorizados, situações ilícitas ou acidentais de destruição, perda, alteração, comunicação ou difusão de dados pessoais; o segundo (prevenção) demanda a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Outro princípio relacionado às obrigações é o da responsabilização e prestação de contas, o qual determina que os agentes de tratamento devem evidenciar a adoção de medidas eficazes que comprovem a conformidade com as normas LGPD, além de estarem sempre preparados para justificar suas ações perante os titulares dos dados e as autoridades competentes.

Por fim, tem-se ainda o princípio da não discriminação, que proíbe expressamente o tratamento de dados para fins discriminatórios ilícitos ou abusivos, garantindo que as informações pessoais não sejam utilizadas para prejudicar os titulares ou perpetuar desigualdades sociais.

2.4 Bases legais para o tratamento de dados

Outro aspecto relevante trazido pela LGPD é a exigência de que toda atividade de tratamento de dados pessoais esteja respaldada por uma base legal específica. Os artigos 7º e 11 da LGPD delineiam essas bases legais, apresentando hipóteses taxativas que conferem legitimidade e licitude ao tratamento de dados pessoais (art. 7º) e dados pessoais sensíveis (art. 11) (Brasil, 2018).

A primeira base legal citada pelo regulamento é o consentimento, prevista no art. 7º, I, que exige a manifestação livre, informada e inequívoca do titular quanto à realização do tratamento de dados para a finalidade específica. Apesar de o legislador ter dado destaque ao consentimento, não há hierarquia entre as bases legais, sendo certo que – em alguns casos – o consentimento pode não ser a base adequada.

Nesse contexto, para alcançar a finalidade almejada, é possível a utilização de outras bases legais, que dispensam o consentimento, como a hipótese de cumprimento de obrigação legal ou regulatória por parte do controlador (art. 7º, II) – segunda base legal trazida pela LGPD.

A terceira base legal é direcionada ao tratamento de dados pela administração pública, quando necessários à execução de políticas públicas (art. 7º, III), enquanto a quarta base legal aplica-se aos órgãos de pesquisa, quando a finalidade do tratamento de dados é a realização de estudos (art. 7º, IV).

A LGPD também permite o tratamento de dados pessoais quando necessário à execução de contratos ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do mesmo (art. 7º, V), bem como para o exercício regular de direitos em processo judicial e administrativo (art 7º, VI). A tutela da saúde, exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, também é outra base legal prevista na lei (art. 7º, VII).

A nona base legal prevista pela LGPD é a utilização de dados para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (art. 7º, VIII). A aplicação dessa base legal reveste-se de controvérsias: se por um lado a terminologia aberta da expressão “interesses legítimos” amplia as hipóteses de

tratamento de dados, por outro há uma falta de delimitação – uma nebulosidade na expressão –, exigindo especial cautela na sua adoção (Grossi, 2020, p. 59).

Por fim, o art. 7º, X, da LGPD prevê a hipótese de tratamento de dados para a proteção de crédito, de modo que os titulares não precisam concordar, por exemplo, com seu registro nos cadastros de inadimplentes, como o SERASA.

No que tange ao tratamento de dados sensíveis – que englobam informações sobre raça, convicção religiosa, saúde, vida sexual, entre outras –, a LGPD estabelece critérios ainda mais restritivos no art. 11º, exigindo consentimento específico e destacado ou o enquadramento nas demais hipóteses trazidas pelo art. 7º, com exceção da execução de contrato, legítimo interesse ou proteção de crédito, que não autorizam o tratamento de dados sensíveis.

2.5 Direitos dos titulares de dados

Os direitos dos titulares de dados pessoais encontram-se previstos no art. 18 da LGPD e representam mecanismos fundamentais para assegurar ao cidadão controle efetivo sobre suas informações, mas também a transparência nas relações estabelecidas com empresas e órgãos públicos (Brasil, 2018).

O primeiro deles é o direito à confirmação da existência do tratamento de dados: trata-se de uma prerrogativa que permite ao titular saber de modo claro se seus dados estão sendo coletados, tratados ou armazenados por certo agente (art. 18, I). Essa confirmação é o ponto de partida do exercício de direitos pelo titular, sendo exigível do controlador a qualquer momento, sem justificativa prévia e de forma gratuita.

Ademais, também é direito do titular exigir o acesso aos dados pessoais que estejam sob posse do controlador (art. 18, II). Este acesso não se restringe à simples ciência da existência dos dados, mas se estende ao fornecimento de cópias, informações sobre a origem dos dados, critérios utilizados para o tratamento e a finalidade a que se destinam.

Outra garantia concedida ao titular é o direito à correção de dados incompletos, inexatos ou desatualizados (art. 18, IV). Aqui, assegura-se que as informações mantidas a respeito do titular sejam corretas e ajustadas à realidade, evitando prejuízos provenientes do uso de dados obsoletos ou errôneos.

Tem-se ainda os direitos de anonimização, bloqueio ou eliminação de dados considerados desnecessários, excessivos ou tratados em desconformidade com a legislação (art. 18, III). Este dispositivo permite ao titular solicitar o bloqueio temporário daqueles dados ou a própria exclusão definitiva, cabendo aos agentes o cumprimento da obrigação, respeitados os limites legais.

Tratando-se de tratamento autorizado por consentimento, o titular tem o direito à informação sobre a possibilidade de não fornecer o consentimento e sobre as consequências da negativa (art. 18, VI). Quando já consentido, o titular tem o direito de revogar o aceite (art. 18, IX) e de requerer a eliminação dos dados (art. 18, VI).

Nas hipóteses de tratamento realizado com base distinta do consentimento – como em cumprimento de obrigação legal ou por legítimo interesse – é possível ao titular exercer o direito de oposição quando identificar irregularidades no tratamento de dados, devendo o controlador analisar o pedido (art. 18 § 2º, LGPD).

Além das garantias previstas no art. 18, a LGPD prevê no art. 20, Caput e § 1º, o direito à revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais. Tal prerrogativa assegura ao indivíduo não apenas a explicação sobre os critérios e procedimentos utilizados na decisão, mas também a possibilidade de solicitar a revisão da decisão automatizada.

2.6 Responsabilidade Administrativa e Civil

No tocante às consequências legais pelo tratamento irregular de dados, a LGPD prevê duas esferas de responsabilidade: a administrativa, que consiste em sanções aplicadas pela ANPD (art. 52), e a civil, cujo reconhecimento pelo Poder Judiciário implica o dever de indenização (art. 42) (Brasil, 2018).

No âmbito administrativo, as penalidades variam desde uma simples advertência até multa pecuniária, além de outras medidas, como a publicização da infração, bloqueio ou eliminação dos dados pessoais relacionados à infração.

A aplicação de sanções pela ANPD exige apuração prévia dos fatos, respeitado o contraditório e à ampla defesa e ponderando elementos como a natureza dos dados, a existência de políticas de governança e de medidas para mitigar o dano (art. 50, § 1º)

Noutro turno, à luz do art. 42 da LGPD, a responsabilidade civil recai sobre o controlador ou operador, quando tratamento inadequado dos dados causar danos patrimoniais, morais, individuais ou coletivos a titulares e terceiros. Ademais, quando o dano decorrer por descumprimento do operador aos comandos lícitos do operador, a responsabilidade será solidária, salvo no caso de excludentes (art. 42, I).

Na doutrina, a redação aberta do art. 42 da LGPD enseja debates sobre a natureza da responsabilidade civil dos agentes de tratamento de dados – se objetiva ou subjetiva: por um lado o tratamento de dados é baseado na vulnerabilidade do titular e no risco à coletividade, o que fundamentaria a responsabilidade objetiva, como ocorre no CDC; por outro a LGPD inclui casos de exclusão de responsabilidade (§ 1º do art. 43) ou mitigação (art. 44, LGPD), aproximando-se de uma natureza subjetiva.

Para evitar uma digressão extensa sobre esse amplo tema – já que não é o foco da presente pesquisa – apresenta-se uma terceira via, proposta pelo professor Bruno Bioni, segundo a qual não é possível enquadrar a responsabilidade prevista na LGPD à clássica teoria binária (subjetivo ou objetivo). Assim explica Bioni e Dias:

> Deve-se, assim, avançar para além da análise binária do regime jurídico de responsabilidade civil da LGPD, julgando-o de natureza objetiva ou subjetiva. Isto porque não deve haver dúvidas de que a política legislativa adotada exige a investigação em torno de um juízo de culpa dos agentes de tratamento de dados, mas, ao mesmo tempo, prescreve uma série de elementos com alto potencial de erosão dos filtros para que os agentes de tratamentos de dados sejam responsabilizados. O resultado parece ir no sentido de um regime jurídico de responsabilidade civil subjetiva com alto grau de objetividade (Bioni; Dias, 2020, p.21).

Diante do exposto, observa-se que a LGPD estrutura um modelo de responsabilização múltipla e autônoma entre as esferas administrativa e civil. Cada esfera opera com fundamentos, objetivos e procedimentos próprios: enquanto a responsabilidade administrativa visa à disciplina e à conformidade regulatória, a responsabilidade civil busca reparar danos efetivamente causados.

3 A TUTELA DE DADOS PESSOAIS NAS RELAÇÕES TRABALHISTAS

A Consolidação das Leis do Trabalho (CLT) foi promulgada em 1943 para proteger o empregado celetista, que representa uma categoria específica dentro do amplo conceito de trabalhador. O gênero “trabalhador” engloba diversas figuras jurídicas presentes nas relações laborais, tais como o empregado (regido pela CLT), o trabalhador autônomo, os eventuais, os diaristas e os estagiários.

O empregado, para ser assim reconhecido e usufruir das proteções da CLT, deve preencher requisitos específicos expressos no art. 3º da CLT: "Considera-se empregado toda pessoa física que prestar serviços de natureza não eventual a empregador, sob a dependência deste e mediante salário" (Brasil, 1943, art. 3º).

Ou seja, só é considerado empregado aquele que exerce trabalho de natureza habitual, sob comando direto do empregador, com remuneração e sem possibilidade de transferir a terceiros a execução de suas tarefas.

O objetivo central da legislação trabalhista é equilibrar a relação dicotômica entre empregador e empregado, orientando-se a partir do reconhecimento da hipossuficiência e vulnerabilidade do trabalhador, o que justifica a necessidade de atuação do Estado como agente regulamentador e fiscalizador das relações laborais.

O conceito de hipossuficiência está tradicionalmente atrelado à condição de desigualdade entre indivíduos, que dificulta ou impede a parte hipossuficiente de exercer seus direitos em condições de igualdade. No âmbito laboral, essa noção parte da premissa de que o empregado, por não dispor dos meios de produção e depender do salário para seu sustento, está em posição de fragilidade em face do empregador.

Enquanto a hipossuficiência foca no aspecto econômico da desigualdade, o conceito de vulnerabilidade abrange outras dimensões, considerando não apenas o aspecto econômico, mas também social, técnico e informacional. Nas relações de trabalho, a vulnerabilidade informacional alcança a questão da capacidade do trabalhador de se informar, de compreender seus direitos e deveres e de participar efetivamente das decisões que impactam sua vida profissional (Alves, 2019, p. 125-126).

No atual contexto de produção, armazenamento e transferência de dados pessoais, a vulnerabilidade informacional do trabalhador vem sendo acentuada, à

medida que o empregador detém amplo acesso e controle sobre as informações do empregado, enquanto este, muitas vezes, desconhece como seus dados são coletados, armazenados e utilizados ou – ainda que tenha ciência – não possui os meios para intervir nesse procedimento.

Desse modo, diante deste cenário de vulnerabilidade informacional e considerando a necessidade de restringir o poder das empresas no tratamento dos dados dos empregados, torna-se imperativo discutir a aplicação da LGPD nas relações de trabalho como uma resposta normativa a essa questão.

3.1 Aplicabilidade da LGPD às relações de trabalho

A Lei Geral de Proteção de Dados Pessoais (LGPD), embora seja uma legislação ampla e de grande relevância social, não prevê expressamente dispositivos específicos voltados ao contexto das relações de trabalho. Paralelamente, a Consolidação das Leis do Trabalho (CLT) também não estabelece um regime jurídico específico para a proteção da privacidade e dos dados pessoais dos empregados.

Diante desse vazio normativo, a discussão sobre a incidência da LGPD às relações de emprego ganha relevância, especialmente perante os desafios trazidos pela sociedade da informação.

O ponto de partida para a aplicação da LGPD nas relações de trabalho é compreender a opção do legislador por uma norma de caráter geral e abrangente, destinada à proteção de qualquer pessoa natural cujos dados foram coletados ou tratados no Brasil. Essa abrangência é evidente pela leitura do art. 1º e do 3º, da LGPD:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Brasil, 2018).
> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que [...] (Brasil, 2018).

Nesse sentido, a aplicabilidade da LGPD não se restringe a um ramo específico do direito, sendo perfeitamente possível integrá-la a outros microssistemas quando as normas específicas forem omissas quanto ao tratamento de dados.

Somado a isso, como já esclarecido, a própria CF/88 confere o status de direito fundamental à intimidade, à privacidade e, especificamente, à proteção de dados pessoais. Assim, assegurar esses direitos é um dever constitucional, o que confirma a aplicabilidade ampla e geral da LGPD.

No caso da CLT, a ausência de regulamentação sobre privacidade e proteção de dados evidencia uma lacuna normativa, demandando o seu preenchimento. Trata-se de uma legislação promulgada em 1943, muito antes do advento das tecnologias digitais e da centralidade dos dados na vida social. Assim como outros ramos do direito, a CLT não foi capaz de acompanhar as rápidas mudanças sociais e evoluções tecnológicas, o que explica o vazio normativo sobre temas atuais, como a privacidade de dados.

No Direito do Trabalho, a integração normativa pode ocorrer pela autointegração, quando há uso de normas do mesmo ramo, ou pela heterointegração, na qual se recorre a outras fontes jurídicas relevantes (Delgado, 2019, p. 279-280). Inclusive, a CLT, no seu art. 8º, §1 º, autoriza expressamente a utilização subsidiária do direito comum quando não houver norma trabalhista específica (Brasil, 1943).

Nesse sentido, Priscila Zoghbi conclui que “é possível auferir que a LGPD consiste em uma norma de direito comum, ou seja, não específica do direito laboral que pode vir a ser utilizada de forma subsidiária” (Zoghbi, 2022, p. 87).

Diante disso, torna-se evidentemente possível a aplicação da LGPD às relações de trabalho, seja pela abrangência prevista no art. 3º da respectiva lei, seja porque a CLT autoriza a integração normativa quando há omissão – ou ainda pela necessidade de proteção a direitos fundamentais dispostos na CF/88, especialmente a privacidade e proteção de dados.

No entanto, essa integração não pode ocorrer de maneira acrítica ou dissociada dos fundamentos do direito do trabalho, devendo haver compatibilidade, principalmente com o princípio da proteção ao trabalhador. Assim, é necessário estabelecer um diálogo entre os princípios e conceitos trazidos pela LGPD e as peculiaridades do ambiente de trabalho regulamentado pela CLT.

3.2 Dados pessoais e sujeitos da LGPD nas relações de trabalho

O diálogo entre a CLT e a LGPD se tornou inevitável diante de uma sociedade cada vez mais digitalizada e do crescente fluxo de dados no ambiente laboral. As novas dinâmicas laborais caracterizadas pelo uso de plataformas, aplicativos e mecanismos de gestão algoritmizada intensificam o tratamento de dados pessoais, exigindo dos empregadores e operadores atenção redobrada.

A CLT, cujo espírito é de proteção e equilíbrio nas relações laborais, agora se vê interligada à LGPD, que passa a atuar na tutela de direitos do empregado-titular e a impor deveres ao empregador-controlador no tratamento de dados.

Um ponto essencial para estabelecer essa integração é a classificação dos dados tratados no ambiente de trabalho: se pessoais ou sensíveis. Os dados pessoais são aqueles de identificação, tipicamente coletados para registro do empregado, como o nome, endereço, estado civil, quantidade de filhos, dados bancários, histórico acadêmico e profissional e números de CPF, CTPS, PIS e NIT.

Por sua vez, os dados sensíveis trazem informações íntimas, que podem gerar discriminação. Entre os dados sensíveis, citam-se informações sobre origem étnica ou racial, gênero e orientação sexual, filiação sindical, saúde (relacionadas ao ASO, por exemplo) e dados biométricos (para o controle de jornada ou acesso interno).

A compreensão do diálogo entre as legislações também exige a identificação dos sujeitos previstos na LGPD (titular de dados, controlador, operador e encarregado) e suas correspondências dentro das relações de trabalho.

Nesse contexto, o empregado normalmente figura como titular, pois é dele que se extraem e processam dados para fins de cadastro, folha de pagamento, benefícios, registro de ponto, e outros processos internos. Apesar de aqui focar-se no empregado celetista, é certo que o titular de dados também pode ser um profissional autônomo, avulso, eventual ou terceirizado – desde que seja pessoa natural (art. 5º, V, LGPD).

O empregador, a seu turno, tipicamente se enquadra como controlador (art. 5º, VI), pois detém o poder de decisão sobre a finalidade e os meios do tratamento dos dados de seus empregados e de terceiros, como clientes e fornecedores. Nada impede, contudo, que o empregador exerça cumulativamente a função de operador, quando realizar, ele próprio, o tratamento de dados.

As empresas terceirizadas ou profissionais autônomos que realizam diretamente o tratamento de dados – por exemplo, para processamento de folhas de pagamento e benefícios laborais – também são considerados operadores.

Atualmente, existem debates acerca da posição do operador de dados, em especial sobre a necessidade de tal função ser exercida por agente externo à organização, o que repercute diretamente na responsabilização legal. Para uma primeira corrente, a necessidade se fundamenta no Guia Orientativo Para Definições de Agente de Tratamento de Dados Pessoais e do Encarregado (2021) elaborado pela ANPD, que – baseando-se na legislação europeia (GDPR), prevê no item 51:

> [...] empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta não devem ser considerados operadores. [...] o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos (Brasil, ANPD, 2021, p. 8).

Contudo, para a corrente majoritária, é possível que o empregado interno exerça a função de operador, seja porque não há expresso impeditivo na LGPD, seja pela natureza não vinculante do Guia Orientativo da ANPD.

Por sua vez, a figura do encarregado ou Data Protection Officer (DPO) pode ser desempenhada por um funcionário interno ou externo, desde que atue com independência e imparcialidade, haja vista a natureza de suas atividades – muitas vezes contrárias aos interesses econômicos da empresa. Por esse motivo, inclusive, autores como Tarcísio Teixeira recomendam que “o encarregado seja independente do resto da empresa [...] sem qualquer vínculo da sua remuneração com os resultados da empresa, com total imparcialidade” (Teixeira; Armelin, 2019, p. 116)

Dessa forma, a relação entre LGPD e CLT extrapola o simples enquadramento conceitual dos sujeitos envolvidos. O entrelaçamento dos papéis revela desafios jurídicos para a delimitação da responsabilidade, principalmente em contextos de subordinação laboral, terceirização, compartilhamento de dados entre vários agentes.

3.3 Bases legais para o tratamento de dados do empregado-titular

Conforme elucidado, a aplicação da LGPD às relações de trabalho não ocorre automaticamente; é essencial que haja compatibilidade. Nesse contexto, é crucial observar os princípios trabalhistas, como o da proteção e o da razoabilidade, a fim de evitar ações que aumentem a vulnerabilidade do empregado titular. Assim, é evidente que a adequação das bases legais ao contexto laboral reveste-se de especificidades, demandando maior cautela por parte do empregador como controlador de dados.

A base legal do consentimento – muito utilizado em outras áreas – aparece como inadequada para a esfera trabalhista. Nos termos do art. 5º, XII, da LGPD, o consentimento não deve ser um ato involuntário e irrefletido, mas sim uma manifestação livre, informada e inequívoca – o que, nas relações marcadas pelo desequilíbrio entre as partes, pode ser especialmente complexo.

O vínculo de dependência e subordinação, típico do contrato de trabalho, constitui um empecilho para a aferição da legitimidade na manifestação. Especificamente nas relações laborais, o empregado-titular se sente compelido a consentir para evitar prejuízos ou constrangimentos, o que esvazia o próprio sentido de proteção almejado pela LGPD. Nesse sentido esclarece Sankievicz e Pinheiro:

> [...] a mera obtenção desse consentimento não é algo a garantir, por si só, a segurança jurídica ao tratamento pelo empregador. Primeiro, porque o consentimento pode ser retirado a qualquer momento pelo empregado sem que, desse fato, possa haver qualquer prejuízo a outros direitos. Segundo, porque, tendo em vista o desequilíbrio de poder existente nas relações de trabalho, sempre se poderá questionar judicialmente a livre manifestação de vontade do subordinado no momento do consentimento para o fornecimento de dados biométricos (Sankievicz; Pinheiro, 2021, p. 517).

Além de considerar a assimetria das relações, o uso dessa base legal implica em direitos e deveres especiais, os quais serão explorados em tópico específico sobre a adequação prática do consentimento no ambiente laboral.

Assim, ainda que o consentimento possa ser utilizado em situações excepcionais na esfera trabalhista, sua aplicação é subsidiária – ou seja, só se justifica quando nenhuma outra base legal for capaz de amparar o tratamento de dados.

Por essas razões, dentro do cenário trabalhista, o tratamento de dados deve ser orientado por outras bases legais, que assegurem simultaneamente a conformidade com a LGPD e a proteção dos direitos do empregado – evitando que o consentimento se torne mais um instrumento de controle patronal.

Nesse contexto, Pinheiro e Bomfim (2022, p. 47) identificam bases legais mais adequadas ao cotidiano trabalhista, quais sejam: i) o cumprimento de obrigação legal ou regulatória; ii) execução de contrato ou procedimento preliminares relacionados ao contrato do qual o titular seja parte; iii) o exercício de direitos em processo judicial, administrativo ou arbitral. Além destas, outros autores também citam como adequadas as seguintes bases legais: iv) para a proteção da vida ou da incolumidade física do titular ou de terceiro; v) o legítimo interesse do controlador (Carloto, 2021, p. 134).

A “obrigação legal ou regulatória” constitui a base legal mais recorrente no âmbito laboral, pois diversas obrigações impostas pela legislação trabalhista e previdenciária demandam o tratamento de dados pessoais e, por vezes, de dados sensíveis do empregado-titular (Coutinho, 2020, p. 297).

Entre essas obrigações estão: o registro do empregado e as anotações em carteira (arts. 29 e 41, CLT), o controle de jornada (art. 74, CLT), o envio de informações de vínculos, salários e desligamentos pelo eSocial (Decreto nº 8.373/2014), a prestação de dados à Previdência Social (art. 32, Lei nº 8.212/1991), e o repasse de informações ao FGTS (art. 17-A, Lei nº 8.036/1990).

Outra base legal amplamente utilizada no âmbito trabalhista é a da “execução de contrato ou de procedimentos preliminares relacionados ao contrato do qual seja parte o titular”. No processo de admissão, a checagem de documentos é um procedimento indispensável para formalização do vínculo. Após essa formalização, diversas rotinas administrativas – como o controle de jornada e o pagamento de salários – também impõem o tratamento contínuo de dados do empregado para execução do contrato.

Ademais, o armazenamento de dados também pode ser necessário para viabilizar o exercício de defesa da empresa em eventual processo judicial, administrativo ou arbitral. Para se desincumbir do ônus de prova e atender às exigências processuais, pode ser necessário que o controlador-empregador apresente documentos coletados ao longo do vínculo laboral.

Essa lógica coaduna com a sistemática processual trabalhista, uma vez que CLT, no art. 818, também atribui ao empregador o encargo de comprovar fatos impeditivos, modificativos ou extintivos do direito do empregado (Brasil, 1943).

A proteção da vida e da incolumidade física do titular também pode justificar o tratamento de dados, especialmente em ambientes laborais que apresentam riscos à saúde ou requerem atenção à segurança patrimonial. Exemplo disso é o monitoramento por câmeras para fiscalizar a utilização de EPI´s por parte dos funcionários.

Por fim, o legítimo interesse do controlador aparece como uma base legal adequada quando não há uma obrigação legal ou contratual explícita, mas existe uma necessidade real e legítima de tratamento de dados para finalidades compatíveis com a relação de trabalho.

Por exemplo, o monitoramento de desempenho mediante métricas e a utilização de vigilância digital podem ser amparados por esse fundamento, pois é do legítimo interesse do empregador a otimização de suas atividades e a proteção de seu patrimônio. Contudo, o legítimo interesse exige uma análise criteriosa, considerando sempre os direitos e expectativas do empregado-titular, de modo a evitar excessos ou abusos que coloquem em risco sua privacidade e dignidade.

A escolha da base legal adequada para o tratamento de dados no ambiente de trabalho é essencial para a proteção jurídica das empresas, ao passo que garante os direitos do empregado – devendo integrar as políticas de *compliance*, desde a fase de recrutamento até o momento posterior à rescisão contratual.

Rememore-se, contudo, que a LGPD é um regulamento geral e recente, motivo pelo qual sua incidência no ordenamento jurídico é marcada por divergências doutrinárias e jurisprudenciais, principalmente em microssistemas regidos por normas próprias, como o celetista. Nesse sentido, a aplicação das bases legais em exemplos concretos do cotidiano laboral não é tema uniforme na doutrina, sendo fundamental – em todo caso – a observância a princípios gerais e o acompanhamento jurisprudencial.

3.4 Responsabilização do empregador pelo tratamento de dados

No contexto da proteção de dados nas relações laborais, três esferas de responsabilidade recaem sobre o empregador-controlador: administrativa, civil e

trabalhista. Cada uma detém aspectos e requisitos próprios e pode resultar em consequências específicas.

A responsabilidade administrativa relaciona-se às sanções impostas pela ANPD em caso de infração à LGPD. O empregador que realiza tratamento inadequado, inseguro ou ilícito de dados pessoais pode ser submetido a advertências, multas simples ou diárias, a publicização da infração, bloqueio dos dados, eliminação das informações e medidas restritivas, conforme o art. 52 da LGPD (Brasil, 2018).

No âmbito civil, persiste a divergência doutrinária sobre a natureza da responsabilidade pelo tratamento de dados: se objetiva, subjetiva – ou ainda, situada em uma zona intermediária. Em matéria de direito do trabalho, alguns autores se utilizam da teoria do risco empresarial (art. 927, Parágrafo Único, CC) e da teoria geral de responsabilidade objetiva dos empregadores por danos causados aos empregados (arts. 932, III, e 933, Parágrafo Único) para defender a dispensa do requisito culpa.

De todo modo, sem definição clara, é possível concluir que o dever de reparação exige a demonstração do ato ilícito praticado pelo empregador-controlador, do dano causado ao empregado-titular e, dependendo da tese adotada, de culpa ou dolo. Ao refletirem sobre a questão, os Correia e Boldrin destacam:

> Ademais, em sendo identificado o prejuízo ao trabalhador, o empregado terá direito à indenização por danos morais em decorrência da violação de seu direito fundamental à privacidade e intimidade.
> Quando identificada repercussão social que traga prejuízo à coletividade dos trabalhadores, haverá atuação do MPT, por meio de tutela inibitória da conduta lesiva ao trabalhador, com o estabelecimento de Termo de Ajustamento de Condutas com os infratores ou o ajuizamento de ação civil pública para se evitar o cometimento de novas práticas que prejudiquem os trabalhadores (Correia; Boldrin, 2020).

O quantum indenizatório pode ser ampliado quando o incidente recai sobre dados sensíveis, como informações de saúde, religião, opinião política, biometria ou filiação sindical (art. 52, §1º, I, VI, IX). Além disso, na esfera cível, a responsabilidade pode alcançar operadores externos, prepostos ou terceirizados, que – em nome do empregador – manuseiam dados dos empregados (arts. 42, §1º, e art. 39 da LGPD).

No plano trabalhista, a responsabilidade do empregador pelo tratamento inadequado dos dados do empregado-titular pode ensejar a rescisão indireta do

contrato de trabalho, nos termos do art. 483, alínea “d”, da CLT, principalmente se tratando de dados sensíveis, como complementam Correia e Boldrin:

> [...] especialmente se houver exposição de dados íntimos e sensíveis que tragam prejuízos aos direitos de personalidade do empregado, é possível o reconhecimento da rescisão indireta do contrato de trabalho por violação das obrigações contratuais (Correia; Boldrin, 2020).

Assim, o descumprimento das obrigações legais e contratuais relacionadas à proteção de dados – como a exposição indevida, o uso discriminatório de informações ou a recusa em atender solicitações do empregado – pode ser considerado falta grave, tornando insustentável a continuidade do vínculo laboral.

Nesse caso, será assegurado ao funcionário os direitos referentes à dispensa sem justa causa, quais sejam, o saldo de salário, aviso prévio indenizado, férias proporcionais e vencidas – ambas acrescidas do terço proporcional –, 13º salário proporcional, FGTS com multa de 40% e acesso ao seguro-desemprego.

Por fim, ressalte-se que cada esfera de responsabilidade (administrativa, cível e trabalhista) é independente, ou seja, a condenação em uma esfera não exclui a possibilidade de condenação em outra. A falta de conformidade às normas da LGPD pode desencadear procedimentos administrativos, ações cíveis e litígios trabalhistas, evidenciando a transversalidade da proteção de dados no ambiente laboral.

Nesse contexto, é evidente que a busca pela conformidade às normas de proteção de dados demanda mais do que ações pontuais ou respostas reativas aos incidentes. Exige, sobretudo, o desenvolvimento de uma postura preventiva e estruturada, capaz de envolver todos os níveis da organização. Neste ponto, surge a importância do estudo do *compliance* como ferramenta de adequação sistemática da LGPD às relações de trabalho.

4 *COMPLIANCE* E LGPD NAS RELAÇÕES DE TRABALHO

A origem etimológica do termo “*compliance*” está no verbo inglês “to comply”, que significa “agir de acordo”, “cumprir” ou “estar em conformidade”. Esse conceito vem ganhando relevância diante da crescente complexidade das relações empresariais e do avanço constante da regulamentação em diversos setores econômicos.

Juridicamente, o termo *compliance* refere-se ao conjunto de mecanismos, políticas, práticas e condutas que buscam garantir a conformidade das atividades de pessoas jurídicas – e, cada vez mais, de pessoas naturais em posições de gestão – às legislações vigentes, regulamentações setoriais, normas internas e padrões éticos reconhecidos.

Essa cultura de conformidade não oferece uma fórmula única para ser replicada: sua estrutura deve ser adequada às realidades de cada organização, aos tipos de negócio, aos problemas concretamente verificados, aos setores a que se destinam e, principalmente, às normas que o regulamentam.

De modo geral, três são os pilares fundamentais do *compliance*: prevenção, detecção e correção. A prevenção consiste na adoção de medidas proativas que minimizam a ocorrência de irregularidades e reduzem a exposição a riscos legais. Isso inclui o mapeamento e análise de riscos, códigos de conduta e políticas internas, além de treinamentos regulares e outros.

Por sua vez, a detecção diz respeito à identificação tempestiva de falhas, por meio de mecanismos como auditorias, monitoramento e canais de denúncia. Já a resposta (ou correção) refere-se à conduta institucional perante a ocorrência de irregularidades, o que envolve a apuração dos fatos, a responsabilização dos envolvidos, a contenção e remediação dos danos, entre outras medidas cabíveis.

No Brasil, o *compliance* como prática empresarial se consolidou com a edição da Lei Anticorrupção (Lei nº 12.846/2013), que trata da responsabilização das empresas por atos ilícitos contra a administração pública. Para Soares *et al* (2021 p, 35), os desdobramentos da lei na operação “Lava Jato” e o “Mensalão” despertaram novas preocupações na sociedade, exigindo das empresas a implementação de programas de *compliance* para garantia da integridade e reputação.

Se no início o *compliance* se restringia às grandes corporações e ao combate à corrupção, com o tempo suas diretrizes foram adaptadas a diversos ramos do Direito, incluindo áreas como direitos do consumidor, concorrência, meio ambiente, as relações de trabalho e, mais recentemente, a proteção de dados. O amadurecimento do tema revelou que a conformidade não se atém ao dever jurídico, mas também ético e cultural.

Apesar disso, a consolidação do *compliance* no Brasil ainda enfrenta obstáculos, existindo uma grande distância entre o discurso e a prática, especialmente quando se trata de transformar o *compliance* em cultura organizacional real, e não em meras políticas documentais. Ademais, muitos programas ainda estão centrados apenas na proteção da empresa, e não na efetivação de direitos – o que esvazia seu propósito transformador.

4.1 *Compliance* trabalhista

No âmbito trabalhista, a existência de um programa de conformidade efetivo ganha ainda mais relevância, haja vista a inerente hipossuficiência do trabalhador, alhures esclarecida. Mais do que garantir a observância à lei, o *compliance* trabalhista atua diretamente na contenção de práticas que aprofundem desequilíbrios estruturais, contribuindo para a equidade material.

Em seu sentido tradicional, a conformidade trabalhista exige a observância a todos os princípios e normas, internos ou externos, aplicáveis às relações de trabalho. Isso inclui a própria CLT e seus princípios específicos, como o da proteção ao trabalhador, mas também a CF/88 e os direitos fundamentais nela previstos, tais como liberdade, igualdade, intimidade e privacidade.

A dignidade da pessoa humana, prevista no art. 1º, III, da CF/88 (Brasil, 1988), surge como princípio basilar do *compliance* laboral, fundamentando a promoção de um ambiente laboral ético e transparente, pautado no reconhecimento do valor intrínseco de cada trabalhador.

Ao tratar do tema, Vólia Bomfim, Fabrício Lima Silva e Iuri Pinheiro identificam funções específicas do *compliance* trabalhista, a saber, a função de cumprimento, função de prevenção e função de excelência laboral.

> [...] o compliance trabalhista é uma ferramenta essencial para prevenção e gestão de riscos na área trabalhista, cuidando de garantir o cumprimento das normas trabalhistas (função de cumprimento), evitando que os riscos previstos ocorram (função de prevenção) e estimulando a adoção de boas práticas destinadas à valorização do capital humanos das empresas (função de excelência laboral) (Bomfim *et al,* 2022, p. 7-8).

Quando bem estruturados e postos em prática, os pilares da prevenção, detecção e correção contribuem para a sustentabilidade e integridade das organizações em longo prazo. Ao estruturar suas práticas e processos com base na conformidade legal, a empresa minimiza a exposição a sanções e litígios judiciais, ao mesmo tempo em que fortalece sua imagem institucional perante o mercado.

Esse compromisso com a ética e a transparência também favorece o engajamento interno, criando um ambiente de trabalho mais claro, seguro e colaborativo, no qual o empregado tem melhores condições de reconhecer e denunciar práticas abusivas. Assim, o *compliance* trabalhista repercute no reconhecimento e bem-estar dos funcionários e, consequentemente, em sua produtividade.

Contudo, apesar de suas promissoras potencialidades, a aplicação do *compliance* nas relações de trabalho ainda esbarra em obstáculos estruturais. Frequentemente, a adoção de mecanismos de conformidade ocorre de maneira meramente formal e simbólica, voltado mais à autoproteção das empresas perante as autoridades do que à promoção dos direitos dos trabalhadores, o que limita o potencial protetivo dessas ferramentas e pode acentuar a assimetria das relações.

O porte da empresa também representa um desafio à efetivação do *compliance* trabalhista, na medida em que organizações de menor porte muitas vezes não atribuem prioridade ao tema, sob a justificativa de possuírem estruturas mais simples.

Todavia, tal argumento não se sustenta, seja porque a legislação não distingue obrigações conforme o porte da empresa, salvo exceções pontuais, seja porque o modelo de *compliance* é flexível, podendo – e devendo – ser adaptado à realidade econômica e estrutural de cada organização. Nesse sentido, dispõe Carloto:

> O compliance trabalhista não é apenas vital em grandes corporações, é patente a necessidade do mesmo na promoção e efetividade dos direitos humanos para as empresas eliminarem passivos e manterem sua imagem e reputação, por meio de cultura ética, independente do porte e tamanho da empresa (Carloto, 2021, p. 44).

Para que o *compliance* não reforce o desequilíbrio estrutural já existente, é fundamental que haja a participação dos empregados, os quais detém uma visão mais exata dos problemas enfrentados e que devem ser objetos do programa de conformidade trabalhista. A participação dos empregados não deve acontecer somente na criação dos programas de conformidade, mas precisa ser um ponto central e constante em todo o funcionamento do programa.

Embora o *compliance* trabalhista tenha origem em uma perspectiva tradicional voltada ao atendimento das normas trabalhistas e constitucionais, sua eficácia contemporânea depende da evolução para um modelo moderno e dinâmico, capaz de considerar as transformações sociais e tecnológicas que impactam o mundo do trabalho e põem em xeque práticas antigas.

Nesse contexto, temas emergentes e complexos, como a proteção de dados, impõem novas responsabilidades e obrigações às empresas em relação aos direitos dos empregados, exigindo uma postura proativa na atualização e adequação das práticas de *compliance* – que deve ir além da mera formalidade simbólica e tradicional.

4.2 *Compliance* e Governança no âmbito da LGPD

Com o advento da LGPD, o *compliance* trabalhista passou a incorporar também desafios e princípios relacionados à proteção de dados pessoais e à privacidade. Hoje, falar em *compliance* no ambiente de trabalho vai além da observância às tradicionais normas celetistas, exigindo-se uma conformidade holística, que abrange desde as obrigações legais estabelecidas na própria LGPD, como também as resoluções, guias e cartilhas complementares.

Entre as principais resoluções de proteção de dados, citam-se a Resolução CD/ANPD nº 10/2023, que estabelece ciclos regulares de monitoramento e evolução regulatória, a Resolução CD/ANPD nº 15/2024, que dispõe sobre comunicação de incidentes de segurança, a Resolução CD/ANPD nº 18/2024, dedicada à definição e atribuições do encarregado (DPO) e, por fim, a Resolução CD/ANPD nº 19/2024, referente a transferências internacionais e cláusulas contratuais.

Além das resoluções, recomenda-se aos agentes de tratamento de dados a observância aos Guias Orientativos da ANPD, como o Guia de Boas práticas (2020),

Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade (2021), Guia para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado (2022), Guia de Elaboração de Inventário de Dados Pessoais (2023), Guia de Elaboração de Programa de Governança em Privacidade (2024), Guia de Resposta a Incidentes de Segurança (2024) e outros.

Essa multiplicidade de instrumentos exige a existência de um sistema de conformidade capaz de articular conhecimentos jurídicos, técnicos e de gestão, adaptando práticas e procedimentos à evolução contínua das normas e orientações. Nesse cenário, para garantir a adequação, prevenção e correção em matéria de tratamento de dados, o *compliance* é fundamental.

Inclusive, atribuindo devida importância ao tema, a LGPD estabelece as bases para implementação de um programa de *compliance* em proteção de dados, especificamente na seção intitulada “Das Boas Práticas e da Governança”.

Embora a LGPD utilize predominantemente o termo "governança" em seu texto legal, entende-se que os “principais elementos do *compliance* seriam também elementos da governança em privacidade, dispostos expressamente no art. 50, da Lei Geral de Proteção de Dados” (Garbaccio *et al,* 2025). Assim, na prática, governança e *compliance* operam de forma complementar, sendo ambos fundamentais para a efetiva estruturação da LGPD nas relações de trabalho.

Segundo a legislação de proteção de dados, o programa de *compliance* (e de governança) deve abranger aspectos como a organização interna, os procedimentos relacionados às reclamações dos titulares, as normas de segurança, os padrões técnicos, as obrigações específicas de cada agente envolvido, as ações educativas e os mecanismos internos de supervisão e mitigação de riscos (Brasil, 2018).

Um ponto notável nessa seção da LGPD é o cuidado que teve o legislador em indicar um modelo-base de *compliance* passível de implementação prática, que considera as especificidades e riscos de cada tratamento e, ao mesmo tempo, a efetiva capacidade das empresas – sem impor obrigações excessivas ou desnecessárias. Essa singular proporcionalidade é verificada nos § 1º e § 2º do art. 50:

> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a

> natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
>
> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: [...] (Brasil, 2018).

Dessa forma, fica evidente que todas as empresas – independentemente do porte ou da sua capacidade técnica e econômica – devem possuir programas eficientes de *compliance* em proteção de dados. A LGPD admite adaptações e flexibilizações conforme a realidade organizacional, mas não abre margem para a exclusão total dessas obrigações.

No âmbito laboral, isso reforça o entendimento de que a conformidade legal e a proteção dos direitos dos trabalhadores são deveres universais, e não obrigações restritas a grandes corporações. Mais uma vez, o argumento de que empresas menores estariam dispensadas de adotar modelos de *compliance* não encontra respaldo na legislação, incluindo a LGPD.

Retomando ao texto da lei, percebe-se que a LGPD impõe um papel central ao controlador, seja na implementação da estrutura de *compliance* (art. 50, § 2º, I), seja na demonstração de efetividade quando apropriado ou solicitado pelas autoridades (art. 50, § 2º, II). Nas relações trabalhistas, esse dever pertence ao empregador-controlador, o qual deve implementar um efetivo programa de *compliance* para tutela de dados dos empregados-titulares (Brasil, 2018).

Mas a adoção de um programa de governança e *compliance*, por si só, não é suficiente: é imprescindível que ele observe os requisitos mínimos previstos no art. 50, § 2º, inciso I, alíneas ‘a’ a ‘h’ da LGPD, que detalham os elementos fundamentais para sua efetiva aplicação.

> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
> g) conte com planos de resposta a incidentes e remediação; e
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas (Brasil, 2018).

Assim, o programa de *compliance* e governança previstos na LGPD busca diminuir a exposição a incidentes de segurança, fraudes e violações, resguardando dados pessoais e evitando violações a direitos fundamentais do titular. Mais que isso, trata-se de critério utilizado na dosimetria das sanções administrativas, conforme o art. 52, da LGPD, quando já ocorrido o incidente (Brasil, 2018).

A presença de normas claras e procedimentos bem estruturados evidencia o comprometimento da empresa com a privacidade e segurança, gerando maior credibilidade e reconhecimento por parte de clientes, parceiros e outros. Sob a perspectiva do trabalhador, políticas de *compliance* em proteção de dados proporcionam um ambiente de trabalho mais seguro, transparente e confiável, no qual seus dados pessoais são tratados com respeito, responsabilidade e sigilo.

Contudo, não obstante a robustez normativa da LGPD e o detalhamento técnico das resoluções e guias, a efetiva implementação de estruturas de *compliance* em proteção de dados no contexto das relações de trabalho ainda enfrenta um paradoxo fundamental: ao mesmo tempo em que se exige um elevado grau de conformidade, ainda são esparsos os mecanismos específicos voltados à efetividade desses deveres.

Nesta problemática, a hipossuficiência e subvalorização do empregado aparecem novamente como causas centrais: o empregado – muitas vezes visto apenas como mão-de-obra – tem sua proteção limitada à esfera trabalhista da CLT, ofuscando os direitos do sujeito enquanto titular de dados perante a LGPD.

Esse fator também leva a problemas de engajamento interno – que é determinante para efetividade com *compliance*. Quando programas de conformidade são implementados “de cima para baixo”, sem diálogo com os empregados ou com os sindicatos, há um descrédito, uma baixa adesão e a sensação de que as políticas existem apenas para proteger a empresa, e não para garantir direitos.

Diante desses desafios, é essencial promover a integração entre as ferramentas de proteção de dados e os instrumentos do direito do trabalho, a fim de garantir que as políticas de *compliance* em proteção de dados sejam voltadas à efetiva tutela do empregado. Essas ferramentas não se limitam a aspectos formais ou simbólicos; elas podem – e devem – dialogar com os requisitos mínimos de efetividade previstos pela LGPD para os programas de *compliance*.

4.3 Ferramentas de *Compliance* para implementação da LGPD nas relações de trabalho

No contexto de proteção de dados de empregados-titulares, o programa de *compliance* exige a implementação de um conjunto articulado de processos, metodologias e controles – aplicados de modo sistêmico nas rotinas de recursos humanos (RH), tecnologia da informação (TI), segurança patrimonial e todos os demais setores que, de alguma forma, operam com dados pessoais.

Para tanto, ferramentas típicas de proteção de dados, como o mapeamento de dados, e instrumentos tradicionalmente trabalhistas, como treinamentos e canais de denúncia, são desenvolvidas, adaptadas e operacionalizadas com um objetivo comum: implementar a LGPD nas relações de trabalho e garantir a proteção dos dados do empregado-titular.

Ao trazer a LGPD para o *compliance* trabalhista, reconhecendo o empregado como titular de dados, essas e outras ferramentas conduzem a um ambiente laboral mais justo e seguro – evitando o aprofundamento de assimetrias e desigualdades históricas. Sobre a importância dessas ferramentas, elucida Carloto:

> O compliance trabalhista, com todas as suas ferramentas, consegue levar a empresa à conformidade, em todos os institutos trabalhistas, identificando e gerenciando riscos de desconformidade, com monitoramento contínuo, com escopo de detecção de irregularidades e de evitar-se impactos negativos aos direitos humanos dos trabalhadores, identificando-se cláusulas que deverão ser colocadas em suas políticas internas, incluindo os códigos de conduta e os regulamentos internos, para coibir os assédios moral e sexual, discriminação e quaisquer outras práticas ilícitas (Carloto, 2021, p. 34).

Assim como qualquer mecanismo de conformidade, tais ferramentas não podem se tornar meros símbolos formais, que apenas sustentam a aparência e reputação da

organização. Para que as ferramentas de *compliance* funcionem efetivamente, é crucial a participação ativa de todas as áreas da organização, do engajamento da liderança e de um processo contínuo de implementação, monitoramento e revisão.

Nas linhas a seguir, serão abordadas sinteticamente algumas das principais ferramentas de *compliance* para implantação da LGPD nas relações de trabalho, quais sejam: banco de dados, *data mapping*, políticas de privacidade, termos de uso, códigos de ética, regulamentos internos, termos de consentimento, canais de denúncia, treinamentos e capacitações e, por fim, mecanismos robustos de resposta a incidentes de segurança da informação.

4.3.1 Banco de dados

Se antes a coleta de dados de empregados se limitava à tradicional “ficha de registro”, utilizada apenas para controle burocrático, hoje – com o avanço das tecnologias e novas exigências legais – essa rotina administrativa se transformou em um sofisticado sistema de processamento e custódia de dados, concentrando desde informações básicas, como nome e endereço, até informações sensíveis, como histórico médico, afiliação sindical, crenças religiosas ou dados bancários.

Nesse cenário de grande volume de informações, o banco de dados deve ser tratado como um dos principais pontos de atenção das empresas no que se refere à proteção de dados dos empregados-titulares. As práticas de *compliance* recomendam o inventariamento completo dos dados armazenados, definindo-se a finalidade de cada coleta, os locais de armazenamento, os responsáveis pelo acesso e os controles adotados para garantir a rastreabilidade e a segurança das operações realizadas.

Para garantir a integridade do banco de dados, as organizações devem combinar mecanismos robustos de segurança – restringindo o acesso e minimizando o risco de vazamentos e eventuais sanções administrativas. Entre essas medidas, cita-se como exemplo a autenticação de dois fatores (2FA), a criptografia de dados, o controle de acesso baseado em perfis (RBAC), a realização de backups seguros e o uso de firewalls e segmentação de redes (NIST, 2020).

Neste ponto, rememore-se que o custo de investimento e a complexidade dos bancos de dados – bem como dos mecanismos de segurança – devem atender a

critérios de necessidade e proporcionalidade, compatíveis com o porte da empresa, o volume de dados, a finalidade do tratamento e os demais fatores previstos no art. 50, § 1º e § 2º, da LGPD.

Ademais, em alguns casos, a necessidade de manter performance operacional pode conflitar com medidas de segurança mais restritivas, exigindo que a empresa encontre um equilíbrio entre proteção e funcionalidade. Aqui, cabe ao empregador-controlador realizar a ponderação de princípios, auferir a probabilidade e a gravidade dos riscos e, sempre que possível, optar pela solução menos gravosa para os direitos do empregado-titular.

Por fim, a comunicação entre as áreas reforça essa responsabilidade coletiva: o compartilhamento de dados entre setores deve ser feito sempre com cautela, observando as permissões e a estrita necessidade de cada área. Cabe ao RH, juntamente com as áreas de tecnologia e *compliance*, desenvolver e adotar políticas claras, treinar operadores e garantir que todos compreendam a relevância do tema.

Nesse cenário de múltiplas operações de tratamento, não se trata apenas de armazenar a volumosa quantidade de dados: exige-se o acompanhamento detalhado do ciclo de vida desses dados. E é aqui que surge a importância do *data mapping.*

4.3.2 Mapeamento de dados (data mapping)

O *data mapping*, ou mapeamento de dados, tem como objetivo identificar, registrar e descrever todos os fluxos de dados pessoais dentro da empresa, desde a origem (fonte inicial dos dados) até as etapas subsequentes de processamento, armazenamento, acessos, integrações com bases de terceiros e até sua eventual eliminação ou anonimização.

Conforme Saavedra (2021), “O inventário de dados, também conhecido como ‘mapa de dados’ ou ‘data map’, é um dos elementos fundamentais de um sistema de gestão de compliance de dados e tem por função principal identificar os dados que transpassam vários sistemas [...]” (Saavedra, 2021, p. 1027).

Esse processo sistemático, detalhado e contínuo envolve o levantamento de quais dados pessoais são tratados, de que forma isso ocorre, por quais departamentos

ou agentes internos e externos são tratados, bem como os meios tecnológicos, físicos ou digitais utilizados para cada movimentação.

Isso inclui não apenas a identificação dos fluxos de dados entre sistemas internos, mas também entre parceiros contratados, fornecedores e ferramentas terceirizadas. Essa abrangência é especialmente relevante nas áreas de RH e Medicina do Trabalho, onde frequentemente há compartilhamento de informações com terceiros, inclusive de natureza sensível, como dados de saúde e registros biométricos.

Quando bem conduzido, o mapeamento permite a identificação de riscos de segurança, irregularidades e armazenamentos indevidos ou desnecessários e coletas excessivas. Sob a perspectiva do empregado-titular, o *data mapping* é essencial para garantir transparência sobre o uso de seus dados pessoais, pois indica quais dados são coletados, por quê, por quem e por quanto tempo.

Nesse sentido, também facilita o exercício efetivo dos direitos dos titulares, como o direito de acesso, correção, anonimização e eliminação de dados desnecessários ou tratados de forma irregular. Sem o mapeamento, a empresa sequer teria condições técnicas de localizar todos os dados relativos a um titular em tempo hábil para atender uma requisição formal.

Para Vieira (2020), especialista em privacidade de dados e GRC (governança, riscos e *compliance*), o mapa de dados deve conter informações sobre:

> 1) questões legais (contratos formais e vigentes); 2) finalidade de tratamento de dados; 3) formas coleta de dados; 4) volume de dados; 5) classificação do dado (cadastral, transacional, sensível); 6) origem dos dados; 7) base legal utilizada; 8) responsabilidade da coleta de dados; 9) locais de armazenamento dos dados (diretórios, ftps, bancos de dados, plataformas em nuvem, HDs externos, arquivos de papel), segurança da informação (acesso, proteção de senhas, desenvolvimento seguro, gestão de mudanças, monitoramento contínuo, gestão de incidentes, etc); 11) compra de dados externos (uso de enriquecimento); 12) uso de criptografia e anonimização; 13) compartilhamento de dados com parceiros (categoria de dados transferidos, canais de transferência, nível de segurança); 14) sistemas, aplicações e banco de dados que suportam o fluxo dos dados; 15) segmentação de dados de titulares (para Campanhas, análise de comportamento); 16) atendimento aos direitos do titular de dados (opout, esquecimento, consulta, correção) (VIEIRA, 2020).

No entanto, é inegável que a busca pelo nível ideal de detalhamento enfrenta desafios, seja em grandes empresas – devido à utilização simultânea de diversos

aplicativos, sistemas e softwares terceirizados –, seja em empresas menores, onde estruturas menos complexas e maior informalidade dificultam o controle das informações.

Assim, na realidade prática, o mapeamento deve ser pensado de forma adaptável, adequando-se à estrutura e capacidade de cada organização, bem como à real necessidade de detalhamento exigida pela natureza das operações empreendidas. Empresas maiores podem optar por soluções tecnológicas que automatizam o mapeamento, enquanto pequenas e médias empresas podem realizar o procedimento de forma manual, por meio de planilhas (Roxo, 2022, p. 423).

Independentemente do tamanho da empresa, o importante é garantir que todos os departamentos estejam engajados nesse levantamento, assegurando máxima abrangência à cobertura dos fluxos de dados na instituição. O engajamento interno envolve não somente o trabalho direto no mapeamento de fluxos, mas a existência de uma cultura de privacidade, em que as partes são devidamente orientadas sobre o uso de tecnologias e compartilhamento de dados.

4.3.3 Política de privacidade, Termo de Uso, Código de Ética e Conduta, Regulamento Interno

Para a implementação da LGPD nas relações de trabalho, as práticas de *compliance* orientam para existência de regras, diretrizes e orientações. No processo de formalização e organização desses dispositivos, destaca-se quatro ferramentas essenciais: política de privacidade, termos de uso, código de conduta e ética e regulamento interno.

Cada uma delas assume um papel específico, mas complementar na promoção da conformidade legal, na definição de responsabilidades e, sobretudo, na defesa dos direitos dos empregados.

Para Carvalho, Mattiuzzo e Ponce (2021, p. 516), essa é a fase de adequação de documentos – uma das etapas de implementação da LGPD nas organizações. Sobre a fase de adequação, os autores esclarecem:

> A implementação de boas práticas em uma entidade também passa pela criação e adequação de documentos internos aos princípios de

> tratamento de dados pessoais. Dentre esses documentos, ganham destaque os regulamentos ou documentos que regem a relação entre a organização e o titular de dados pessoais, assim como contratos assinados pela organização e terceiros, códigos de conduta interna (Carvalho; Mattiuzzo; Ponce, 2021, p. 516-535).

Embora os termos de uso sejam mais conhecidos por sua aplicação na esfera consumerista, também têm papel relevante na esfera trabalhista, ao estabelecerem, de maneira transparente e formal, as regras e condições de acesso e utilização dos recursos tecnológicos disponibilizados pela empresa – como sistemas internos, e-mails corporativos, aplicativos móveis, ambientes virtuais de aprendizagem e outros.

Se por um lado o empregado-titular toma ciência sobre a conduta que lhe é esperada, por outro se resguarda de cobranças arbitrárias ou abusivas – devendo sempre haver um equilíbrio entre a proteção jurídica da empresa e a proteção de direitos fundamentais do empregado.

Por sua vez, a política de privacidade dialoga diretamente com a LGPD, devendo indicar os direitos do empregado-titular e possibilitar que identifique quais dados são coletados (dados de identificação, registros de ponto, bancários, produtividade e outros), qual a finalidade específica do tratamento (folha de pagamento, benefícios, avaliações internas), como são armazenados, com quem podem ser compartilhados, e demais informações pertinentes.

Já o código de ética funciona como uma bússola moral e comportamental, transmitindo à comunidade interna e externa a seriedade com que a empresa encara questões como respeito à privacidade, transparência e integridade na gestão das informações. Esse instrumento contribui para que o respeito à privacidade seja internalizado como valor central da empresa.

A internalização dos valores éticos, no entanto, depende menos do conteúdo normativo do código e mais de sua vivência cotidiana. Caso o código de ética não dialogue com a realidade cultural da empresa e não seja amplamente difundido e adotado – inclusive pela liderança –, permanece apenas como peça de marketing institucional. Assim, a sua efetividade exige coerência entre discurso e prática.

No regulamento interno, as normas legais – muitas vezes de difícil compreensão – e os princípios abstratos do código de conduta são transformados em regras claras, de fácil aplicação, direcionadas aos empregados e empregadores. Esse documento

especifica, por exemplo, quem pode acessar determinados dados, como são tratadas informações sensíveis e que providências devem ser tomadas em casos de incidentes ou vazamentos.

Ressalte-se que, na fase de adequação, o dever de conformidade com a LGPD não se encerra com criação desses documentos, sendo necessária a existência de um Programa de Privacidade e Proteção de Dados Pessoais permanente, composto por ações e revisões constantes, conforme elucida Roxo:

> O Programa de Privacidade e Proteção de Dados Pessoais tem como ações a revisão dos procedimentos internos, a adequação do fluxo de tratamento dos dados e a implementação de novos procedimentos. É necessário também revisar os contratos e documentos existentes e consolidar os novos documentos. Os documentos que envolvem os dados dos empregados devem ser revisados e, se necessário, substituídos. É necessário revisar os contratos de trabalho, regulamento de empresa, manual de conduta, controles de jornada e demais documentos sob a ótica da cultura da privacidade e proteção de dados pessoais. (Roxo, 2022, p. 433).

Esse processo de criação, revisão e substituição de documentos demanda atuação conjunta dos departamentos de RH, TI e jurídico, sendo essencial que haja um sistema de gestão e organização desses instrumentos, tanto para registro de revisões e atualizações, como de comunicações e manifestações de ciência.

Um ponto sensível nesse processo é a acessibilidade e clareza dos instrumentos. No cotidiano das organizações, é comum que esses documentos utilizem uma linguagem excessivamente técnica, pouco acessível aos empregados e, muitas vezes, acessíveis apenas em meio digital, dificultando a compreensão de indivíduos com menor familiaridade tecnológica.

Nesse contexto, o objetivo de reduzir a vulnerabilidade informacional deve orientar os agentes de tratamento – principalmente o controlador-empregador – na implementação de instrumentos claros e acessíveis. À luz do princípio da proteção e da transparência, o empregado-titular deve ser capaz de entender, sem dificuldades técnicas ou jurídicas, quais os seus direitos e deveres enquanto titular de dados.

Ademais, é importante reconhecer que qualquer regra interna, por mais bem elaborada que seja, permanece vulnerável caso não seja acompanhada de mecanismos de fiscalização ativa e prestação de contas, sob risco de produzir um

compliance de fachada, dissociado da realidade organizacional e com fins meramente simbólicos e formais.

Em síntese, para além da elaboração formal de Políticas de Privacidade, Termos de Uso, Código de Ética e Regulamentos Internos, é essencial que sua efetividade seja garantida por meio da aplicação prática, linguagem acessível e fiscalização permanente, evitando o risco de um *compliance* meramente simbólico. Apenas assim será possível proteger de fato os direitos dos trabalhadores e promover uma cultura organizacional comprometida com a privacidade e a transparência.

4.3.4 Termo de consentimento

O consentimento previsto na LGPD é um mecanismo jurídico de grande relevância, porém – como já esclarecido – seu uso no contexto trabalhista demanda cautela, uma vez que a assimetria das relações pode comprometer a livre manifestação de vontade do empregado.

De forma categórica, Bomfim e Pinheiro (2022, p. 51) alertam: “como medida de 'compliance', para qualquer tipo empregado, visando à gestão e mitigação de riscos, é recomendável evitar a utilização do consentimento como base legal de tratamento de dados no âmbito das relações de trabalho”. Essa advertência revela que, longe de garantir proteção, o consentimento pode facilmente se esvaziar, tornando-se mais uma estratégia de blindagem jurídica destinada a legitimar práticas empresariais.

Apesar dessas restrições, é certo que o consentimento pode ser necessário em situações específicas, notadamente quando o tratamento de determinados dados não encontra respaldo nas demais hipóteses legais previstas pela legislação.

Como exemplo, cita-se a manutenção de currículos em bancos de talentos, o uso da imagem e depoimentos de funcionários em campanhas institucionais e de marketing, o processamento de dados para integrar rankings comparativos de produtividade, bem como a divulgação de nomes, datas e imagens para comemorações de aniversários.

Rememore-se que, quando utilizada a base legal do consentimento, o titular de dados faz jus a direitos específicos. No caso das relações de trabalho, o empregado-titular deve ser informado sobre a possibilidade de não fornecer o consentimento e sobre as consequências da negativa (art. 18, VI). Após o

consentimento, o titular tem o direito de revogar o aceite (art. 18, IX) e de requerer a eliminação dos dados (art. 18, VI) (Brasil, 2018).

Além disso, ao aplicar essa base legal, o controlador-empregador deve garantir que o consentimento seja destacado, específico e devidamente documentado, conforme dispõe o art. 8º, §1º, 2º e 3º, da LGPD (Brasil, 2018).

A forma destacada exige que o consentimento seja tratado em cláusula destacada das demais quando previsto em contrato. Ocorre que, considerando que os contratos de trabalho possuem natureza de contrato de adesão, as boas práticas de *compliance* orientam para coleta de consentimento em instrumentos autônomos, utilizando-se – por exemplo – termos de consentimento.

O objetivo é garantir que a manifestação de vontade do empregado-titular acerca do uso de seus dados não esteja vinculada a outras obrigações contratuais que venham a influenciar o ato de aceite. Ademais, em empresas com muitos trabalhadores, o termo apartado facilita a gestão e organização dos consentimentos, inclusive para fins de revogação, modificação e correção à pedido do titular.

Ademais, o consentimento deve ser específico para cada finalidade de tratamento e não genérico, permitindo ao titular escolher de modo independente as causas para as quais autoriza o uso de seus dados. Nesse sentido, o aceite específico também dialoga com a proteção contra o compartilhamento indevido de dados, uma vez que exige o consentimento específico para essa operação.

Para Bomfim e Pinheiro (2022, p. 52) essa consequência da especificidade “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”.

De fato, nos contratos laborais – em que o empregado hipossuficiente tende a aceitar quaisquer condições contratuais em prol do trabalho – é inegável o potencial que tem a garantia da especificidade na promoção da liberdade e autonomia negocial. Contudo, na prática, a assimetria das relações trabalhistas conduz à repetição do problema geral do consentimento: o empregado-titular se sente coagido a autorizar todas as condições, ainda que de modo específico.

Trata-se, na realidade, de uma “autonomia ilusória”, seja porque o titular não tem conhecimento da possibilidade de recusa, em contrariedade com o direito à informação, seja porque – ainda que o tenha – acredita que sofrerá sanções e retaliações caso não aceite o tratamento. Em muitas empresas, essa crença se revela uma realidade.

Em suma, para ser legítimo, o termo de consentimento precisa ser radicalmente diferente de um mecanismo de autoproteção das organizações. Deve traduzir, na prática, a possibilidade de o trabalhador exercer sua autonomia, revogar, corrigir, eliminar ou se opor ao tratamento de dados – sem medo de sanções ou discriminação.

Nesta seara, é essencial que as empresas invistam não apenas na adequação dos termos formais, mas também na conscientização de seus empregados, capacitando-os para o exercício dos direitos previstos na LGPD. Sem essa consciência sobre dados e privacidade, o consentimento – ainda que específico, destacado e documentado – dificilmente representará a verdadeira autonomia do empregado-titular, permanecendo como base legal inadequada para as relações de trabalho.

4.3.5 Treinamentos e capacitações

A consolidação do *compliance* em privacidade exige mais do que políticas documentais e processos sofisticados: para que a proteção de dados se torne um valor intrínseco e espontâneo na organização, é necessário preparar e treinar funcionários e agentes de tratamento para lidar corretamente com dados pessoais.

A respeito do tema, Vieira (2020) explica que as “pessoas são o elo mais fraco de toda a cadeia de tratamento de dados” e, por esse motivo, é essencial que o programa de *compliance* inclua o treinamento e capacitação dos empregados e demais envolvidos. A seu turno, Carloto (2021, p.134) destaca que “dificilmente todos os trabalhadores lerão todas as cláusulas de um código de conduta, ou de um regulamento empresarial”, reforçando a importância dos treinamentos para conscientização e instrução de empregados.

Os programas de treinamento devem abordar de forma concreta as situações reais enfrentadas pelos setores, sem se ater a conceitos abstratos sobre privacidade. Por exemplo: o setor de RH precisa padronizar os procedimentos de coleta de currículos e descarte de dados; a equipe de TI deve garantir o acesso restrito a bancos

de dados e implementar medidas de segurança adequadas; os médicos do trabalho devem estar cientes sobre a natureza sensível dos dados de saúde, atuando cautela na coleta e manuseio dessas informações.

No cenário atual de constantes mudanças tecnológicas e normativas, é fundamental que o conteúdo abordado nas capacitações seja regularmente atualizado, para incluir abordagens sobre incidentes recentes, alterações regulatórias ou decisões da ANPD que impactem a rotina interna. Quando os treinamentos são repetitivos, desatualizados ou excessivamente genéricos, é comum que haja menor adesão ou atenção das partes envolvidas.

Assim, entre as estratégias para aumentar o engajamento e a efetividade do treinamento, cita-se a realização de workshops práticos, simulações de incidentes de vazamento de dados ou estudos de caso reais. Ademais, o engajamento também exige uma organização interna do volume e metas de trabalho, para garantir a participação genuína dos empregados – não apenas a presença passiva.

É fundamental que cada treinamento seja documentado, com registro dos participantes, aplicação de avaliações ou testes de assimilação e disponibilidade de materiais de consulta atualizados. Esse cuidado não apenas facilita auditorias internas e externas, como também comprova para a ANPD e demais partes interessadas o compromisso genuíno da empresa com a conformidade e com o desenvolvimento de uma cultura robusta de proteção de dados.

Em última análise, um programa de treinamentos só será legítimo e eficaz se repercutir mudanças reais nas ações cotidianas, nos processos internos e, principalmente, na responsabilidade ética de todos os envolvidos. Do contrário, todo o esforço não passará de mais um ritual simbólico, perpetuando práticas que fragilizam a proteção de dados no ambiente de trabalho.

4.3.6 Canal de Denúncias

O Canal de Denúncias é parte vital do sistema de *compliance*, pois oferece aos empregados uma via formal, segura e, muitas vezes, anônima para relatar condutas inadequadas ou ilícitas no ambiente corporativo. Com a promulgação da LGPD,

tornou-se imperativo reestruturar esse canal para atender às novas exigências legais e proteger os direitos dos titulares de dados.

A existência de um canal de denúncias em conformidade com a LGPD exige, primeiramente, a segurança das informações compartilhadas, incluindo o conteúdo da denúncia e os dados do denunciado e denunciante – sendo possível, neste ponto, realizar o processo de anonimização dos dados pessoais do denunciante quando pertinente, previsto no art. 12 da LGPD (Brasil, 2018).

Aqui, surge a controvérsia sobre revelar ou não a identidade do denunciante em casos de denúncias infundadas: se por um lado é importante proteger quem denuncia para incentivar a apuração de irregularidades, por outro denúncias falsas podem prejudicar injustamente terceiros (Neves, 2024, p. 467). Não havendo disposição legal específica sobre o tema, cabe à organização definir políticas claras de proteção e, se necessário, de revelação da identidade do denunciante, sempre considerando os princípios legais e as circunstâncias do caso concreto.

De toda sorte, mantém-se sempre a lógica da minimização: apenas os dados necessários para o processamento da denúncia devem ser coletados. As medidas de segurança devem evitar o acesso de pessoas não autorizadas, bem como situações acidentais ou ilícitas de destruição, perda, alteração e compartilhamento de dados, atendendo ao princípio da Segurança e Prevenção, previstos na LGPD.

Para atender ao princípio da Finalidade, o Canal de Denúncias deve ater-se aos objetivos éticos e jurídicos, para investigar e penalizar atos inadequados – jamais para caluniar ou prejudicar indivíduos inocentes. Não apenas a denúncia propriamente dita, mas outros documentos produzidos ao longo da investigação também devem ser tratados em conformidade com a lei. Gimenez chama atenção para a necessidade de discrição nesses procedimentos:

> [...] Uma denúncia poderá ser tratada, seja pelo departamento interno da companhia ou pelo terceirizado, de forma responsável, e com expertise, além de toda discrição, pois estamos tratando de fatos sensíveis envolvendo a organização, que poderão relacionar situações de assédio, corrupção, e vida privada dos trabalhadores (Gimenez, 2024, p. 475)

Essa responsabilidade deve ser redobrada diante do tratamento de dados sensíveis, comuns em denúncias laborais, que muitas vezes tratam de situações de

assédio, abusos de poder e aspectos privados da vida dos empregados. O equilíbrio, aqui, consiste em tratar cada caso com discrição e rigor investigativo, resistindo tanto à banalização quanto ao uso punitivista do canal.

Ademais, essa ferramenta também deve ser adaptada para receber e tratar denúncias relacionadas especificamente a violações de privacidade e à gestão inadequada de dados pessoais. Isso implica na criação de procedimentos específicos para identificar, investigar e remediar incidentes que envolvam o uso indevido ou não autorizado de informações pessoais, assegurando a conformidade com a LGPD.

A expansão do escopo dos canais de denúncia representa não só adequação à nova legislação, como oportunidade de consolidar uma cultura em que a proteção de dados se insere no rol dos valores institucionais e é incorporada à rotina com naturalidade. Ainda assim, é necessário investir em comunicação clara e treinamentos periódicos, para que todos saibam como utilizar a ferramenta, quais seus direitos e como acompanhar o desdobramento das denúncias.

Percebe-se, portanto, que um canal de denúncias adaptado às demandas modernas dialoga diretamente com a implantação da LGPD nas relações de trabalho, tanto por envolver a coleta e uso de dados, como por abrir espaço para denúncias de violações à privacidade dos empregados. O equilíbrio entre proteção, transparência e responsabilização é o vértice do sucesso desse mecanismo na proteção de dados pessoais dos empregados.

4.3.7 Ferramentas de Resposta a Incidentes de Segurança

Embora a prevenção e a antecipação de riscos à segurança sejam pilares indispensáveis de um programa de *compliance* em proteção de dados, essas medidas, por si só, não garantem a imunidade das organizações diante de ameaças cada vez mais sofisticadas. É fundamental reconhecer que, invariavelmente, falhas podem ocorrer – seja por deslizes humanos, seja por vulnerabilidades técnicas.

Diante desse cenário, não basta adotar práticas preventivas e controles; torna-se imprescindível que a organização esteja preparada para reagir de forma estruturada e eficiente quando um incidente de segurança se concretizar, buscando identificar

rapidamente sua origem, conter seus efeitos e mitigar as consequências para os titulares dos dados e para a própria empresa.

As práticas de *compliance* recomendam a adoção de mecanismos ágeis para gestão desses incidentes, capazes de identificar eventos anômalos em tempo real, disparar alertas e acionar respostas previamente definidas, como ocorre em plataformas de *Security Information and Event Management* (SIEM) (Palhares, Francoski, 2024).

No tocante à contenção técnica e remediação, destacam-se ferramentas de isolamento do sistema, bloqueio imediato de acessos, realização de backups emergenciais e outros – direcionados não apenas para o sistema comprometido, mas para os demais que a ele se conectem. Essas medidas trazem segurança à rotina empresarial, impedindo que falhas ou ataques resultem em maior exposição de dados.

O Engenheiro de Computação Fábio José Buchedid Vazques identifica protocolos e medidas práticas que devem ser adotadas durante o incidente de segurança de dados, a saber:

> Protocolos: [...] 5. Levantar e reunir todas as informações do incidente. Definir se o problema foi interno dos funcionários ou externo. 6. Correção imediata da vulnerabilidade sistêmica [...] 10. Alerta de incidente aos funcionários da empresa. [...] 12. Medidas judiciais e pedido de instauração de inquérito policial; 13. Levantamento da necessidade de confecção do Relatório de impacto para a Autoridade Nacional de Proteção de Dados (ANPD) [...] 16. Verifique a necessidade de o titular do dado realizar alguma ação afirmativa (cancelamento do cartão de crédito, por exemplo) [...] (Vazques, 2024, p. 117).

Para Lima (2022), caso haja um incidente de segurança de dados, a empresa deve apurar, entre outras informações, o número de titulares atingidos, a facilidade ou não de identificação dos titulares e a gravidade das consequências para os titulares. No contexto laboral, tal análise prévia é essencial para direcionar medidas imediatas de proteção ao empregado afetado e promover orientações preventivas.

Essa coleta de informações dialoga diretamente com o princípio da transparência e com o dever de comunicação de incidentes, previstos nos arts. 47 a 49 da LGPD (Brasil, 2018). A comunicação tempestiva e assertiva é pilar ético, jurídico e estratégico, que reforça a confiança dos trabalhadores na empresa e impede agravamentos desnecessários.

Para tanto, é essencial a existência de um canal direto entre empregador e empregado – como e-mail institucional ou aplicativo de mensagens – por onde o empregado seja prontamente informado sobre vazamentos e riscos, e orientado sobre ações corretivas, como alteração de senhas ou bloqueio de cartões (Vazques, 2024, p. 117).

Outro aspecto relevante é a integração dos sistemas de gestão de incidentes, evitando a fragmentação de informações e decisões. Neste ponto, a atuação coordenada multiprofissional – envolvendo TI, jurídico, RH, marketing e alta gestão – é condição necessária para respostas completas, consistentes e que traduzam o compromisso institucional real com a privacidade.

Em meio a tantos protocolos e agentes acionados, é aconselhado às empresas a integração dos sistemas de gestão de incidentes, para que todos os envolvidos estejam cientes dos procedimentos a serem adotados. Para tanto, são adequados aplicativos de *workflow*, que permitem distribuir responsabilidades, acionar automaticamente os membros do comitê de crise e realizar avaliações periódicas de protocolos.

Além do aspecto normativo, ter um plano robusto de resposta a incidentes contribui para a imagem da empresa, demonstrando responsabilidade e comprometimento com a integridade das informações dos empregados-titulares.

Reitere-se, contudo, que a adequação das medidas de segurança e das ferramentas de resposta a incidentes deve considerar o porte da empresa, o volume e a sensibilidade dos dados tratados e outros critérios de necessidade e proporcionalidade. Uma pequena empresa com operações limitadas e poucos titulares de dados não está sujeita às mesmas ameaças, nem precisa adotar a mesma infraestrutura tecnológica de grandes corporações que manipulam informações altamente sensíveis e possuem extensa cadeia de tratamento.

Assim, é evidente que a efetividade das ferramentas de resposta a incidentes de segurança depende não apenas da adoção de protocolos sólidos e tecnologias apropriadas, mas, sobretudo, do alinhamento dessas práticas à realidade específica de cada organização.

4.4 *Compliance* ao longo do processo contratual trabalhista

As ferramentas de *compliance* não se esgotam em medidas pontuais e isoladas, sendo fundamental compreendê-las à luz do ciclo de vida dos dados pessoais – que, nas relações trabalhistas, abrange as fases pré-contratual, contratual e pós-contratual. O percurso dos dados se inicia na coleta, durante o recrutamento (fase pré-contratual), passa pela gestão e uso durante a vigência do contrato (fase contratual) e chega ao armazenamento e descarte após a rescisão (fase pós-contratual).

Apesar de, na prática, ser perceptível uma maior preocupação das empresas com medidas de proteção de dados na fase contratual, tal zelo não pode se restringir ao período em que o vínculo empregatício está em vigor, como pondera Janz (2022):

> De fato, o elevado fluxo de dados tratados nas relações de trabalho faz com que seja necessária ampla atenção sobre a questão, notadamente porquanto o empregador tem acesso a uma grande quantidade de dados pessoais de seus empregados, desde as fases pré-contratuais, em decorrência de processos seletivos e de admissão, e até a fase pós-contratual, ante o dever de guarda dos documentos do vínculo de emprego. (Janz, 2022, p. 207).

Visualizar essas ferramentas sob a ótica do ciclo de dados permite que a empresa avalie riscos e implemente salvaguardas específicas para cada etapa, garantindo que a conformidade e o respeito aos direitos dos empregados estejam presentes em todo o fluxo da informação – e não apenas em momentos fragmentados.

Nas linhas subsequentes, serão detalhados os principais aspectos e medidas de *compliance* aplicáveis a cada uma dessas etapas: fase pré-contratual, fase contratual e fase pós-contratual.

4.4.1 Fase pré-contratual

Na fase pré-contratual – composta pelas etapas de negociação, proposta de emprego e aceitação – o *compliance* orienta que a coleta de informações dos candidatos seja limitada ao mínimo necessário, considerando somente aqueles dados imprescindíveis para o registro do candidato e para avaliação das competências técnicas e profissionais do titular.

Assim, além de dados pessoais – como nome, telefone, e-mail, CPF e endereço – é admissível solicitar currículo, comprovantes de escolaridade, certificações específicas correlatas à função, e referências profissionais. Por outro lado, exigir informações excessivas e sensíveis sobre opiniões políticas, orientação sexual, gravidez, religião e outros aspectos da vida privada pode configurar potencial violação à LGPD e resultar práticas discriminatórias, contrárias aos valores constitucionais.

Do ponto de vista procedimental, a escolha dos dados a serem coletados nessa etapa exige o mapeamento das funções do cargo e da legislação aplicável, para fundamentar cada dado requisitado. Exemplo disso são os antecedentes criminais, que – apesar de serem dados sensíveis – podem ser solicitados do candidato quando a natureza do ofício exigir alto grau de confiança (Bomfim; Pinheiro, 2022, p. 45).

Independentemente do canal de recebimento dos currículos – seja presencialmente, por e-mail ou via sistemas eletrônicos –, é fundamental que todos os trâmites estejam previstos em políticas internas de privacidade. Estes documentos devem detalhar não apenas os procedimentos para coleta e armazenamento, mas também orientar sobre o consentimento dos candidatos, o compartilhamento de informações com terceiros, o tempo de guarda dos dados e o processo de descarte.

Quando o currículo for entregue pessoalmente, o titular deve autorizar o tratamento de dados, prestando seu consentimento de modo livre, informado e inequívoco. Quando a entrega do currículo se der por terceiros, o professor Alan Martinez Kozyreff alerta:

> A entrega do currículo por um terceiro é motivo de polêmica, pois quem realizar a entrega não poderá consentir com o tratamento. Dessa forma, o recrutador pode instituir como política não receber currículo por terceiro ou ainda reservar um local para buscar o consentimento do titular de alguma forma (Kozyreff, 2024, p. 41).

Em hipótese de envio de currículo por e-mail, as práticas de compliance recomendam a prévia devolução do e-mail, de modo a solicitar o consentimento do candidato para o tratamento de dados. Para garantir a manifestação livre, inequívoca e informada do titular, pode ser enviado termo de consentimento para assinatura e, apenas após a autorização, deve a empresa dar prosseguimento ao tratamento de dados (Kozyreff, 2024, p. 41).

De forma semelhante, quando o currículo for enviado por meio de plataforma de recrutamento, uma possibilidade é que o upload do arquivo (contendo o currículo) preceda a leitura do Termo de Uso e de Privacidade e a demonstração de consentimento – por exemplo, pela marcação das denominadas checkboxes.

Se os procedimentos de recrutamento e seleção de candidatos forem realizados por agente externo, como empresa terceirizada, é necessário que o titular de dados seja cientificado sobre o compartilhamento de seus dados – previamente à demonstração de consentimento.

Diante disso, é evidente a importância de termos de consentimento na fase pré-contratual, de modo destacado, específico e documentado, seja por meio de procedimentos eletrônicos – como checkboxes obrigatórios –, seja por documentos físicos, contendo a assinatura a punho do candidato.

Internamente, o *compliance* demanda a existência de políticas e diretrizes rigorosas, principalmente quanto à disponibilidade dos currículos (e dados pessoais) na base de dados da empresa. Isto porque, principalmente em empresas de grande porte, é comum que os currículos fiquem acessíveis para outras equipes, setores e filiais, seja por falta de organização, seja para facilitar novos processos seletivos.

Aqui, surge um problema de manutenção, acesso e compartilhamento dos currículos, como explica Guilherme Neves:

> Uma prática comum nas empresas é disponibilizar o currículo dos candidatos aos entrevistadores ou gerente de vaga (aqui podemos também refletir se há real necessidade de entrevistadores terem acesso aos dados completos de candidatos). Caso o currículo seja compartilhado com entrevistadores via e-mail, após a realização do processo seletivo, estas pessoas continuarão com o acesso aos dados pessoas (e confidenciais) sem que haja finalidade objetiva, uma vez que a vaga tenha sido fechada com outro candidato (Neves, 2024, p.131).

Nesse contexto, as ferramentas de *compliance* conectadas a banco de dados, especialmente com mecanismos de controle de acesso, podem ser utilizadas para restringir o acesso aos dados dos candidatos apenas aos responsáveis diretos pela seleção.

Ademais, ao receber e repassar currículos, os profissionais de recursos humanos devem ter em mente que estão compartilhando dados pessoais dessas pessoas, uma

vez que – no currículo profissional – geralmente constam informações do candidato que permitem sua identificação direta ou indiretamente, como nome, telefone, e-mail, formação acadêmica e outros.

Em suma, caso a empresa opte por armazenar os currículos de candidatos não admitidos em banco de dados, os ditames da *compliance* recomendam: a) solicitar o consentimento do titular para manutenção e compartilhamento do currículo, de modo que haja base legal para o tratamento; b) informar os fins pretendidos (como a integração em banco de talentos), onde e por quem poderão ser utilizados (filiais e terceirizados, por exemplo), tempo de manutenção e processo de descarte dos dados.

Neste ponto, políticas de privacidade e termos de consentimento bem estruturados podem assumir papel central na conformidade com a LGPD na fase pré-contratual. Trata-se de dupla garantia: de um lado, amparam a empresa responsável pelo processo seletivo perante a fiscalização e o judiciário; de outro, protegem os direitos do titular, ora candidato à vaga.

Para facilitar a estruturação desses documentos formais, o mapeamento de dados pode revelar-se uma ferramenta essencial, pois identifica quais dados trafegam desde o recebimento do currículo até sua eventual exclusão, por onde trafegam, a finalidade do tratamento e outras informações. A partir dessa base de conhecimento, o RH pode elaborar políticas de privacidade mais completas e transparentes e fundamentar os pedidos de consentimento.

Além dos cuidados com a coleta de currículos, é fundamental atentar para o crescente uso de sistemas automatizados e algoritmos nos processos seletivos, sobretudo em grandes organizações que empregam inteligência artificial no recebimento, análise e triagem de currículos.

Esses sistemas têm como propósito principal identificar, entre os candidatos, aqueles com o “perfil ideal” para determinada vaga. Ocorre, porém, que os algoritmos aprendem a partir de grandes volumes de dados históricos. Se os dados originários refletem padrões de desigualdade estrutural – como preferências por determinados gêneros, raças ou idades –, o resultado pode ser a perpetuação ou até o agravamento dessas distorções na etapa de seleção.

Exemplo disso são os sistemas de triagem que raqueiam currículos a partir de critérios enviesados, como podem levar à exclusão automática de perfis de grupos minoritários, mesmo quando os indivíduos apresentam qualificações equivalentes.

Rememore-se que a LGPD, em seu art. 20, caput e § 1º, estabelece o direito do titular de revisão e explicação quando decisões forem tomadas unicamente com base em tratamentos automatizados. Para candidatos e empregados, esse dispositivo representa um mecanismo de proteção à discriminação algorítmica, como elucida Bioni:

> A Lei Geral de Proteção de Dados (Lei 13.709/2018) inaugura esse regime com o direito de revisão de decisões automatizadas, previsto em seu art. 20, caput. Além disso, o art. 20 §1º vem sendo entendido por alguns autores como uma garantia de direito à explicação. Ambas são importantes salvaguardas que permitem uma permeabilidade do Direito nos processos algoritmos (Bioni, 2020).

Assim, para assegurar a conformidade com a LGPD e mitigar os riscos de exposição à discriminação algorítmica, torna-se indispensável incluir auditorias regulares e avaliações sobre os critérios adotados nos procedimentos de recrutamento e seleção. Ademais, deve ser garantida a transparência da decisão uniformizada, bem como o direito à revisão e à explicação desse procedimento.

Dessa forma, na fase pré-contratual, pode ser necessária a reestruturação dos processos seletivos por parte dos Recursos Humanos (RH), de modo a adequar procedimentos, solicitando apenas informações relevantes para eventual admissão e, em regra, requerendo o consentimento para o tratamento de dados e eventual manutenção. Mais do que a reestruturação do processo, a prática de *compliance* conduz ao treinamento contínuo dos funcionários – neste caso, os de recursos humanos.

4.4.2 Fase contratual

Na fase contratual, o empregador tem acesso contínuo a um volume maior de dados pessoais sensíveis, incluindo documentos para registro, informações bancárias, dados biométricos e atestados médicos.

Se no momento pré-contratual o cuidado estava centrado nos limites da coleta e tratamento de dados do candidato, uma vez firmado o vínculo empregatício, o foco

desloca-se para a incorporação desses princípios nas rotinas diárias, permeando desde a admissibilidade do contrato até a gestão cotidiana das informações pessoais do trabalhador.

O RH, setor diretamente envolvido na gestão de dados, deve adotar protocolos rigorosos de acesso, manipulação e armazenamento dessas informações. A lógica da mínima coleta se mantém e somente funcionários autorizados devem acessar bancos de dados, reduzindo o risco de vazamentos e usos indevidos. Aqui, a existência de sistemas de controle de acesso, e autenticação em dois fatores, registros de logs e senhas são medidas de segurança recomendadas.

Nesta fase, a formalização do vínculo empregatício acentua ainda mais a assimetria nas relações e a vulnerabilidade do trabalhador, o que reforça a inadequação da base legal do consentimento, atraindo a incidência de outras hipóteses de tratamento de dados.

Como esclarecido alhures, a base legal mais frequentemente utilizada é o cumprimento de obrigação legal ou regulatória, já que grande parte dos dados coletados e processados – como informações para registro de funcionários, elaboração da folha de pagamento, recolhimento de encargos sociais e emissão de guias trabalhistas e previdenciárias – está vinculada a determinações da legislação trabalhista, fiscal e previdenciária.

Além das bases legais relativas ao cumprimento de obrigação legal ou regulatória, também se observa a base de execução do contrato. Dados indispensáveis para a prestação dos serviços, gestão de benefícios, controle de jornada, concessão de vale-transporte, plano de saúde e outros direitos trabalhistas podem ser coletados e processados sem necessidade de consentimento, desde que haja vínculo direto com a execução do contrato.

Outro ponto central para o programa de *compliance* na fase contratual é atentar para a utilização de ferramentas de vigilância digital, como ferramentas de geolocalização e câmeras de segurança. Nesses casos, para apurar a legitimidade e legalidade dessas ferramentas, BIONI propõe a realização do “teste de proporcionalidade”, composto por 4 etapas:

> a) Verificação da legitimidade do interesse: situação concreta e finalidade legítima (art. 10, caput e I, da LGPD) [...]
> b) Necessidade: minimização e outras bases legais (art. 10, § 1º , da LGPD) [...]
> c) Balanceamento: impactos sobre o titular dos dados e legítimas expectativas (art. 10, II, da LGPD) [...]
> d) Salvaguardas: transparência e minimização dos riscos ao titular do dado (art. 10, §§ 2º e 3º , da LGPD) (Bioni, 2018, p. 324-328).

No caso da geolocalização, o teste exige a verificação de uma finalidade legítima, vinculada à base legal, como garantir a segurança do empregado-titular (cumprimento de obrigação legal) ou atender ao interesse do empregador de proteger a sua empresa (legítimo interesse); o exame de necessidade verifica se existem meios menos invasivos para alcançar o mesmo fim; já o balanceamento demanda que o rastreamento ocorra exclusivamente durante o expediente, resguardando a privacidade do empregado fora do horário de trabalho.

De modo similar, no monitoramento por câmeras, o teste de proporcionalidade avalia se há propósitos legítimos, como a segurança do ambiente (legítimo interesse) ou fiscalização do uso de EPI's (cumprimento de obrigação legal). A premissa de necessidade impõe que a medida seja restrita a locais adequados, sem expor áreas de intimidade como vestiários ou banheiros, enquanto o balanceamento requer a ponderação dos direitos de privacidade frente ao direito de propriedade do empregador.

Ao refletir sobre o tema, Silva (2022) reforça a necessidade de informar o funcionário previamente sobre o monitoramento, em observância ao princípio da transparência:

> [...] para que ocorra o tratamento das imagens, deverá existir prévia informação ao trabalhador sobre o monitoramento, com a indicação de sua finalidade, sem possibilidade, de tratamento posterior de forma incompatível com essas finalidades, com a observância dos demais princípios elencados no art. 6° da LGPD (Silva, 2022, p. 482).

Em relação ao controle de acesso à internet e monitoramento de e-mails, a proporcionalidade conduz à necessidade de se diferenciar equipamentos de propriedade do empregador e do empregado, e-mails pessoais e e-mails corporativos. Aqui, o interesse legítimo reside na proteção do patrimônio eletrônico e informações sensíveis. Contudo, o critério de necessidade recomenda a adoção de medidas menos invasivas, como filtros de navegação e antivírus, ao invés do monitoramento direto.

Ainda, em caso de registro biométrico de jornada, a aplicação do teste inicia-se pela identificação de uma finalidade legítima – que será geralmente o cumprimento de obrigação, já que o controle de jornada é dever do empregador em estabelecimentos com mais de 20 funcionários (Art. 74, §2º CLT).

Mais uma vez, o exame de necessidade exige a demonstração de que a biometria é indispensável para garantir a autenticidade dos registros. Para Bomfim e Pinheiro (2022, p. 51), ainda que existam outros instrumentos para controle de jornada, o registro biométrico por impressão digital, íris, face e voz demonstram maior eficácia na garantia de integridade e autoria dos registros.

No entanto, por se tratar de dados sensíveis, os registros biométricos merecem proteção redobrada na fase de balanceamento e salvaguardas. Com a tecnologia permeando a seara privada, o vazamento de dados biométricos pode gerar danos irreparáveis ao titular, seja pelo potencial acesso indevido a redes sociais e contas bancárias, seja pela própria afronta ao direito fundamental à privacidade.

Outro ponto delicado na fase contratual é o compartilhamento de dados com terceiros, como fornecedores de benefícios, empresas de medicina do trabalho, planos de saúde ou parceiros de tecnologia. Nessa seara, a transferência de dados deve ser expressamente autorizada pelas bases legais, cabendo ao empregador-controlador garantir que o terceiro possua medidas de segurança em proteção de dados.

Diante disso, considerando o volume de operações com dados na fase contratual, torna-se ainda mais perceptível das políticas de privacidade, que devem ser acessíveis aos empregados, detalhando quais informações são coletadas, como são utilizadas, com quem são compartilhadas e quais medidas de segurança são adotadas para garantir a confidencialidade e integridade dos dados, bem como os direitos do titular, tais como correção, eliminação e bloqueio, respeitados os limites legais.

Aqui, recomenda-se a integração das políticas internas à rotina dos empregados por meio de canais de comunicação fáceis, e inclusive do canal de denúncias, instrumento já amplamente utilizado em *compliance* trabalhista e agora fundamental para relatar práticas inadequadas relativas à proteção de dados pessoais. O anonimato e o sigilo no tratamento dessas denúncias reforçam o compromisso da empresa com o ambiente ético e seguro.

Somado a isso, as boas práticas de *compliance* passam a exigir auditorias colaborativas, padronização de contratos e uma dinâmica de responsabilização compartilhada – avanços que ampliam a maturidade institucional, mas criam demandas adicionais e desafios práticos de fiscalização e integração.

Em conclusão, na fase contratual, o desenvolvimento da estrutura de *compliance* depende do diálogo permanente entre empregador, atentando-se para todos os momentos e procedimentos do cotidiano laboral que, de algum modo, envolvem o manuseio de dados pessoais do empregado-titular.

4.4.3 Fase pós contratual

Após o encerramento do vínculo empregatício, despontam novos desafios para o *compliance* e a aplicação da LGPD, exigindo a adoção de critérios estritos, tanto para a manutenção quanto para o descarte dos dados pessoais do ex-empregado. Enquanto houver guarda de dados, o ex-empregado permanece como titular, fazendo jus aos direitos previstos na lei.

Na fase pós-contratual, a finalidade do tratamento deve ser constantemente revisitada pelos agentes de tratamento, pois a conservação de informações só se justifica enquanto subsistirem obrigações legais, regulatórias ou litígios – como a necessidade de resguardar provas para eventual demanda judicial ou cumprimento de obrigações junto a órgãos de fiscalização, conforme o art. 16, I, da LGPD (Brasil, 2018). Nesses casos, a manutenção independe do consentimento do ex-empregado.

> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
> I - cumprimento de obrigação legal ou regulatória pelo controlador (Brasil, 2018).

Entre os documentos que podem ser exigidos pela legislação previdenciária e trabalhista, destacam-se os contratos de trabalho, folhas de pagamento, comprovantes de recolhimento de FGTS, INSS, laudos médicos e registros do histórico funcional.

Contudo, embora a LGPD permita a manutenção dos dados, impõe também a observância crítica aos princípios da minimização, finalidade, adequação e segurança,

de modo que apenas as informações estritamente necessárias para atender tais obrigações devem ser guardadas – e pelo tempo pertinente.

Esse ponto evidencia um equilíbrio delicado: armazenar menos pode expor a empresa a riscos jurídicos, mas reter em excesso pode representar violação de direitos do titular, resultando em responsabilização administrativa e administrativa.

Por esse motivo, requer-se atenção ao tempo de armazenamento, que varia de documento para documento e relaciona-se aos prazos legais de prescrição e decadência. Esse período pode ser delimitado à 2 anos ou, conforme regra geral de prazo quinquenal trabalhista, pode chegar a 5 anos (arts. 7, XXIX, da CF, e 11, da CLT). Em alguns casos, recomenda-se o armazenamento por até 30 (trinta) anos, haja vista o prazo prescricional disposto no art. 23, § 5º, da Lei 8036/90, na Súmula 362, TST.

Assim, para a adequada política de *compliance*, os profissionais responsáveis pela guarda e descarte de dados devem ser treinados para observar os prazos legais e acompanhar continuamente decisões administrativas e judiciais que possam impactar na contagem prescricional, evitando a retenção ou exclusão indevida de informações.

Portanto, a estrutura de *compliance* na fase pós-contratual requer: (i) controle rigoroso do acesso às informações por meio de protocolos específicos, garantindo rastreabilidade e confidencialidade; (ii) descarte seguro e definitivo das informações quando exaurido o prazo legal ou a finalidade específica; (iii) elaboração de política de privacidade claras sobre o armazenamento e a eliminação.

4.5 O futuro da proteção de dados do empregado: desafios e perspectivas do *compliance*

A promulgação da LGPD no Brasil atraiu atenção para o tema da proteção de dados e impactou diretamente as relações jurídicas, inclusive as de natureza laboral: ela inaugurou um novo campo de direitos e deveres para empregadores e empregados. Nesse ambiente historicamente marcado pelo conservadorismo institucional e resistência às transformações, o *compliance* surge como peça-chave para a efetiva concretização da LGPD e da proteção de dados nas relações de trabalho.

A efetividade da estrutura de *compliance* exige das empresas um compromisso que vai além da simples formalidade documental ou da adoção de soluções

padronizadas e automatizadas; exige uma abordagem sistêmica que integre pessoas, processos e tecnologia, com engajamento genuíno da liderança e participação ativa de todos os trabalhadores (Frazão; Oliva; Abílio, 2019, p. 372).

Para alcançar esse objetivo, é essencial a implementação de ferramentas de *compliance*, como políticas internas, banco de dados e treinamentos, desde que sejam tratadas como partes vivas e dinâmicas do cotidiano institucional. Mais que isso, a efetividade do *compliance* – operalizado pelas ferramentas – também requer uma abordagem integral e contínua, voltada para a proteção de dados em todas as fases do processo contratual trabalhista, desde a fase pré-contratual até a pós-contratual.

Contudo, é inegável que a implementação efetiva do *compliance* em proteção de dados ainda enfrenta desafios complexos. Na realidade, antes mesmo da implementação, persiste obstáculo cultural nas empresas: a visão tradicional do empregado apenas como força de trabalho e não como sujeito de direitos. Quando os empregados não são vistos como sujeitos de direito perante a LGPD, os seus dados também são subvalorizados, sendo submetidos a usos indiscriminados, excessivos e desnecessários, em inobservância à LGPD.

Ademais, durante o desenvolvimento das estruturas de *compliance,* uma dificuldade comum diz respeito à garantia de efetividade. Existe uma tendência empresarial de reduzir as políticas de conformidade a documentos simbólicos e protocolos burocráticos – voltados mais à mitigação de sanções legais do que à tutela de direitos – o que descaracteriza o objetivo principal dos programas de conformidade sob a perspectiva da LGPD.

Esse apego à formalidade não decorre apenas da falta de conhecimento técnico e da histórica desvalorização do empregado, mas também da resistência aos custos e investimentos exigidos por um programa robusto de *compliance*. Muitas organizações percebem investimentos em ferramentas de segurança, treinamentos e adequação de sistemas como despesas desnecessárias, especialmente quando não há um retorno econômico imediato ou pressões regulatórias.

Outrossim, a heterogeneidade do mercado também representa um desafio concreto: grandes empresas e setores fortemente regulados têm avançado na estruturação de programas robustos de conformidade, enquanto pequenas e médias

empresas, por limitações técnicas ou financeiras, muitas vezes não atribuem a devida importância ao tema.

Por fim, há ainda a questão do desenvolvimento tecnológico que, apesar de trazer inúmeros benefícios, também cria uma escalada de novos riscos, incrementando a complexidade necessária a programas de *compliance* e exigindo atualizações periódicas. Essa atenção permanente é frequentemente incompatível com os principais interesses da empresa, centrados na produtividade e maximização do lucro.

Entretanto, superar esse quadro de obstáculos não apenas é possível, como se mostra vital diante dos direitos fundamentais envolvidos no tratamento de dados. O caminho para uma efetiva proteção de dados nas relações laborais pressupõe, primeiramente, o reconhecimento do empregado como titular de dados e, portanto, sujeito de direitos. No mesmo sentido, empregadores devem entender-se como controladores, assumindo os deveres previstos na LGPD.

Sem esse reconhecimento prévio, dificilmente as empresas veem significado na implementação de programas de *compliance* para proteção de dados do empregado-titular. Assim, a princípio, é imprescindível que haja esse processo de observância à LGPD, integrando seus princípios e conceitos à seara trabalhista.

Com tal perspectiva internalizada, as empresas devem visar à implementação de programas de *compliance* efetivos – e não meramente simbólicos, limitados à blindagem jurídica. Trata-se de um processo de maturação institucional, ético e legal, que deve ser adequado à capacidade e à necessidade de cada empresa. Dessa forma, independentemente do porte e dos recursos da organização, torna-se possível concretizar a proteção de dados por meio de políticas de *compliance* proporcionais.

A construção de uma cultura organizacional forte, que transborde o aspecto formal e envolva efetivamente todos os atores – alta direção, gestores, RH, TI, empregados e sindicatos –, é a principal resposta a um cenário de constante transformação. Essa convergência de esforços estabelece uma base sólida de conhecimento distribuído e responsabilidade compartilhada, facilitando a identificação precoce de lacunas nos procedimentos e a adoção ágil de revisões e atualizações.

É justamente nessa construção coletiva, orientada pela ampla participação, transparência e conscientização contínua, que reside o potencial de êxito do

compliance como fator estruturante de uma nova era de proteção de dados nas relações de trabalho. A consolidação desse modelo exige a superação de obstáculos culturais, econômicos e regulatórios por meio do reconhecimento dual do empregado como titular de direitos e do empregador como controlador responsável e diligente.

Em suma, é evidente que futuro das relações laborais sob a égide da LGPD dependerá essencialmente da capacidade das organizações de transformar obrigações legais em valores institucionais genuínos, criando ambientes onde a privacidade do empregado não seja vista como limitação operacional, mas como elemento constitutivo de relações de trabalho dignas, sustentáveis e economicamente viáveis.

5 CONSIDERAÇÕES FINAIS

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) representou um marco regulatório para a tutela de direitos fundamentais no Brasil, sobretudo no que se refere à privacidade, liberdade e proteção de dados.

Nas relações empregatícias, a assimetria entre empregador e empregado agrava a vulnerabilidade informacional do trabalhador, tornando-o especialmente suscetível à utilização excessiva ou inadequada de seus dados pessoais. A LGPD, ao estabelecer diretrizes claras para o tratamento desses dados, se revela como instrumento normativo eficaz para a proteção do empregado como titular de dados.

Embora a LGPD não apresente dispositivos específicos sobre as relações laborais, a análise realizada ao longo deste estudo demonstrou, de forma inequívoca, sua aplicabilidade aos contratos de trabalho. Essa aplicação decorre de fundamentos constitucionais, como a garantia do direito à privacidade e à proteção de dados, assim como de fundamentos legais, previstos tanto na LGPD – quanto à sua abrangência – como na CLT, no que se refere à possibilidade de integração normativa.

Contudo, a aplicação da LGPD nas relações de trabalho não é automática; é necessário que haja compatibilidade com os princípios da CLT, especialmente o da proteção ao trabalhador. Tal requisito demanda uma análise pormenorizada dos conceitos e princípios previstos na LGPD quando inseridos nas relações de trabalho, como sujeitos, bases legais e responsabilidades.

Ao realizar esse diálogo, é possível identificar o empregado como titular de dados e o empregador como controlador e, por vezes, também operador de tratamento de dados. A análise das bases legais para o tratamento de dados no ambiente laboral evidencia a inadequação do consentimento, especialmente diante do desequilíbrio entre as partes, atraindo a incidência de outras hipóteses – como o cumprimento de obrigação legal, a execução de contrato e o legítimo interesse – sempre balizadas pelos princípios da LGPD, como a finalidade, necessidade, proporcionalidade e não-discriminação, e da CLT, como a proteção ao trabalhador.

Verifica-se, ainda, que a responsabilidade do empregador no tratamento de dados não se restringe à esfera administrativa e civil, estendendo-se à responsabilidade trabalhista. Nesse sentido, a violação à LGPD pode resultar desde obrigações impostas

pela ANPD e pela Justiça Comum, até a rescisão indireta do contrato de trabalho – inclusive em litígios trabalhistas, por determinação da Justiça do Trabalho – reforçando a importância de um sistema robusto de tutela de dados, com acurada gestão de riscos.

O presente estudo evidenciou que a proteção de dados do empregado é um processo complexo e permanente, que exige a articulação de toda a organização em prol de uma verdadeira cultura de privacidade. É nesse cenário que o *compliance* assume um papel estruturante, capaz de traduzir os princípios e diretrizes gerais previstos na LGPD em rotinas concretas e compatíveis com o ambiente de trabalho.

Não se trata apenas de um conjunto de boas práticas ou de cumprimento formal da legislação, mas de um sistema integrado e contínuo de gestão, operacionalizado por ferramentas práticas durante todo o processo contratual trabalhista, desde o recrutamento, passando pela vigência do contrato, até o período pós-contratual.

Nesse sentido, a adoção de ferramentas como bancos de dados, políticas de privacidade, termos de consentimento, programas de treinamentos, canais de denúncia e mecanismos de resposta a incidentes deve ser vista como uma etapa integrante das políticas de *compliance*. Esses instrumentos, se bem aplicados e revisados periodicamente, asseguram maior transparência no tratamento de dados e fortalecem a confiança entre empregado e empregador.

No entanto, ainda que a LGPD represente um avanço significativo, sua plena implementação nas relações laborais demanda amadurecimento doutrinário, jurisprudencial, normativo e, principalmente, institucional. A natureza geral e recente da nova lei, a ausência de dispositivos específicos na CLT e a complexidade das relações laborais impõem à doutrina o desafio de construir interpretações que integrem os princípios da proteção de dados aos fundamentos do direito do trabalho.

Nos próximos anos, é certo que a Justiça do Trabalho será chamada a enfrentar temas até então pouco explorados, como a validade de cláusulas contratuais envolvendo tratamento de dados de empregados, a reparação por danos informacionais, o direito à rescisão indireta por exposição indevida de dados, os limites da vigilância digital e os dilemas impostos por algoritmos em decisões automatizadas.

Paralelamente, é essencial o contínuo avanço normativo e fiscalizatório, especialmente por meio da atuação da ANPD, acompanhando as mudanças jurídicas e

as evoluções tecnológicas. A elaboração de novos manuais, guias e resolução proporciona orientações claras para as empresas, facilitando a adoção de boas práticas de *compliance* e, assim, a real proteção de dados no ambiente de trabalho.

A fiscalização, por sua vez, é essencial para garantir que as normas sejam efetivamente cumpridas, prevenindo abusos e promovendo a responsabilização em casos de irregularidades. Dessa forma, a atuação normativa e fiscalizatória da ANPD se complementa, fortalecendo a cultura de proteção de dados e assegurando um ambiente de trabalho mais seguro e alinhado com os direitos fundamentais dos trabalhadores.

Além da atuação da ANPD, destaca-se também o papel relevante do Ministério Público do Trabalho (MPT) na efetivação da proteção de dados nas relações trabalhistas. Como órgão tradicionalmente responsável pela fiscalização das condições de trabalho, o MPT pode atuar de forma integrada com a ANPD, incluindo a proteção de dados pessoais como pauta de suas inspeções e fiscalizações.

Quanto ao *compliance* propriamente dito, sua efetiva implementação enfrenta resistências de ordem cultural, econômica e técnica, sobretudo em ambientes tradicionalmente resistentes a mudanças, como o trabalhista. A superação desse desafio requer transformações profundas, que partem do reconhecimento do empregado como titular de dados.

A implementação de políticas de *compliance* deve seguir tanto os princípios da LGPD – como transparência, finalidade e necessidade – quanto os da CLT, voltados à proteção do trabalhador, além das garantias constitucionais, como o direito fundamental à privacidade e à proteção de dados. O caráter vivo e dinâmico do *compliance* permite acompanhar as mudanças contemporâneas, normativas e jurídicas, tornando-se imprescindível para a sustentabilidade e integridade das empresas.

Dessa forma, o *compliance* alcança seu papel estruturante, capaz de garantir a aplicação da LGPD nas relações de trabalho, de modo compatível e abrangente. Assim, com a efetiva integração da LGPD ao ambiente trabalhista, a proteção de dados do empregado-titular se torna um valor perene, fundamental e, sobretudo, tangível – que é vivenciado no cotidiano laboral.

6 REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia de boas práticas.** Brasília, DF: ANPD, 2020. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-guia-de-boas-praticas. Acesso em: 20 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia de requisitos e de obrigações quanto a segurança da informação e privacidade**. Brasília, DF: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/guia-seguranca-da-informacao-e-privacidade. Acesso em: 20 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia para definições dos agentes de tratamento de dados pessoais e do encarregado.** Brasília, DF: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/guia-agentes-de-tratamento-e-encarregado. Acesso em: 20 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia de elaboração de inventário de dados pessoais.** Brasília, DF: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/guia-inventario-dados-pessoais. Acesso em: 20 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia de elaboração de programa de governança em privacidade**. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/guia-programa-governanca. Acesso em: 20 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia de resposta a incidentes de segurança.** Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/guia-resposta-incidentes. Acesso em: 20 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 10, de 28 de fevereiro de 2023.** Aprova o Mapa de Temas Prioritários para o biênio 2024-202 e dispõe sobre a periodicidade do Ciclo de Monitoramento.. Diário Oficial da União: seção 1, Brasília, DF, 01 mar. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-10-de-5-de-dezembro-de-2023-530258528. Acesso em: 20 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 15, de 14 de março de 2024.** Aprova o Regulamento de Comunicação de Incidente de Segurança. Diário Oficial da União: seção 1, Brasília, DF, 15 mar. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 20 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 18, de 02 de maio de 2024.** Aprova o Regulamento sobre a atuação do encarregado pelo

tratamento de dados pessoais. Diário Oficial da União: seção 1, Brasília, DF, 03 maio 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074. Acesso em: 20 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 19, de 16 de maio de 2024**. Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. Diário Oficial da União: seção 1, Brasília, DF, 17 maio 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396. Acesso em: 20 jul. 2025.

ALVES, Amauri Cesar. **Direito, trabalho e vulnerabilidade.** *Revista da Faculdade de Direito UFPR*, Curitiba, v. 64, n. 2, p. 111-139, maio/ago. 2019. Disponível em: https://revistas.ufpr.br/direito/article/view/63907. Acesso em: 20 jun. 2025.

ALVES, Guilherme. A implementação da LGPD no Brasil e seus impactos para as estratégias de recursos humanos. In: PERREGIL, Fernanda; CALCINI, Ricardo (Orgs.). **LGPD e compliance trabalhista**. 2. ed. Leme-SP: Mizuno, 2024. p. 130-135.

BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. 1. ed. Rio de Janeiro: Forense, 2019.

BIONI, Bruno; MARTINS, Pedro, **Devido processo informacional: um salto teórico-dogmático necessário**. JOTA, 21 nov. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/devido-processo-informacional-um-salto-teorico-dogmatico-necessario. Acesso em: 10 jul. 2025.

BIONI, Bruno; DIAS, Daniel. **Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor.** *Civilistica.com*, Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/. Acesso em: 19 jun. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 03 jun. 2025.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Diário Oficial da União, Rio de Janeiro, 13 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 19 jul. 2025.

BRASIL. **Decreto-lei nº 5.452, de 1º de maio de 1943**. Aprova a Consolidação das Leis do Trabalho, Imprensa Nacional, Rio de Janeiro, 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 19 jul. 2025.

BRASIL. **Decreto nº 8.373, de 11 de dezembro de 2014**. Institui o Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas (eSocial) e

dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/decreto/d8373.htm. Acesso em: 22 jul. 2025.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. *Diário Oficial da União*, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 9 jul. 2025.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 19 jul. 2025.

BRASIL. **Lei nº 8.036, de 11 de maio de 1990**. Dispõe sobre o Fundo de Garantia do Tempo de Serviço, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8036consol.htm. Acesso em: 30 jul. 2025.

BRASIL. **Lei nº 8.212, de 24 de julho de 1991**. Dispõe sobre a organização da Seguridade Social, institui Plano de Custeio e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8212cons.htm. Acesso em: 22 jul. 2025.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 19 jul. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Marco Civil da Internet. *Diário Oficial da União*, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 9 jul. 2025.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília: Senado Federal, Secretaria de Editoração e Publicações, 2015.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República

BRASIL. Secretaria de Governo Digital. **Guia para elaboração de termo de uso e política de privacidade.** Brasília, DF: Governo Digital, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_termo_uso_politica_privacidade.pdf. Acesso em: 9 jul. 2025.

CARLOTO, Selma. **O compliance trabalhista e a efetividade dos direitos humanos dos trabalhadores.** São Paulo: LTR, 2021.

CORREIA, Henrique; BOLDRIN, Paulo Henrique Martinucci. **Lei Geral de Proteção de Dados (LGPD) e o direito do trabalho.** 2020. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2020/09/25/lei-geral-de-protecao-de-dados-lgpd-e-o-direito-trabalho/. Acesso em: 29 jun. 2025.

COUTINHO, Aldacy Rachid. Proteção de dados do trabalhador e a questão do necessário consentimento: uma abordagem a partir da Lei n. 13.709/2018. In: CARELLI, Rodrigo de Lacerda; CAVALCANTI, Tiago Muniz; FONSECA, Vanessa Patriota da (Org.). **Futuro do trabalho: os efeitos da revolução digital na sociedade**. Brasília: ESMPU, 2020.

CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (coord.). Tratado de **Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021. Cap. 18. p. 516-523

DELGADO, Mauricio Godinho. **Curso de Direito do Trabalho.** 18. ed. São Paulo: LTr, 2019.

FRANZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: FRANZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019. p. 372. Parte II, Cap. 10.

GARBACCIO, Grace Ladeira; BUJOSA VADELL, Lorenzo-Mateo; TORCHIA, Bruno. **Principais disposições da governança em privacidade à luz da Lei Geral de Proteção de Dados no Brasil.** Revista Justiça do Direito, v. 36, n. 1, p. 204-230, 2022. Disponível em: https://doi.org/10.5335/rjd.v36i1.13379. Acesso em: 6 jul. 2025.

GIMENEZ, Perla Martinez. Canal de denúncia - investigações internas corporativas. In: PERREGIL, Fernanda; CALCINI, Ricardo (Orgs.). **LGPD e compliance trabalhista**. 2. ed. Leme-SP: Mizuno, 2024. p. 473-479.

GROSSI, Bernardo Menicucci. **Lei Geral de Proteção de Dados: uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial.** Porto Alegre: Editora Fi, 2020.

INSTITUTO NACIONAL DE PADRÕES E TECNOLOGIA (EUA). **NIST SP 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations.** Gaithersburg: NIST, 2020. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Acesso em: 14 jul. 2025.

SILVA, Fabrício Lima. A autodeterminação informativa e os limites do poder fiscalizatório do empregador. In: MIZIARA, Raphael; PESSOA, André; MOLLICONE,

Bianca Medalha (Coords.). **Reflexos da LGPD no Direito e no Processo do Trabalho.** São Paulo: Thomson Reuters Brasil – Revista dos Tribunais, 2022. p. 470-484

JANZ, Roberta Philippsen et al. **Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática.** Coord. Fabiano Menke. Indaiatuba: Editora Foco, 2022. Disponível em:https://konektacommerce.nyc3.cdn.digitaloceanspaces.com/TEXT_SAMPLE_CONTENT/lei-geral-de-protecao-de-dados-subsidio-teorico-a-aplicacao-pratica-1a-ed-2022-173606-1.pdf#page=203. Acesso em: 10 jun. 2025.

KOZYREFF, Alan Martinez. O tratamento dos dados curriculares**.** In: PERREGIL, Fernanda; CALCINI, Ricardo (Orgs.). **LGPD e compliance trabalhista.** 2. ed. Leme-SP: Mizuno, 2024. p. 40-43.

LIMA, Adriano Carlos de. Capítulo 3 – Fase 3: Implementação e desenvolvimento da LGPD. In: MALDONADO, Viviane Nóbrega (coord.). **LGPD: Lei Geral de Proteção de Dados Pessoais: manual de implementação.** São Paulo: Thomson Reuters Brasil, 2019. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/como-eu-posso-preparar-minha-empresa-para-receber-a-lgpd-capitulo-3-fase-3-implementacao-e-desenvolvimento-da-lgpd-lgpd-lei-geral-de-protecao-de-dados-pessoais-ed-2022/1643176316. Acesso em: 30 jun. 2025.

MIZIARA, Raphael. Eficácia espacial da LGPD: doutrina dos efeitos e sua aplicação no tratamento transfronteiriço de dados nas relações de trabalho. In: BARZOTTO, Luciane Cardoso; COSTA, Ricardo Hofmeister de Almeida 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; Diadorim Editora, 2022. p. 168-180.

MIZIARA, Raphael; PESSOA, André; MOLLICONE, Bianca Medalha (Coords.). **Reflexos da LGPD no Direito e no Processo do Trabalho.** 2. ed. São Paulo: Thomson Reuters Brasil – Revista dos Tribunais, 2022.

NEVES, Marcela Cioccia. Canal de denúncias e anonimato: novas discussões sobre a possibilidade de revelação da identidade do denunciante em caso de falso relato. In: PERREGIL, Fernanda; CALCINI, Ricardo (Orgs.). **LGPD e compliance trabalhista**. 2. ed. Leme-SP: Mizuno, 2024. p. 465-470.

PALHARES, Felipe; FRANCOSKI, Denise de Souza Luiz**.** Capítulo 21. O uso de ferramentas open source no compliance ao princípio de segurança da LGPD. In: **Temas atuais de direito digital.** Ed. 2024. Jusbrasil, 2024. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/1-introducao-capitulo-21-o-uso-de-ferramentas-open-source-no-compliance-ao-principio-de-seguranca-da-lgpd-temas-atuais-de-direito-digital-ed-2024/2485212471. Acesso em: 15 jul. 2025.

PERREGIL, Fernanda; CALCINI, Ricardo (Org.). **LGPD e compliance trabalhista.** 2. ed. Leme, SP: Mizuno, 2024.

PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus Impactos nas Relações de Trabalho**.** In: BARZOTTO, Luciane Cardoso; COSTA, Ricardo

Hofmeister de Almeida Martins (org.). **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; Diadorim Editora, 2022. p. 35-56.

SAAVEDRA, Giovani Agostini. Compliance de dados. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 1027-1050.

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

SILVA, Fabrício Lima; PINHEIRO, Iuri; BOMFIM, Vólia. **Manual do compliance trabalhista: teoria e prática.** 3. ed. rev., ampl. e atual. Salvador: Editora Juspodivm, 2022. Disponível em: https://juspodivmdigital.com.br/cdn/arquivos/jus2160_previa-do-livro.pdf. Acesso em: 30 jun. 2025.

SILVA, Fabrício Lima. A autodeterminação informativa e os limites do poder fiscalizatório do empregador. In: MIZIARA, Raphael; PESSOA, André; MOLLICONE, Bianca Medalha (Coords.). **Reflexos da LGPD no Direito e no Processo do Trabalho.** São Paulo: Thomson Reuters Brasil – Revista dos Tribunais, 2022. p. 470-484

SOARES, Fábio Lopes (org.); STROBEL, Carolina; GOMES, Marcelo Borowski; PEDRO, Wagner Osti. **Compliance: fundamentos e reflexões para integridade nas empresas**. Rio de Janeiro: Lumen Juris, 2021.

SOUSA ROXO, Tatiana Bhering Serradas Bon de. Como implementar na prática um programa de proteção de dados. In: MIZIARA, Raphael; PESSOA, André; MOLLICONE, Bianca Medalha (Coord.). **Reflexos da LGPD no direito e no processo do trabalho.** São Paulo: Thomson Reuters Brasil, 2022. p. 423-450.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais.** Salvador: JusPodivm, 2019.

VAZQUEZ, Fabio José Buchedid. **Política de resposta a incidentes cibernéticos e estratégias de aderência à legislação brasileira**. Dataset Reports, v. 3, n. 1, p. 114-119, 2024. Disponível em: https://doi.org/10.58951/dataset.2024.020. Acesso em: 29 jun. 2025.

VIEIRA, Claudinei. Capítulo 1 – Fase 1: Preparação. In: MALDONADO, Viviane Nóbrega (coord.). ***LGPD: Lei Geral de Proteção de Dados Pessoais: manual de implementação*.** São Paulo: Thomson Reuters Brasil, 2019. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/introducao-capitulo-1-fase-1-preparacao-lgpd-lei-geral-de-protecao-de-dados-pessoais-ed-2022/1643176314. Acesso em: 29 jun. 2025.

ZOGHBI, Priscila Kuhl. Lei Geral de Proteção de Dados no Direito do Trabalho: Integração e Aplicabilidade. In: MIZIARA, Raphael; PESSOA, André; MOLLICONE, Bianca Medalha (Coords.). **Reflexos da LGPD no Direito e no Processo do Trabalho.** São Paulo: Thomson Reuters Brasil – Revista dos Tribunais, 2022. p. 87-97