**UNIVERSIDADE FEDERAL DO CEARÁ**
**FACULDADE DE DIREITO**
**PROGRAMA DE GRADUAÇÃO EM DIREITO**

**PEDRO HUGO IBIAPINA**

# A PROTEÇÃO DE DADOS DO TRABALHADOR E O EMPREGADOR: RESPONSABILIDADES E DESAFIOS DA FASE PÓS-CONTRATUAL

**FORTALEZA**
**2025**

PEDRO HUGO IBIAPINA

# A PROTEÇÃO DE DADOS DO TRABALHADOR E O EMPREGADOR: RESPONSABILIDADES E DESAFIOS DA FASE PÓS-CONTRATUAL

Monografia submetida à Coordenação do Curso de Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito. Área de concentração: Direito Civil.

Orientadora: Joyceane Bezerra de Menezes.

.

FORTALEZA

2025

.

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

---

I1p IBIAPINA, PEDRO HUGO.
A PROTEÇÃO DE DADOS DO TRABALHADOR E O EMPREGADOR: RESPONSABILIDADES E DESAFIOS DA FASE PÓS-CONTRATUAL / PEDRO HUGO IBIAPINA. – 2025.
48 f.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2025.
Orientação: Prof. Dr. Joyceane Bezerra de Menezes..

1. Responsabilidade Civil. 2. Proteção de Dados. 3. Dados Laborais. 4. Documentos Trabalhistas. I. Título.

CDD 340

PEDRO HUGO IBIAPINA

# A PROTEÇÃO DE DADOS DO TRABALHADOR E O EMPREGADOR: RESPONSABILIDADES E DESAFIOS DA FASE PÓS-CONTRATUAL

Monografia submetida à Coordenação do Curso de Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito. Área de concentração: Direito Civil.

Aprovada em: ___/___/_____.

BANCA EXAMINADORA

_____
Profª. Drª Joyceane Bezerra de Menezes (Orientadora)
Universidade Federal do Ceará (UFC)

_____
Profª Drª Márcia Correia Chagas
Universidade Federal do Ceará (UFC)

_____
Profª Drª Herika Janaynna Bezerra de Menezes Macambira Marques
Universidade de Fortaleza (UNIFOR)

## RESUMO

O presente trabalho tem como objetivo principal analisar a responsabilidade civil do empregador no contexto da proteção de dados do trabalhador, considerando os desafios relacionados à administração de dados após o término do contrato de trabalho. Para isso, inicialmente visa-se compreender os fundamentos da responsabilidade civil no âmbito da proteção de dados, explorando seus conceitos, definições e princípios. Em seguida, pretende-se analisar as implicações da LGPD no ambiente de trabalho, com foco nas responsabilidades do empregador, nos direitos dos titulares e nos desafios relacionados à gestão de dados laborais. A metodologia desta pesquisa é qualitativa, teórica, exploratória e descritiva, focando na análise de doutrinas jurídicas e legislações à proteção de dados no ambiente laboral. O estudo utiliza uma revisão bibliográfica abrangente para fundamentar teoricamente os conceitos de responsabilidade civil e proteção de dados, além de uma análise documental detalhada da LGPD e outros normativos relevantes, no que concerne às informações do trabalhador. Complementarmente, proporciona uma compreensão crítica das responsabilidades e desafios enfrentados por empregadores no gerenciamento de dados digitais dos trabalhadores. Constatou-se não apenas a importância de seguir rigorosamente a LGPD, mas também a urgência em torno do fato de que as organizações precisam estar em constante evolução e adaptação em resposta aos riscos trazidos pela tecnologia. A responsabilidade civil não deve, pois, ser entendida apenas como uma imposição normativa, mas também como orientação principiológica frente a essa evolução tecnológica.



**Palavras-chave:** Responsabilidade Civil; Proteção de Dados; Dados Laborais; Documentos Trabalhistas.

## ABSTRACT

The main goal of this study is to analyze the civil liabilities of employers in the context of worker data protection, considering the challenges related to data management and digital inheritance after the termination of the employment contract. To achieve this, the study initially aims to understand the foundations of civil liability in the realm of data protection, exploring its concepts, definitions, principles, as well as the history and evolution of the right to privacy. Next, it seeks to analyze the implications of the LGPD (General Data Protection Law) in the workplace, focusing on employer responsibilities, data subjects' rights, and the challenges associated with the management of labor data. The methodology of this research is qualitative, theoretical, exploratory, and descriptive, focusing on the analysis of legal doctrines and legislation on data protection in the labor environment. The study uses a comprehensive literature review to theoretically substantiate the concepts of civil liability and data protection, as well as a detailed documentary analysis of the LGPD and other relevant regulations that regard worker data. Additionally, it provides a critical understanding of the responsibilities and challenges faced by employers in managing workers' digital data. It was found, not only the importance of rigorously complying with the LGPD but also urgency around the fact that organizations need to be constantly evolving and adapting in response to the risks brought by technology. Civil liability, as it stands, should not be understood as a normative imposition, but also as a principle guidance before technological evolution.



**Keywords:** Civil Liability; Data Protection; Worker Data; Employment Documentation.

**SUMÁRIO**

# 1 INTRODUÇÃO

A crescente digitalização das relações jurídicas e sociais tem emergido à ágora popular, consoante dita os aspectos formadores e limitadores de uma realidade moderna. Não é díspar o efeito desse fenômeno nas relações de trabalho, que veem muitas de suas facetas engolfadas pela inovação. Os dados do trabalhador, especialmente, tornaram-se foco de análise especial, tendo em vista sua proteção e tratamento repentinamente ímpares, frente à implementação da Lei Geral de Proteção de Dados Pessoais - LGPD (nº 13.709/2018) no Brasil (Brasil, 2018).

A natureza singular do tratamento desses dados se desdobra em múltiplos contextos práticos e jurídicos, como a inovação documental e a proteção de dados após o término do contrato de trabalho. Os dilemas incluem o acesso a esses dados e documentações, agora digitalizados, dentro do âmbito da temporalidade, com destaque para o momento posterior ao término do contrato de trabalho.

Nesse contexto, faz-se imprescindível indagar: Em que medida é o empregador responsável pelo tratamento de dados e documentos fornecidos pelo empregado em decorrência da relação de emprego, e como há de ser classificada e delimitada essa responsabilidade?

Visando responder esse questionamento, tem-se como objetivo principal analisar a responsabilidade civil do empregador no contexto da proteção de dados do trabalhador após o término do contrato de trabalho. Deste objetivo principal decorrem os seguintes objetivos específicos: a) examinar os fundamentos da responsabilidade civil no âmbito da proteção de dados, explorando seus conceitos, definições e princípios; b) verificar as implicações da LGPD no ambiente de trabalho; c) estudar a responsabilidade do empregador nos direitos dos titulares e na gestão de dados laborais.

Busca-se analisar o tratamento e gestão do empregador perante os dados e documentos decorrentes do vínculo empregatício, considerando o instituto da responsabilidade civil e destacando a proteção de dados na fase pós-contratual.

A pesquisa tem uma abordagem qualitativa, vez que não busca obter informações quantificáveis. Se dá ainda, primordialmente, por meio de procedimento de análise bibliográfica e documental, sendo feito o uso de artigos científicos, revistas acadêmicas, dissertações e teses, além do estudo da Lei Geral de Proteção de Dados (LGPD) e demais projetos de lei que envolvem o direito à privacidade e a proteção de dados.

O presente estudo é tanto exploratório quanto descritivo, e realiza levantamento inicial acerca da temática, com pequena revisão de literatura, baseada em artigos de revistas,

livros e documentos, sem se eximir de tentar exaurir a bibliografia que envolve a matéria estudada. Por fim, trata-se de viés teórico, no que diz respeito à utilização dos resultados obtidos.

Tais ferramentas visam produzir análise holística e coerente do conhecimento acumulado acerca da responsabilidade do empregador perante os dados fornecidos pelo empregado no curso da relação de emprego. O trabalho, para atender a finalidade a que se propõe, foi dividido, além da introdução e conclusão, em três capítulos de desenvolvimento.

No primeiro capítulo, pretende-se analisar os conceitos fundamentais. Inicia-se com a análise da origem da responsabilidade civil na legislação pátria e o seu conceito, bem como situando o homem no âmbito virtual de forma a analisar a evolução e conceito do tratamento dos dados. O referido capítulo finaliza demonstrando a importância da responsabilização civil no cenário de proteção dos dados atualmente.

O segundo capítulo, por sua vez, analisa a implementação da tecnologia nas relações de emprego; as implicações da LGPD no ambiente de trabalho, com foco nas responsabilidades do empregador, nos direitos dos titulares e nos desafios relacionados à gestão de dados laborais. O último capítulo de desenvolvimento cuida de analisar a aplicação prática dos conceitos de responsabilidade civil e proteção de dados no trabalho, principalmente na fase pós-contratual da relação de emprego.

Por fim, as considerações finais indicam a resposta ao questionamento inicial, bem como as perspectivas futuras e possíveis cenários esperados em relação ao avanço da tecnologia e à proteção dos dados dos empregados por seus empregadores, além de sugestões de iniciativas para mitigar as repercussões negativas decorrentes de tais fatores, com a consequente resposta à problemática central estabelecida anteriormente, tanto no objetivo principal, quanto nos objetivos específicos decorrentes.

# 2 RESPONSABILIDADE CIVIL E PROTEÇÃO DE DADOS

A responsabilidade civil surge como instituto que serve à restauração de um direito, violado por outrem. Para realizar uma análise desse conceito em caráter holístico, são utilizadas ferramentas principiológicas, históricas, pragmáticas e conceituais, contextualizando-as no âmbito do cenário jurídico pátrio.

Paralelamente, é notável a importância que os dados têm adquirido, não apenas no aspecto pessoal, como no aspecto profissional. O decorrente tratamento e proteção emergem como questão central no ordenamento jurídico nacional, como por exemplo o status constitucional, bem como legislações especializadas, como a Lei Geral de Proteção de Dados.

Diante da tutela jurídica do acervo de dados individual e coletivo, as eventuais violações dessas informações impõe a necessidade de responsabilizar civilmente o agente responsável por tal ofensa, sendo o direito civil a via mais apropriada para a recomposição dos danos materiais e extramateriais.

## 2.1 A responsabilidade civil e sua evolução no direito brasileiro

A responsabilidade civil no Brasil evoluiu do sistema de culpa do Código Civil de 1916 para um modelo que também inclui a responsabilidade objetiva no Código Civil de 2002. Inicialmente, era preciso provar a culpa do causador do dano para obter indenização. Com o tempo, a jurisprudência e a legislação introduziram a responsabilidade objetiva em casos específicos, dispensando a prova da culpa. O Código Civil de 2002 consolidou essa tendência, mantendo a responsabilidade subjetiva como regra, mas ampliando a aplicação da responsabilidade objetiva, especialmente em situações de risco e nas relações de consumo.

O civilista Cavalieri Filho (2003), assevera que, ao passo em que o sistema subjetivista começou a falhar, se mostrou exíguo, por motivo de avanços tecnológicos, da evolução da ciência, do aumento populacional, foi indispensável assumir outras conceituações de responsabilidade civil alheias à culpa, o que ocorreu fora dos códigos civis, em legislação especial.

Em sequência, faz-se necessário lançar o pilar conceitual da responsabilização, vital para o desenvolvimento e o entendimento das relações a serem esposadas, principalmente no que se refere a aplicações práticas. Isso porque, a responsabilidade civil vai ganhar ainda mais destaque no contexto de desenvolvimento tecnológico e digital exponencial, como fator de contrapeso e orientação. Nesse sentido, “Sem desprezar as demais esferas de atuação do poder

público, dar-se-á maior enfoque à responsabilidade civil em razão de seu protagonismo na resposta a este estado de coisas trazido à baila pela sociedade tecnológica" (Yaegashi; Otero, 2022).

Para Caldas, Soares e Martins (2022), a responsabilidade civil aplicada é nada além do que uma tentativa do legislador de estimular uma conduta no contexto social, coibindo e refreando possíveis violações ao normatizado, que é garantidor de direitos. Segundo Fernandes, Pereira e Pedrosa (2024), é possível verificar que o próprio ordenamento pátrio apresenta o conjunto de ações do indivíduo como primeiro componente da responsabilização civil. Essa coleção abrange tanto a conduta ativa quanto a passiva, que por meio de omissão, podem vir a modificar o contexto em que se insere.

Entende-se, pois, que a responsabilização civil possui natureza de imposição individual, independente de seu receptáculo ser entidade de caracterização física ou jurídica. Tal imposição consiste no dever ou obrigação da reparação de danos, sejam eles de ordem material ou não, que tenham sido causados a outrem, decorrente de uma observância a instrumento contratual ou extracontratual, com o fito de manter ou restaurar a paz do contexto social (Fernandes; Pereira; Pedrosa, 2024).

## 2.2 Sociedade da informação e direitos fundamentais na era digital

Santos, Leitão e Wolkart (2022), afirmam que há uma crescente transposição da experiência humana para a subjetividade e o abstracionismo do âmbito virtual, realidade que se apresenta de maneira inesperada; ao passo que rejeitam o reducionismo dessa mesma experiência ao digital, não consideram possível evitar o papel da troca constante de base informacional na composição da autopercepção individual e coletiva.

Há, portanto, um tecido social que está ligado diretamente a um sistema econômico em que o fluxo informacional é o núcleo, e que a participação do indivíduo componente desse sistema se reproduz, principalmente, na rapidez produtiva e na generalizada capacidade de capilarização informacional (D'Oliveira; Cunha, 2024).

Partindo de uma ideia de sociedade em redes, é factível aduzir que as relações sociais, econômicas e políticas se tornaram cada vez mais complexas com o passar dos anos, o que se deve à inovação tecnológica em caráter exponencial. Contemporaneamente, conceitos primordiais de segurança cibernética se imiscuem no núcleo do debate governamental, pelo menos no que se refere à gestão e resguardo de informações na realidade global atual. A rede mundial de computadores torna, pois, a preocupação com a segurança cibernética e de dados

ainda mais intensa, ao passo em que governos e demais entidades almejam se instruir perante as modificações ensejadas pelo crescimento exponencial da internet (Paula, 2024).

Paralelamente, insta examinar que os Direitos Fundamentais são um conjunto de direitos inerentes à dignidade humana, reconhecidos e protegidos pelas constituições e tratados internacionais. Eles visam assegurar condições mínimas para o desenvolvimento da personalidade, a liberdade, a igualdade e a participação na vida social e política.

O direito à privacidade, por exemplo, é um direito fundamental autônomo que protege a intimidade, a vida privada, a honra e a imagem das pessoas, garantindo a cada indivíduo o direito de controlar o acesso a informações sobre sua vida pessoal e de decidir quais informações deseja compartilhar com os outros. A internet, com sua dinâmica de coleta e compartilhamento de dados, representa um desafio para a proteção da privacidade, uma vez que aumenta a facilidade com que informações pessoais podem ser coletadas, armazenadas e compartilhadas online aumenta o risco de violações da intimidade.

Como lembra Teresa Ancona Lopez (2010, p. 1223) “Nossos dados são públicos. Hoje, o famoso "Grande Irmão" toma conta de nossas vidas e nos leva aprender a lidar com o fundamental direito de privacidade nessa também sociedade de vigilância”.

Santos, Leitão e Wolkart (2022) destacam o rastreamento de perfis digitais, onde fragmentos da vida pessoal são armazenados em diversos sites. Padrões de consumo e preferências são facilmente identificáveis, havendo a preocupação de que entidades possam documentar aspectos íntimos da experiência humana, expondo indivíduos a vulnerabilidades.

Nesse contexto, emerge o sujeito digital, parte de uma nova realidade e tecido social, inserido em uma complexa rede de relações e vulnerável por sua natureza digital. “O cenário cibernético, essencialmente instável, apresenta uma preocupação a ser enfrentada: a banalização no fornecimento de dados pessoais e a utilização indiscriminada desses dados por empresas” (De Téffe; Bodin, 2017, p. 24). Contudo, essa vulnerabilidade coexiste com a titularidade de direitos.

Segundo Sarlet (2020), a conexão entre a garantia à autodeterminação informativa e princípios basilares de dignidade da pessoa humana, se mostra, de certo modo, dobrada, uma vez que se apresenta tanto pela sua relação com a conceituação de autonomia, quanto com a gama de direitos de personalidade. Em outras palavras, a proteção de dados pessoais não se limita a salvaguardar informações. Ela se estende à garantia de que cada indivíduo possa desenvolver sua personalidade de maneira plena e autônoma. Por essa razão, a preservação da privacidade é fundamental.

A distinção da natureza materialmente basilar do direito à proteção de dados pessoais logo resulta em decorrências práticas de caráter argumentativo (Acyoly; Silva; Monteiro Neto, 2024). A título de exemplificação, vale ressaltar que, ainda que se adote o argumento majoritário de que somente pessoas naturais possuem a garantia à salvaguarda dos dados pessoais, isso não se traduz em negação do fato de que demais entidades podem ser titulares de direitos fundamentais. De todo modo, é plausível indagar se a classificação de pessoas jurídicas enquanto titulares de direito à proteção de dados pessoais resulta em benefício da qualidade protetiva (Sarlet, 2020).

O agente governamental, por exemplo, também pode se transformar em vetor de desestabilização proposital da segurança cibernética de terceiros, com a composição de grupos que irão ter dúplice função: proteger o ente de violações cibernéticas ou utilizar-se de poder ofensivo para o objetivo supramencionado (Paula, 2024).

Pinto e Mota (2022), ensinam que a vulnerabilidade das instituições vitais do Estado Nacional a ataques cibernéticos revela uma fragilidade ou flexibilização da soberania estatal. Diante do cenário atual de conflitos humanos, impulsionados pelo desenvolvimento tecnológico e pela guerra cibernética, a matriz constitucional da soberania estatal exige reconstrução ou, no mínimo, uma nova interpretação.

Dessa forma, cumpre destacar a pureza conceitual do direito do sujeito à proteção de dados enquanto direito fundamental, embora nem todos os possíveis titulares de direitos fundamentais alcançarão a mesma utilidade no âmbito dessa salvaguarda. Em verdade, é majoritária a caracterização da pessoa jurídica enquanto parte do outro polo da relação, restando às leis o dever de regular essa atuação.

É propício afirmar, pois, que a confecção de uma base de dados, por entidades privadas ou estatais, possibilita a melhor execução do objeto de atividade. Contudo, deve se caracterizar por uma operação delimitada por princípios éticos e jurídicos. Assim, é dever das leis regular o tratamento desses dados, sob a égide de proteger garantias fundamentais de liberdade e privacidade, além do livre desenvolvimento do indivíduo (Maciel, 2023).

## 2.3 Evolução legislativa da proteção de dados no Brasil

A proteção de dados no Brasil evoluiu gradualmente, começando com a Constituição Federal de 1988, que estabeleceu direitos fundamentais como a privacidade e o habeas data. O Código de Defesa do Consumidor também contribuiu para a proteção de dados, especialmente em relação aos consumidores; ao passo em que, com a crescente digitalização, o

Marco Civil da Internet trouxe princípios para a proteção de dados online.

Foi, entretanto, a Lei Geral de Proteção de Dados (LGPD) que representou um marco, estabelecendo um arcabouço legal abrangente para o tratamento de dados pessoais, definindo o conceito de tratamento de dados e criando a Autoridade Nacional de Proteção de Dados (ANPD). A LGPD alinhou o Brasil aos padrões internacionais, promovendo uma cultura de privacidade e segurança de dados.

Adicionaria Sarlet (2020) que, há no ordenamento pátrio a designação da conceituação de dados pessoais para o legislador infraconstitucional, mesmo que tacitamente. Urge restar destacado, tendo em mente que a definição em tela é receptáculo direto da salvaguarda estatal, que não se pode ir de encontro ao arcabouço constitucional e nem desviar de seu aspecto teleológico originário.

Torna-se relevante constatar que, ocorrendo em sede infraconstitucional, a proteção de dados deve emergir derivada de direitos fundamentais e princípios jurídicos. Assim, está ainda vinculada à hierarquia normativa conhecida, estando proibida de contrariar a lei constitucional ou mesmo o fim teleológico de seus dispositivos. Nesse contexto de resposta regulatória, emerge a LGPD.

É plausível constatar que a LGPD configura reação do ordenamento pátrio ao desenvolvimento do aspecto digital que se fez presente nos anos passados, possuindo como enfoque a proteção basilar das esferas do livre e do privado, prezando ainda pela evolução do teor personalíssimo do indivíduo (Santos; Leitão; Wolkart, 2022).

D’Oliveira e Cunha (2024) lecionam que a LGPD pode ser classificada como mais uma legislação específica ao armazenamento de informações, trazendo efeitos pragmáticos, regramentos e responsabilizações acerca da política de informação aplicada. Diz-se ainda que existe na norma um movimento, ainda que mínimo, de gerenciamento social do conteúdo informacional elaborado no que diz respeito ao indivíduo, por meio de uma realocação de recursos informacionais: trata-se da fixação da autodeterminação informativa como um dos fundamentos da norma.

Aduz ainda Tasso (2020) que a Lei Geral de Proteção de Dados fixa ainda o titular de direitos como alvo singular dos dispositivos protetivos, além de proprietário inequívoco de seus dados pessoais. Isto é, no que se refere às relações que contenham o contato de outros para com esses dados. Nesse contexto, faz-se mister trazer a conceituação da própria LGPD para o tratamento de dados, em seu art. 5º, inciso X, que infere que é tratamento que toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento,

arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018).

Analisa-se, logo, a LGPD sob o enfoque indubitável do indivíduo, enquanto titular de direitos de privacidade e liberdade. Importa ressaltar, porém, alguns pontos que enriquecem os contornos do tratamento de dados na lei.

Primeiramente, há na LGPD um balanceamento intencional da dualidade que compõe a proteção de dados pessoais dentro de um âmbito mercadológico. Essa dualidade se traduz na privacidade dos titulares e na gestão da movimentação de dados, que ensejam o advento de regras acerca da conduta dos agentes de tratamento de dados, especialmente no que se refere à maneira como esses devem executar atividades envolvendo dados pessoais ao realizarem suas operações (D'Oliveira; Cunha, 2024).

Sob esse prisma, pode-se inferir que, apesar do destaque claro no proprietário de dados pessoais, a relação de tratamento de dados na LGPD não se traduz de forma alguma em rivalização entre o agente responsável e o titular de direitos. Pelo contrário, para atingir o objetivo da norma é necessário um equilíbrio flagrante entre a utilização dos dados e a sua preservação.

Maciel (2023) ensina que a Lei Geral de Proteção de Dados é de grande relevância para pessoas de direito público ou privado, uma vez que abrange o tratamento de dados pessoais de seus respectivos titulares por terceiros, independente da natureza jurídica do agente tratador. Destaca ainda que a norma conceitua dados pessoais como qualquer dado que tenha relação com pessoa natural passível de identificação. No entanto, esposa o advento de ditames mais restritos para a classificação de dados sensíveis, já que estes são informações componentes de um rol mais delicado, passível de ser usado em diversas situações de discriminação.

Sob esta ótica, a LGPD dispõe de maneira extensiva acerca de obrigações de tratamento aos agentes de tratamento de dados, com o fito de coibir interações indesejadas com os dados pessoais, acidentes de caráter modificativo ou qualquer violação do tipo. Insta asseverar o tratamento especial atribuído a dados sensíveis, o que explicita o caráter analítico da norma no que se refere ao tratamento de dados. As restrições servem ao propósito de desestimular mais ainda a conduta transgressora nesse caso específico (Tasso, 2020).

A LGPD traz o pressuposto de boa-fé para qualquer que seja o tratamento de dados, dispondo, porém, do controle específico que visa a manutenção do fluxo informacional seguro, dentro do período de acesso ao dado, pelo agente de tratamento. Esse controle, que inclui dados sensíveis, pode ser utilizado para verificar, de maneira fiscalizável, se os deveres impostos são seguidos, via instalação de uma variedade de instrumentos de gestão para a melhor segurança

dessas informações (Maciel, 2023).

> Ainda sobre dados sensíveis, há de se lembrar que as informações desta ‘persona’ cibernética merecem proteção, contudo, faz-se necessário a atribuição desse selo de resguardo intensificado, uma vez que a manipulação desses dados pode ensejar condutas eivadas de caráter discriminatório, o que vai de encontro aos pilares do sistema jurídico (Matos; De Menezes; Colaço, 2017, p. 14).

Mostram-se, pois, a responsabilidade civil e a proteção de dados conectadas pelo advento da própria LGPD, que carrega as ferramentas necessárias para tornar conduta a transgressora da proteção de dados em explícito descumprimento de instrumento normativo. Ainda assim, esposa-se imprescindível estudar o que traz em específico a lei sobre a responsabilização civil.

## 2.4 A responsabilidade civil na LGPD: natureza, princípios e controvérsias

Acyoly, Silva e Monteiro Neto (2024) entendem que a proteção de dados pessoais é baseada na autodeterminação informativa, apesar de a ela não se restringir. A bem da verdade, esposa uma construção contínua e substancial, demonstrativa de mudanças de paradigmas e visões legislativas do assunto, por um rol de instrumentos.

Os dados são, atualmente, o horizonte mais longínquo do direito privado. Entretanto, apesar de representarem temática muito importante, a legislação já sedimentada e os tribunais vinham encontrando empecilhos em acompanhar tão exponencialmente a inovação tecnológica e o tratamento de dados pessoais, o que exigiu a ação da figura do legislador (Novakoski; Naspolini, 2020).

Os anos de desenvolvimento da LGPD foram preenchidos por complexas argumentações na ágora popular e ocasionais brigas por poder, deixando indicações de interpretação de grande valor, além de hipóteses de análise fundamentadas nos preparativos da lei (Bioni; Dias, 2024).

É possível asseverar que os regimes de informação, no contexto legislativo, são reavaliados ou permanecem. A LGPD, enquanto instrumento jurídico-normativo, trouxe o advento de entes com funções mais delimitadas, transicionando o conteúdo implícito do regime anterior em explícito (D’Oliveira; Cunha, 2024).

Vale lembrar que a garantia da salvaguarda de dados pessoais, ainda que tenha sido positivada em caráter mais substancial na LGPD, é também reflexo de tendências jurídicas e econômicas ao redor do mundo, especialmente no que se refere ao fluxo informacional (Acyoly; Silva; Monteiro Neto, 2024).

A LGPD canaliza e evidencia a proteção de dados pessoais, seguindo as inclinações globais de atrelamento a direitos fundamentais e as necessidades da realidade prática do tratamento de dados. Nessa seara, insta trazer à tona o conceito de responsabilidade civil, já apresentado anteriormente, dentro do instrumento em questão.

Faz-se necessário destacar que, em termos estruturais, a LGPD vem em seu terço final tratar acerca da responsabilização civil dos agentes de tratamento de dados, tendo já estabelecido seus deveres e as bases principiológicas que respaldam o normatizado (Tasso, 2020). Se o agente de tratamento de dados é responsável por um "vazamento", uma danificação, ou mesmo a perda de dados pelos quais estava encarregado, ele será responsável civilmente, podendo ter a si atribuído o ônus reparatório.

Ocorre que, ainda que seja instrumento legislativo analítico, a LGPD não se propõe a esgotar a questão da classificação do regime de responsabilidade civil que pode ser atribuída aos agentes controladores e operadores de dados, o que ensejou dissonância doutrinária acerca do âmago do dever de reparar (Fernandes; Pereira; Pedrosa, 2024).

A LGPD comporta múltiplas interpretações e complementos acerca de sua abordagem aos detalhes da responsabilidade civil em seu âmbito, o que é possível observar em diferentes visões da doutrina nacional.

A responsabilização civil advém da operação de gestão ou tratamento de dados que infrinja o ordenamento pátrio relativo à proteção de dados. Assim, é coerente asseverar que o próprio legislador reforça a ideia de proteção de dados enquanto microssistema, com dispositivos dispersos em instrumentos normativos variados, sendo a LGPD a coluna vertebral dessa estrutura (Capanema, 2020).

Segundo Caldas, Soares e Martins (2022), a responsabilidade civil na LGPD abarca as violações de direitos do titular, sendo estes previstos na própria LGPD ou em demais dispositivos semelhantes. Consequentemente, também entram nesse escopo violações de direitos previstos em normas técnicas, do âmbito de segurança informacional ou, mais particularmente, de proteção de dados. Desse modo, é possível concluir que, no núcleo das dissonâncias hermenêuticas relacionadas ao disposto na LGPD no que se refere à responsabilização civil, encontra-se a interpretação da própria base aplicada pelo legislador na conceituação de responsabilidade civil.

Capanema (2020) ainda destaca que a responsabilização civil está presente na Seção III do Capítulo VI da LGPD. Traz à tona ainda que os dispositivos que compõem essa seara não se aplicam em qualquer ocasião que envolva responsabilidade civil no tratamento de dados, uma vez que a característica da relação jurídica pode ditar o uso de legislação mais

especializada.

Resta evidente, portanto, que há aqui uma relação multifacetada entre a LGPD e os demais dispositivos que tratam acerca da responsabilização civil. Isso porque a especificidade das normas entra em conflito, uma vez que enquanto a LGPD é o principal pilar da proteção de dados, outras relações que podem fazer parte dessa titularidade de direitos também abarcam seu próprio regime de responsabilização. Bons exemplos disso são as relações de consumo.

Santos, Silva e Padrão (2021) reconhecem que se torna possível afirmar que a discussão acerca do regime de responsabilidade é limitada a situações em que não se trata de Direito do Consumidor, uma vez que este está sujeito ao regime destacado no seu código. Sustentam os autores, ainda, que o regime da LGPD possui natureza complementar e alternativa, aplicando-se apenas em relações associativas ou empregatícias, a título de exemplificação. Essa falta de assertividade do instrumento legislativo no que se refere ao regime de responsabilidade civil para casos de relações que não são de consumo traz consigo vasta altercação doutrinária, equilibrada em relevância argumentativa, com enfoque na caracterização jurídica dessa responsabilidade atribuída aos agentes de tratamento de dados.

A LGPD ainda delimita a responsabilização civil ao controlador ou ao operador dos dados, ambos agentes de tratamento. Ocorre que, apesar da relação de alternatividade fortemente sugerida pela conjunção “ou”, é possível que sejam aplicadas as regras de responsabilidade solidária da legislação específica das relações de consumo, por exemplo. Não obstante, caso o operador viole a legislação protetiva ou contrarie as ordens do controlador, também responderá solidariamente, em relacionamento de equiparação. Por fim, é natural inferir que haverá responsabilização solidária também de controladores que executarem atividades rigorosamente inclusas no tratamento de dados, isto é, caso o seu poder decisório seja responsável direto pelo descumprimento da legislação de proteção de dados (Capanema, 2020).

A relação empregatícia, então, estará sob o regime de responsabilidade civil da LGPD no que se refere ao tratamento de dados pessoais, mesmo com as discordâncias doutrinárias mencionadas. Nesse caso, é mister analisar como se dará a classificação dessa responsabilidade.

Existe fundamentação suficiente de modo a classificar a responsabilidade civil como objetiva no que se refere ao agente de tratamento de dados. Isto é, pois ainda que a ideia de culpa possa ser investigada de da melhor maneira, ainda é passível de estar eivada de dano à plena reparação de quem teve os dados vazados. (Fernandes; Pereira; Pedrosa, 2024). Afirma Capanema (2020) que é justamente na modalidade objetiva da responsabilização do agente que

se observa a vulnerabilidade do proprietário de dados pessoais na relação, ao passo em que não existe debate acerca da culpa no dano. Isso em adição à própria inversão do ônus da prova.

A responsabilidade civil aplicada na proteção de dados é a objetiva, prescindindo de análise acerca da existência ou não de culpa, de modo a atingir os fins principiológicos do normatizado, que é a garantia de direitos de autodeterminação informativa ao titular (Capanema, 2020; Fernandes; Pereira; pedrosa, 2024).

Ressalte-se que, apesar de majoritária, essa visão não é unânime, uma vez que as versões anteriores da LGPD deixavam cristalino que sua noção legislativa rejeitou explicitamente um regime de responsabilidade civil na modalidade objetiva. Tem-se diversos componentes da norma que, tacitamente ou não, se alinham para que exista uma valoração circundante à culpa do agente tratador de dados. Isso não está apenas esposado no arrolamento de excludentes de responsabilização, mas, também, na própria base de princípios do texto, além de em outros sítios relevantes da LGPD. Trata-se de uma conclusão racional inequívoca e que sustenta a coerência do regime de responsabilidade (Bioni; Dias, 2024).

Revelam ainda Novakoski e Naspolini (2020), que um impedimento geralmente evidenciado pelos partidários da noção da responsabilização civil na modalidade subjetiva na LGPD se baseia na ideia de que a implementação da teoria do risco da atividade desestimularia a competitividade mercadológica e a própria inovação tecnológica inerente ao direito abordado. Acrescentam que: Equilibrando essas prerrogativas, se assemelha a uma contradição a norma tratar sobre ferramentas de prevenção no âmbito da responsabilidade, que tendem a obstar a ocorrência do dano, e, ao mesmo tempo, condicionar a compensação pelos danos causados à proteção de dados pessoais, que se explicitam um direito fundamental, à alçada da responsabilidade civil subjetiva, com o advento de todos os desafios que vem com esse regime, e que possibilitou a gradual transposição da responsabilidade civil originária em objetiva por meio de instrumentos como a presunção de culpa e as modalidades de risco.

Bioni e Dias (2020) entendem que a redação da lei foi gradativamente montada para delinear as hipóteses excludentes de responsabilidade. Na verdade, as interações mais antigas eram, mesmo que não completamente escassas, consideravelmente exíguas em abordar as delimitações conceituais de uma conduta ilícita, assim como no que se refere ao seu nexo causal para responsabilizar os agentes de tratamento. É somente no último estágio do debate entre legisladores que se atribui fundamentos basilares do regime jurídico da responsabilidade civil da LGPD.

Pode-se afirmar, portanto, que a LGPD é um marco na proteção de dados, mas não esgota a questão da responsabilidade civil, uma vez que há divergências legais identificadas

pela doutrina sobre a natureza da responsabilidade (objetiva ou subjetiva). Existe ainda um conflito de normas com outras legislações, como o Código de Defesa do Consumidor e uma disputa acerca da LGPD prever a responsabilidade solidária dos agentes em determinadas situações. A responsabilização civil na proteção de dados é um tema complexo que exige debate e aprimoramento contínuos.

# 3 A PROTEÇÃO DE DADOS NO ÂMBITO DAS RELAÇÕES DE TRABALHO

É imperioso fazer uma análise crítica da proteção de dados pessoais no contexto do ambiente de trabalho, a partir de noções mais básicas de influência do normatizado no âmbito corporativo, ao passo que, no decorrer dos últimos anos, é possível verificar a advento de inovações relacionadas aos componentes basilares da relação de emprego.

No que concerne ao tratamento de dados pelo empregador e a modernização da documentação pertinente à dinâmica laboral, é especialmente importante a atenção no processamento dos dados do empregado que permanecem em domínio do agente de tratamento de dados após o término do contrato de trabalho.

## 3.1 Transformações tecnológicas nas relações de emprego

A integração da tecnologia no tecido das relações de emprego tem provocado uma metamorfose profunda no panorama laboral, tecendo uma tapeçaria complexa de benefícios e desafios que moldam o futuro do trabalho.

Por um lado, a tecnologia surge como um catalisador de progresso, impulsionando a produtividade a patamares inéditos. A automação de tarefas repetitivas, outrora um fardo para os trabalhadores, liberta-os para atividades mais estratégicas e criativas, permitindo-lhes focar em tarefas que exigem habilidades humanas únicas. A flexibilidade emerge como um dos maiores trunfos da era digital, com o trabalho remoto e a colaboração online a desmantelarem as barreiras geográficas e temporais, proporcionando um equilíbrio mais harmonioso entre vida pessoal e profissional. A comunicação, outrora um processo moroso e burocrático, ganha fluidez e agilidade com ferramentas de comunicação instantânea e videoconferência, facilitando a troca de ideias e a tomada de decisões céleres. Além disso, a internet e as plataformas de conhecimento online democratizam o acesso à informação, promovendo a aprendizagem contínua e o desenvolvimento de novas competências.

No entanto, a jornada rumo à digitalização do trabalho não está isenta de obstáculos. O fantasma do desemprego tecnológico paira sobre alguns setores, com a automação a ameaçar a substituição de trabalhadores por máquinas. A necessidade de requalificação torna-se premente, exigindo que os trabalhadores adquiram novas habilidades para se manterem relevantes no mercado de trabalho em constante evolução. A desigualdade social e econômica corre o risco de se aprofundar, com a falta de acesso à tecnologia e à educação a criar um fosso entre os que têm e os que não têm. A saúde mental dos trabalhadores é posta à prova, com o uso

excessivo de tecnologia e a pressão por resultados a gerarem stress e exaustão. A privacidade e a segurança dos dados pessoais tornam-se preocupações crescentes, exigindo medidas de proteção e transparência por parte das empresas.

Em suma, a tecnologia é uma força transformadora que exige uma abordagem equilibrada e ponderada. É imperativo que empresas e trabalhadores unam esforços para maximizar os benefícios da tecnologia, mitigando os seus riscos. O investimento em educação e requalificação, a promoção de um ambiente de trabalho saudável e a proteção da privacidade dos dados são pilares essenciais para construir um futuro do trabalho mais promissor e equitativo.

## 3.2 A LGPD e seus impactos nas dinâmicas corporativas

Segundo Machado e Marconi (2020), a maneira superior de se compreender instrumentos normativos é por meio do exame dos princípios que compõem o norte dessa determinada lei. Até porque, nenhum desses instrumentos seria capaz de antecipar todas as ocasiões e hipóteses nas quais ele vai ser usado, tornando-se imprescindível estar familiarizado com a base principiológica que os norteiam. Os princípios têm como função atribuir um direcionamento, que irá orientar decisões judiciais em situações em que a letra da lei é exígua. Adicionam os autores que o rastro dos princípios leva à identificação tonal, ou ainda ao intuito almejado pelo legislativo ao atuar, decorrendo daí a imprescindibilidade do conhecimento, interpretação e assimilação das ferramentas que funcionam como a bússola desta ciência jurídica.

É nesse contexto que há de se analisar a legislação de dados no mundo organizacional, seja empresarial ou governamental, uma vez que, ao faltarem os dispositivos específicos que tratam acerca deste conteúdo, muito se extrai dos direitos fundamentais já estudados, que dão sentido a toda a titularidade de garantias de proteção de dados que visou o legislador.

Na década de 60, o processamento informacional automático se encontrava restrito ao governo e a agentes de grande porte do setor privado. O maquinário necessário para esse processamento custava muito caro e ocupava muito espaço. Entretanto, atualmente, até pequenos negócios, como uma banca de jornal, fazem uso cotidiano de ferramentas tecnológicas. Os grandes computadores e sua vasta gama de apetrechos deram lugar a instrumentos gradativamente menores em tamanho e peso, já existindo inclusive a tecnologia em dimensões nano. A superação das barreiras econômicas e físicas permitiu que o

processamento automático da informação se estabelecesse como um procedimento rotineiro. Com o advento da abrupta e significativa queda nos preços de armazenagem, transmissão e processamento da informação, a diminuição da coleta de dados pessoais não tem estímulo econômico nem técnico (Sanden, 2012).

Inegavelmente, as inovações tecnológicas digitais, impulsionadores de inequívocos avanços científicos, põem o país e o globo em experiência de interconectividade ampla e pleno acesso informacional. Com o advento da noção de uma experiência humana compartilhada, vem também a figura dos espaços cibernéticos, o que por sua vez, antagoniza o individualismo e tem como finalidade a coletividade entretida, por meio da retenção de dados pessoais, que se tornaram um valioso ativo para as empresas e organizações em geral (Almeida; Soares, 2022).

Assim, ainda que a Lei Geral de Proteção de Dados não traga dispositivo explícito que aborda expressa e especialmente a proteção de dados do titular nas relações dentro de um contexto organizacional ou de trabalho, não se pode olvidar que a lei se aplica a essas relações, uma vez que o seu artigo 1º mesmo aduz que visa a assegurar o tratamento de dados pessoais das pessoas naturais, com o fito de salvaguardar garantias fundamentais de liberdade e privacidade (Ottoni; Farias, 2022).

Nesse caso, insta asseverar o que trazem Almeida e Soares (2022) acerca do assunto. Afirmam que, além de ditames, orientações normativas, poder regulatório e fundamentos, a Lei Geral de Proteção de Dados Pessoais (LGPD) vem acompanhada do rompimento e subversão culturais nas entidades organizacionais, sejam do setor público ou do setor privado. Isso porque a lei agrega uma responsabilidade majorada na proteção de dados pessoais, viabilizando reavaliar o modo de tratamento e processamento dos dados e ensejando ponderar acerca de seu uso correto, com implicações concretas para os titulares do direito à proteção de seus dados pessoais.

O âmbito digitalizado não possui uma rota alternativa à de se preparar para assimilar e cumprir com o que for regulamentado. Todavia, mostra-se relevante que os setores empresarial e organizacional em sentido amplo se alinhem com o resguardo e processamento de dados pessoais, além de sempre disponíveis para dar suporte aos requerimentos, em rapidez correspondente à da era modernidade digital. Não obstante, as searas da educação e da pesquisa devem ser exemplares no que toca ao atendimento a direitos humanos e ao alinhamento rígido perante os regramentos legais. Em hipótese de não o serem, devem sofrer com sanções, multas severas e advertências substanciais.

Nesse teor, resta incontestável que a relação de trabalho se torna, para todos os efeitos, uma relação entre o agente de tratamento de dados e o proprietário pessoal deles, que

será regida pela LGPD e estará sob a alçada do rol de princípios e fundamentos da norma. Contudo não serão só as relações específicas de trabalho que irão representar a proteção de dados no contexto corporativo e organizacional, uma vez que os titulares de direito à autodeterminação informativa, por exemplo, podem ser clientes, parceiros, ou até outros membros de uma cadeia produtiva.

Até porque, de acordo com Ottoni e Farias (2022), a grande finalidade teleológica da LGPD, em termos amplos, é conduzir com melhor segurança jurídica o tratamento dos dados pessoais do titular, realizado pelos controladores dos dados e operadores, estabelecendo pilares cristalinos para salvaguarda e preservação do direito fundamental. Ademais, é obrigatório estimar que essa reserva alcança todo o ciclo de vida do dado, o que inclui fases que devem ser executadas de acordo com a LGPD.

Se esse é o caso, então seria um contrassenso que se excluísse o trabalhador ou cliente (público atendido também se encaixaria, em caso de organizações governamentais), enquanto pessoas naturais, do ciclo de tratamento de seus dados, diferenciando-os de outros indivíduos e titulares da sociedade. Em verdade, importa asseverar que o contexto organizacional é um dos que vai levantar hipóteses diversas e múltiplas de tratamento de dados, pensando em todo seu ciclo.

Mostra-se relevante pontuar que apesar de não ser o principal enfoque do presente tópico, por não fazer parte do mundo corporativo, é de serventia entender e estudar também o tratamento de dados pelo setor público. Como aduzem Leal Junior, Cordeiro e Leal (2020), pôr o escopo governamental na cobertura da LGPD é forçá-lo a se adequar em searas de segurança que podem ser deixadas de lado. O agente governamental, em tudo que perpassa sua atividade, está cada vez mais pertencente ao digital. Em decorrência disso, muitos são os âmbitos que viabilizam acesso a dados pessoais e informações por meio eletrônico.

Já Paula (2024) disserta ainda acerca do papel crescente da organização empresarial, ao dizer que a dinâmica poder-segurança, conforme analisada acima, ilustra como o equilíbrio de poder mudou o papel dos agentes no ciberespaço além dos estados. Enquanto os governos continuam a reter imenso poder no domínio digital, atores não estatais estão crescendo em poder. À medida que as empresas de tecnologia inovadoras continuam a avançar e as instituições reguladoras da Internet ganham maior autonomia, é provável que o padrão de governança mundial no ciberespaço venha a ser mais diversificado no futuro.

Em reforço, apesar de tratar-se esse segmento do estudo do impacto da LGPD no âmbito corporativo, vale a ressalva rápida de que o setor governamental também emprega

pessoas, possuindo relevância no contexto do presente trabalho como um todo. Independentemente, prosseguir-se-á na análise da atuação corporativa.

De acordo com Reymão, Oliveira e Koury (2023) a LGPD estabelece uma seção completa para delimitar as normas de boa conduta e governança, que está localizada entre os artigos 46 a 51. Essa conduta é caracterizada por como ferramentas de governança corporativa que tem o escopo de firmar processos que possibilitem o alinhamento com o normatizado. Nesse teor, a implementação destes instrumentos por parte dos operadores de dados pessoais tem o fito de viabilizar o ciclo de tratamento e o fortalecer.

Aduzem ainda os autores que é importante delinear a totalidade dos sistemas internos que estejam vinculados ao tratamento de dados pessoais, para que, por meio de uma coleta de todos estes processos, seja viável realizar uma avaliação de riscos. Sendo assim, é formulado um mapeamento dos ciclos internos de diferentes classes de dados pessoais usados e processados.

Para Lima (2020), uma equipe de Tecnologia da Informação é essencial dentro do contexto empresarial, justamente para atender o que a LGPD explicita, qual seja que os agentes de tratamento devem adotar medidas de segurança técnicas e administrativas, controles de acessos, mecanismo de segurança.

Acrescenta que em uma idealização na qual o cerne busca modificar a base e o modo como os procedimentos são desenvolvidos em um núcleo corporativo, o maior empecilho será efetuar uma mudança cultural na empresa. Um novo processo com caráter de complexidade, em empresas que já apresentam certa rigidez por parte de seus empregados, deve mitigar a adesão.

Além disso, a designação de um responsável pela proteção de dados é um ponto central de discussões em ciclo de efetivação da LGPD. Ocorre que a indicação de um encarregado resultaria em gastos para a instituição empresarial, pois ele se tornaria o único incumbido de auxiliar internamente os colaboradores da empresa, proprietários de dados pessoais, acerca da boa conduta de tratamento de dados, além de checar se o praticado está em consonância com normas externas e internas. Nesse caso, o investimento em cursos de capacitação e certificações seriam primordiais (Lima, 2020).

Diante de todo o exposto, fica evidente que a atividade empresarial deve ser modificada, tendo em mente objetivos comuns: a diminuição dos riscos identificados pelo mapeamento e a mitigação de contraposições à LGPD. Assim, o comprometimento da empresa é o núcleo que pode realmente mudar toda a prática corporativa nesse direcionamento, a qual

deve restar conforme valores alinhados com os princípios de tratamento de dados pessoais (Reymão; Oliveira; Koury, 2023).

### 3.3 O papel do empregador como agente de tratamento de dados

Dentro do contexto corporativo, é coerente declarar que a relação de emprego é uma das dinâmicas mais relevantes em exercício, além de predominante para a finalidade organizacional. Isto posto, faz-se necessário examinar o desenvolvimento de uma proteção de dados voltada a essa relação específica, uma vez que isso será essencial para a análise da problemática destacada no presente trabalho.

Pamplona Filho e Coni Júnior (2021) lançam as bases do tópico, quando listam que, em conformidade com a Lei Geral de Proteção de Dados (LGPD), o empregado deve consentir com o uso dos dados em cada relação jurídica individual. A empresa também deve estar preparada para assegurar o cumprimento dos direitos dos empregados como titulares de dados pessoais (direito de acessar os dados, confirmar o processamento, corrigir dados, anonimizar, bloquear ou eliminar dados desnecessários e dados processados em desacordo com a LGPD). Além disso, o empregado tem o direito (mediante solicitação) à portabilidade dos dados de acordo com a transferência de histórico de trabalho, registros médicos e serviços contábeis. O trabalhador também tem o direito de ser informado se, e quais, dados pessoais e para quais finalidades seus dados pessoais são compartilhados com autoridades públicas e outras empresas com as quais o empregador possui uma relação jurídica. Por fim, o empregado pode solicitar que seus dados pessoais sejam removidos e revogar o consentimento previamente dado.

Torna-se imprescindível rememorar que, no que se refere aos dados pessoais, não são apenas nomes, prenomes, endereços e CPF. Em visão mais abrangente, consonante com a delimitação realizada pela própria lei, o número de identificação de seguridade social ou dados bancários para pagamento do salário se alocam nessa conceituação de dados pessoais. Já no tocante aos dados sensíveis, esses se explicitam em categoria especial, relacionada ao próprio âmbito íntimo da pessoa, qual sejam, aqueles dados que se vazados devem ensejar impactos como discriminação sem justificativa (Ottoni; Farias, 2022).

De acordo com Yaegashi e Otero (2022), uma relação de emprego, multifacetada por si só, deve ser reavaliada e reorganizada fundamentando-se na nova seara de uma titularidade de direitos à proteção de dados pessoais, com o escopo de assegurar a devida observância aos direitos de personalidade do empregado-titular num contexto de sociedade

informacional, protegendo sua privacidade, sua autodeterminação informativa e outras diversas garantias que são decorrentes de sua dignidade como pessoa humana.

Além disso, é inequívoco que as relações de trabalho não se eximem dos impactos da revolução digital, assim como não se eximem as ideias que abordam direitos à privacidade e proteção de dados. A escala instituída por esta revolução influencia notadamente as duas áreas. No que se refere às relações de emprego, é de suma importância atenção para a implementação e adaptação veloz ao mercado. Já em relação à privacidade e proteção de dados, reforça-se que devem ser compreendidos como garantias fundamentais, o que vem com o advento de diferente relevância de tratamento (Buim Junior, 2020).

Ademais, é plausível afirmar que a teleologia da LGPD é baseada em assegurar privacidade e transparência no que se refere ao tratamento dos dados, especialmente dos consumidores, empregados e prestadores de serviço, gerando para a totalidade das empresas, independentemente do tamanho ou natureza da atividade, a obrigação de respeitar as novas diretrizes legislativas e se adaptar para seguir o vasto rol de deveres que acompanha os direitos dos titulares dos dados pessoais (Alcântara, 2021).

Em suma, como sedimentado, a própria finalidade principiológica da LGPD aplica uma noção de proteção de dados enquanto instituto a ser observado, derivado de direitos fundamentais já trabalhados. O empregado, aqui, ocupará a posição de titular na relação específica supramencionada. Entretanto, o Direito do Trabalho não deverá e não será tratado como ordinário no espectro de atuação da proteção de dados.

É nesse sentido que Pamplona Filho e Coni Junior (2021) dizem que a Lei Geral de Proteção de Dados (LGPD) tem impacto direto em múltiplos âmbitos do Ordenamento Jurídico, que vai da seara constitucional de direito fundamental à intimidade e privacidade, até os diferentes campos jurídicos, especialmente no Direito do Trabalho.

É possível afirmar, inclusive, que o Direito do Trabalho restará como um dos mais atingidos pelos ditames da LGPD, uma vez que a relação de emprego é composta de consistente fornecimento, utilização, transferência e armazenamento de dados pessoais, não sendo a lei eivada de discriminação ou diferenciação perante porte ou atividade empresarial (Alcântara, 2021).

É por isso que dizem Yaegashi e Otero (2022) que, nesse sentido, é imperativo promover uma evolução no cenário de responsabilidade, particularmente movendo a narrativa de uma cultura de mitigação de danos *ex-post* para uma cultura de prevenção e responsabilidade, conforme manifestado pelos dispositivos regulatórios da Lei Geral de Proteção de Dados. Como uma regulamentação fundamental e essencial para a garantia dos

direitos pessoais, ela dá à pessoa a responsabilidade de assegurar seus direitos e não apenas ser um simples consentidor de decisões sobre seus dados pessoais.

O que tentam trazer à tona os autores é a necessidade de uma modificação no paradigma cultural, de modo que, ao invés do enfoque reparatório, possa ser implementado um direcionamento mais voltado a evitar e precaver qualquer dano, transformando o empregado no principal personagem do seu cenário de direitos e garantias em tela. Isso não significa que ficará sem papel o empregador na relação.

Para Lima (2020), o agente de tratamento de dados está imbuído de conexão direta com o proprietário, devendo implementar diretrizes de boas condutas de segurança e governança, para que esse tratamento fique alinhado com as medidas adotadas pela LGPD. É também dever do controlador armazenar um registro das instruções referentes à política de cada empresa, o que enseja a imprescindibilidade de instrumentos de documentação dos processos aplicados.

Ocorre que, para que meramente se inicie a relação entre os dois sujeitos apresentados, um deles precisa apresentar o seu consentimento, conceito importantíssimo para o entendimento da dinâmica de proteção. Nesse caso, a figura que irá consentir ou apresentar sua anuência é o proprietário de dados pessoais, qual seja o empregado.

Isso se deve ao fato de que, os inquestionáveis receptáculos da proteção do banco de dados de uma organização serão os empregados ou prestadores de serviços. Entretanto, são necessários alguns requisitos para que esse consentimento supracitado seja válido: ele deve ser fornecido de forma clara, expressa, esclarecida e granulada, de modo que a empresa gestora dos dados possa dar o tratamento adequado (Alcântara, 2021).

Reforça Fidelis (2023) que, à medida que a quantidade de dados armazenados e compartilhados em formato digital continua a crescer, a imprevisibilidade do cenário de negócios da cannabis tornou claro que a proteção de dados pessoais é mais relevante do que nunca no mundo de hoje. É importante proteger a privacidade individual porque esses dados são vulneráveis à exploração por terceiros. O consentimento individual, nesse contexto, forma um mecanismo crítico de controle sobre as informações pessoais, cuja proteção é vital para manter a autonomia privada do cidadão.

Adicionam Yaegashi e Otero (2022) que, no que se refere às novas relações de emprego ou mesmo às em vigência, é dever do empregador desenvolver as modificações necessárias, de modo a adotar a sistemática da LGPD. Nesse sentido, em relação às cláusulas que tratem acerca de dados pessoais, essas serão esposadas de maneira explícita e clara no instrumento contratual, possibilitando ao titular conhecer de seu teor e das suas garantias, com

o fito de que não reste dúvida acerca da validade do consentimento que irá disponibilizar esses dados ao empregador.

Em síntese, os autores buscam fixar a noção de que o consentimento do proprietário de dados pessoais tem de ser inegavelmente claro e instruído, independentemente de ser trazido à tona na fase pré-contratual ou mesmo já no decorrer do contrato de trabalho, de modo a se adequar à LGPD. Nessa senda, faz sentido aprofundar um pouco mais a análise acerca das fases do tratamento de dados, que será um discernimento vital para o estudo dos desafios a serem apresentados.

É necessário ponderar que, nas relações empregatícias, desde a fase pré-contratual até o fim da relação, tem-se diversos dados pessoais que necessitam ser fornecidos pelo candidato, à vaga de emprego e à empresa. Essa gama de dados inclui o *curriculum*, inicialmente, até a fase de contratação, em que são fornecidos e guardados documentos, para a observância de diretrizes da legislação pertinente. (Ottoni; Farias, 2022). Aqui, vale o destaque para a fase pré-contratual e os processos seletivos, que muitas vezes iniciam uma relação de tratamento de dados antes de uma relação empregatícia.

Repise-se que a LGPD traz consigo abundantes modificações de tratamento e utilização de dados das pessoas, o que causou, certamente, grande mudança na relação entre titulares de direitos de privacidade e agentes de tratamento de dados. Isso influencia significativamente diferentes setores empresariais, como é o caso do setor de Recursos Humanos e, por consequência, dos processos de seleção das empresas para vagas abertas (Gomes, 2022).

Insta ressaltar que, já segundo Yaegashi e Otero (2022), no que se refere aos mecanismos característicos que serão implementados no decurso de um contrato de trabalho, são proeminentes os preliminares e os ulteriores, que no caso representaria, o fim da relação de tratamento de dados. Os processos seletivos e a gestão de um banco de dados curriculares são os primeiros itens que devem atrair relativo cuidado do empregador no que diz respeito ao tratamento de dados dentro de um contexto empregatício, uma vez que são compostos pelo fornecimento e administração de dados de candidatos para possível ocupação de vagas na organização.

Fica em evidência que existem autores que irão mencionar a ideia de um término de relação de emprego como término também do tratamento de dados pelo empregador. Contudo, como será visto mais a frente, essa tese não se sustentará. Em complementação, importa abordar que essas fases em sua totalidade também sofrem impactos diretos da revolução digital.

A título de exemplificação, aduzem Santos e Graminho (2024) que, em muitas empresas, algoritmos de inteligência artificial são usados na gestão das relações trabalhistas. Mas, apesar das alegações de que esses algoritmos são neutros, eficientes e infalíveis, sua estrutura impõe limitações críticas que, às vezes, resultam em falhas imprevisíveis. Além disso, há questões sobre se é possível haver discriminação nas relações trabalhistas, levando em conta o uso de algoritmos de inteligência artificial na gestão dessas relações.

Aqui, os autores tocam na questão referente ao uso de algoritmos de inteligência artificial nas relações de trabalho, alertando acerca da possibilidade do exercício de práticas discriminatórias por meio deles. Há relevância na ideia de que a automatização desses processos poderia gerar discriminação, por exemplo, na fase de contratação, ou ainda na efetivação de uma promoção dentro do contexto empresarial. De todo modo, esse não é o único desafio a ser tratado.

Outro empecilho sumário para o tratamento de dados pessoais nas relações de trabalho está na exiguidade de diferenciação entre os instrumentos dos quais faz uso o empregado e os colocados à disposição pelo empregador para a execução dos serviços. Isso aumenta, dentre outras questões, a capacidade de rastreio e fiscalização do empregador para com o empregado, de modo que há de se proceder com cuidado (Yaegashi; Otero, 2022). Acrescente-se que, para tratar dessa questão, faz-se uso da "conteinerização", que é composta pela elaboração de um "contêiner" interno no maquinário próprio do trabalhador, com o fito de armazenar e gerir informações exclusivas da empresa. A aplicação desse programa irá se basear na anuência do empregado e será de uso adstrito às atribuições e atividades da empresa (Yaegashi; Otero, 2022).

Em resumo, a relação de emprego ocupa uma posição central no mundo corporativo, e a proteção de dados dentro deste contexto é de extrema importância. De acordo com a LGPD, é necessário o consentimento do empregado para o tratamento de seus dados, conferindo a ele vários direitos, tais como acesso, correção, anonimização e portabilidade de seus dados. Além disso, a lei define o que são dados pessoais e sensíveis, sendo que os últimos exigem um cuidado ainda maior devido à sua natureza íntima.

A LGPD não apenas estabelece direitos, mas também demanda uma mudança cultural nas empresas. O foco deve migrar da reparação de danos para a prevenção, com o empregado assumindo um papel central no controle de suas informações. O empregador, na função de agente de tratamento de dados, deve implementar políticas de segurança e governança, assegurando que o consentimento do empregado seja claro, expresso e informado.

A revolução digital e o uso de novas tecnologias introduzem desafios adicionais. A utilização de algoritmos de inteligência artificial, por exemplo, pode gerar discriminação, exigindo uma vigilância constante para evitar tais práticas. A dificuldade em distinguir entre os instrumentos de trabalho usados pelo empregado e os fornecidos pelo empregador também requer cautela, pois isso pode aumentar a capacidade de rastreamento e fiscalização. A "containerização" se apresenta como uma solução potencial, permitindo a separação das informações da empresa e do empregado, desde que com o consentimento deste.

Por fim, é cediço que as diversas fases do tratamento de dados, desde o período pré-contratual até o término do contrato, requerem atenção especial, sobretudo em processos seletivos e na gestão de dados curriculares. Entretanto, pouco ainda se debate a respeito do período pós-contratual, alvo de inovações tecnológicas e documentais que trazem em seu seio desafios de suma importância para a efetividade da proteção de dados do empregado.

# 4 A FASE PÓS-CONTRATUAL E OS DESAFIOS DA INOVAÇÃO DOCUMENTAL

Como já tratado, é inegável que a fase que se constitui após o término do contrato de trabalho é essencial na lisura do tratamento de dados do empregado-titular. Entretanto, a combinação de sua natureza particular com inovações tecnológicas e normativas gera desafios jurídicos de ordem de complexidade inédita, tanto para o Direito do Trabalho, quanto para o arcabouço legal da proteção de dados.

## 4.1 Relações de emprego no mundo digital

Desde a fase inicial de negociação até a rescisão do contrato de trabalho, a vulnerabilidade econômica do trabalhador o torna subserviente ao empregador. O primeiro ponto é que essa desigualdade não é reconhecida pela visão liberal, de modo que o contrato de trabalho não pode ser considerado um contrato comercial regulado pelo Direito Civil, onde se presume um equilíbrio entre as partes. Devido à inadequação do modelo civil, a teoria contratualista moderna é uma nova teoria relativa à relação de emprego (Pires, 2023).

A vulnerabilidade econômica do trabalhador, inerente à relação de emprego, é um fator determinante na dinâmica de poder entre empregado e empregador. Desde as negociações iniciais, o trabalhador, muitas vezes dependente do salário para sua subsistência, encontra-se em uma posição de desvantagem em relação ao empregador, que detém o poder de contratar ou não. Essa assimetria de poder se mantém ao longo do contrato de trabalho, influenciando as condições de trabalho, a remuneração e a possibilidade de desligamento.

A visão liberal clássica, que pressupõe a igualdade entre as partes contratantes, não se aplica à relação de trabalho, onde a desigualdade é uma característica intrínseca. O Direito Civil, que rege os contratos comerciais, parte do princípio de que as partes são livres e iguais para negociar seus termos. No entanto, essa premissa não se sustenta na relação de trabalho, onde o trabalhador, em virtude de sua vulnerabilidade econômica, tem pouca margem de negociação e, muitas vezes, se vê obrigado a aceitar as condições impostas pelo empregador.

A teoria contratualista moderna surge como uma resposta à inadequação do modelo civil para explicar a relação de emprego. Essa teoria reconhece a desigualdade inerente à relação de trabalho e busca proteger o trabalhador de abusos e exploração. Ao invés de tratar o contrato de trabalho como um mero contrato comercial, a teoria contratualista moderna o encara como um contrato especial, que exige uma proteção jurídica diferenciada em virtude da vulnerabilidade do trabalhador.

Já a reflexão oferecida por Ferreira, Falcão e Bizzocchi (2022) vem com novos deveres impostos aos empregadores, quando afirma que cabe à classe patronal gerenciar o tempo efetivo de armazenamento de dados pessoais. De acordo com a Lei Geral de Proteção de Dados (LGPD), no Artigo 16, os dados pessoais devem ser eliminados após o tratamento dos dados. Contudo, se forem usados para defesas trabalhistas ou previdenciárias para a aposentadoria de um ex-funcionário, e então imediatamente descartados, isso causará muitos problemas para o empregador.

A Lei Geral de Proteção de Dados (LGPD) impõe aos empregadores uma série de obrigações em relação ao tratamento de dados pessoais de seus empregados, incluindo o dever de gerenciar o tempo de armazenamento desses dados. O artigo 16 da LGPD estabelece que os dados pessoais devem ser eliminados após o término de seu tratamento. No entanto, essa regra pode gerar dificuldades para o empregador, que muitas vezes necessita manter os dados por um período mais longo para se proteger em casos de litígios trabalhistas ou para cumprir obrigações legais, como o fornecimento de informações para a aposentadoria de ex-empregados.

Essa situação revela um conflito entre a proteção da privacidade dos empregados e a necessidade de o empregador preservar provas e cumprir obrigações legais. A LGPD busca equilibrar esses dois interesses, estabelecendo regras claras sobre o tratamento de dados pessoais, mas permitindo exceções em casos específicos, como a necessidade de defesa em juízo ou o cumprimento de obrigações legais.

É importante ressaltar que o empregador deve sempre observar os princípios da LGPD, como a finalidade, a necessidade e a proporcionalidade, ao tratar os dados pessoais de seus empregados. Isso significa que o empregador só pode coletar os dados estritamente necessários para a finalidade pretendida e deve mantê-los armazenados pelo tempo mínimo necessário. Além disso, o empregador deve garantir a segurança dos dados e informar os empregados sobre o tratamento de seus dados pessoais.

Consequentemente, o armazenamento de dados pode ser intrusivo na privacidade de candidatos, funcionários e ex-trabalhadores, mas apenas se forem dados pessoais imateriais ao vínculo empregatício (Buim Júnior, 2020). O armazenamento de dados pessoais de candidatos, funcionários e ex-funcionários, quando excessivo ou irrelevante para a relação de emprego, pode configurar uma invasão de privacidade. Informações sobre a vida pessoal, convicções religiosas, orientação sexual ou histórico de saúde, por exemplo, não devem ser coletadas ou armazenadas, a menos que sejam estritamente necessárias para a finalidade do tratamento, como em casos de exames admissionais ou para o cumprimento de obrigações legais relacionadas à saúde e segurança do trabalho.

A coleta e o armazenamento de dados pessoais devem ser limitados ao mínimo necessário para a finalidade pretendida, e o empregador deve garantir a segurança dos dados, evitando o acesso não autorizado e o vazamento de informações. Além disso, o empregador deve informar os titulares dos dados sobre o tratamento de suas informações pessoais, incluindo a finalidade da coleta, o tempo de armazenamento e os direitos que eles possuem, como o direito de acesso, retificação e eliminação de seus dados.

É fundamental que os empregadores adotem políticas e práticas de proteção de dados pessoais, em conformidade com a LGPD, para garantir a privacidade e a segurança das informações de seus empregados. Essas políticas devem incluir a definição de regras claras sobre a coleta, o armazenamento e o uso de dados pessoais, bem como a implementação de medidas de segurança técnicas e administrativas para proteger os dados de acessos não autorizados e vazamentos.

## 4.2 O eSocial e a digitalização da CTPS

A plena implementação do eSocial significa que todas as empresas privadas serão obrigadas a fornecer informações por meio da plataforma em questão, o que preenche automaticamente a versão digital da Carteira de Trabalho e Previdência Social (CTPS). E, nesse sentido, é importante saber como a Tecnologia da Informação está incorporada na rotina dos brasileiros para analisar os impactos do documento digital. Diversas tecnologias passaram por um processo evolutivo e seu uso apresenta aspectos positivos e negativos (Cunha; Nascimento; Dias, 2023).

O eSocial, sistema unificado de informações trabalhistas, previdenciárias e fiscais, representa um marco na digitalização das relações de trabalho no Brasil. A obrigatoriedade de todas as empresas privadas de fornecer informações por meio da plataforma do eSocial trouxe impactos significativos para a rotina dos brasileiros, tanto para empregadores quanto para trabalhadores.

Para os empregadores, o eSocial simplificou o cumprimento de obrigações legais, como o envio de informações sobre folha de pagamento, FGTS e Rais. Além disso, o sistema contribuiu para a redução da burocracia e a diminuição de erros e fraudes. No entanto, a implementação do eSocial também exigiu das empresas investimentos em tecnologia e treinamento de pessoal, além de adaptação a novas rotinas e prazos.

Para os trabalhadores, o eSocial facilitou o acesso a informações sobre seus direitos trabalhistas e previdenciários, já que a CTPS digital é alimentada automaticamente com os

dados enviados pelas empresas. Além disso, o sistema contribuiu para a transparência nas relações de trabalho e a fiscalização do cumprimento das obrigações por parte dos empregadores. No entanto, a digitalização da CTPS também gerou preocupações em relação à segurança dos dados pessoais e a possibilidade de exclusão digital de trabalhadores com menor acesso à tecnologia.

É importante ressaltar que a tecnologia, apesar de trazer diversos benefícios, também apresenta desafios e riscos. A utilização de ferramentas digitais no âmbito das relações de trabalho exige cuidados em relação à proteção de dados pessoais, à segurança da informação e à garantia do acesso à tecnologia para todos os trabalhadores.

Ainda apontou Sanden (2012), que o destino das informações relacionadas aos empregados após o término do contrato raramente é regulamentado. Acompanhando a relação empregado-empregador ao longo do tempo, é possível explorar quais atividades de processamento de informações — aquisição de informações e utilizações de informações — ocorrem ao longo do tempo e incluem fenômenos em uma extremidade do espectro, como as negociações pré-contratuais, e na ponta indesejada do espectro, as exceções que seguem a expiração de uma relação jurídica.

Em relação ao próprio contrato, de fato, devido à enorme quantidade de informações sobre o empregado, mesmo no final do contrato, o empregador ainda possui essas informações. No entanto, a rescisão do contrato de trabalho não exonera o empregador de observar restrições em relação ao tratamento desses dados. O problema também não é rigidamente estruturado em cada fase, pois não temos subordinação nas negociações contratuais prévias ou em situações pós-contratuais, e o poder diretivo do empregador não é explícito. Dada a complexidade teórica de cada fase, vale a pena explorar como esses aspectos são abordados na doutrina ou jurisprudência (Sanden, 2012).

Frente a: (i) o período que as empresas devem manter documentos cujo conteúdo pode referir-se aos direitos trabalhistas de seus empregados e ex-empregados; (ii) a existência de alguns dados que podem exercer direitos em possíveis litígios futuros, o processamento de dados pessoais é permitido pela legislação vigente (Buim Júnior, 2020).

A necessidade de as empresas manterem documentos relacionados aos direitos trabalhistas de seus empregados e ex-empregados por um período prolongado, muitas vezes para se protegerem em eventuais litígios, é um fator importante a ser considerado no contexto da proteção de dados pessoais. A legislação trabalhista exige que os empregadores conservem diversos documentos, como a Carteira de Trabalho e Previdência Social (CTPS), o livro de registro de empregados, os exames médicos e outros comprovantes de pagamentos e benefícios.

Esses documentos contêm dados pessoais dos empregados, como nome, CPF, endereço, histórico profissional, informações salariais e de saúde.

A Lei Geral de Proteção de Dados (LGPD) estabelece que o tratamento de dados pessoais deve ter uma finalidade específica e legítima, e que os dados devem ser eliminados após o cumprimento dessa finalidade. No entanto, a legislação trabalhista, em muitos casos, exige que os documentos sejam mantidos por um período superior ao necessário para o cumprimento da finalidade original. Essa situação gera um conflito entre a LGPD e a legislação trabalhista, que exige uma solução equilibrada que garanta a proteção dos dados pessoais dos empregados, mas que também permita que as empresas cumpram suas obrigações legais e se protejam em casos de litígio.

Quando a informação se refere ao indivíduo, como anotações na Carteira de Trabalho e Previdência Social ou informações sobre a remuneração do empregado na folha de pagamento, o elemento de dados está presente. Os pontos legais que formalizam a necessidade ou possibilidade de proceder com os dados de um empregado são: anotações na CTPS (art. 29 da CLT); livro de registro de empregados (art. 41 da CLT); exames médicos (art. 168 da CLT); e dever de comunicar doenças ocupacionais (art. 169 da CLT); obrigação de apresentação da Relação Anual de Informações Sociais (art. 360 da CLT) (Sanden, 2012).

Os dados pessoais dos empregados, como anotações na CTPS e informações sobre remuneração na folha de pagamento, são informações intrinsecamente ligadas à sua individualidade e, portanto, merecem proteção especial. A LGPD define dados pessoais como qualquer informação relacionada a uma pessoa natural identificada ou identificável. As anotações na CTPS, por exemplo, contêm informações sobre o histórico profissional do empregado, como empresas em que trabalhou, cargos que ocupou, salários e períodos de trabalho. Essas informações são importantes para o empregado, pois podem ser utilizadas para comprovar seu tempo de serviço para fins de aposentadoria, por exemplo.

As informações sobre remuneração na folha de pagamento também são dados pessoais sensíveis, pois revelam informações sobre a vida financeira do empregado. Essas informações devem ser tratadas com cautela e protegidas de acessos não autorizados, pois podem ser utilizadas para fins discriminatórios ou para invadir a privacidade do empregado. É importante ressaltar que a LGPD estabelece que o tratamento de dados pessoais sensíveis, como os dados de saúde e os dados financeiros, exige um consentimento específico e destacado do titular dos dados. Além disso, o tratamento desses dados deve ser realizado com ainda mais cautela e observar os princípios da finalidade, necessidade e proporcionalidade.

A legislação trabalhista estabelece uma série de obrigações para os empregadores em relação ao tratamento de dados pessoais de seus empregados. O artigo 29 da CLT, por exemplo, estabelece que a CTPS deve conter anotações sobre o contrato de trabalho, como data de admissão, salário e função. O artigo 41 da CLT determina que o empregador deve manter um livro de registro de empregados, com informações sobre cada um de seus funcionários.

Além dessas obrigações, a legislação trabalhista também estabelece outras exigências que envolvem o tratamento de dados pessoais dos empregados, como a realização de exames médicos admissionais e periódicos (art. 168 da CLT) e a comunicação de doenças ocupacionais (art. 169 da CLT). Essas obrigações exigem que o empregador colete e armazene dados pessoais sensíveis de seus empregados, como informações sobre saúde.

A Relação Anual de Informações Sociais (RAIS) é outra obrigação legal que exige que o empregador informe ao governo dados sobre seus empregados, como nome, CPF, data de nascimento, salário e função. Essas informações são utilizadas pelo governo para fins estatísticos e para o cálculo de benefícios sociais, como o seguro-desemprego.

Hoje sabemos que a nova promulgação do artigo 6º da CLT autorizou a utilização de meios telemáticos e informatizados para o exercício do poder diretivo do empregador (Lei nº 12.551/2011), mas não tratou nem das condições nem dos limites para o exercício desse poder (Sanden, 2012).

A Lei nº 12.551/2011, que alterou o artigo 6º da CLT, autorizou o uso de meios telemáticos e informatizados para o exercício do poder diretivo do empregador. Essa alteração legislativa reconheceu a realidade do trabalho a distância e do uso de tecnologias de comunicação no ambiente de trabalho. No entanto, a lei não estabeleceu as condições e os limites para o exercício desse poder diretivo por meio de meios telemáticos e informatizados.

Essa lacuna legislativa gera insegurança jurídica para empregadores e empregados, pois não há clareza sobre como o empregador pode exercer seu poder diretivo por meio de tecnologias de comunicação, como email, mensagens instantâneas e videoconferências. Questões como o controle do horário de trabalho, a fiscalização do desempenho dos empregados e a utilização de equipamentos e softwares fornecidos pela empresa ficam sem regulamentação específica.

É importante que o legislador estabeleça regras claras sobre o uso de meios telemáticos e informatizados para o exercício do poder diretivo do empregador, a fim de garantir a proteção dos direitos dos trabalhadores e a segurança jurídica para as empresas.

### 4.3 Cadeia de custódia e integridade de documentos digitais

De acordo com Silva, Siebra e Santos (2023), para assegurar a validade e confiabilidade dos documentos ao longo de seu ciclo de vida, a cadeia de custódia deve ser rigorosamente mantida em todas as suas fases, independentemente da idade dos documentos. Nesse contexto, a utilização de ferramentas tecnológicas que garantam a autenticidade e integridade dos documentos digitais torna-se indispensável para prevenir a ruptura da cadeia de custódia.

A manutenção da cadeia de custódia em todas as fases do ciclo de vida dos documentos digitais é crucial para garantir sua validade e confiabilidade. Isso se torna ainda mais relevante em um contexto em que a digitalização de processos e documentos é cada vez mais presente. A integridade e a autenticidade dos documentos digitais podem ser comprometidas por diversos fatores, como alterações não autorizadas, corrupção de dados ou falhas nos sistemas de armazenamento.

A utilização de ferramentas tecnológicas adequadas é fundamental para assegurar a preservação da cadeia de custódia. Soluções como assinaturas digitais, carimbos de tempo, *hash functions* e sistemas de gestão documental com controle de acesso e trilha de auditoria são essenciais para garantir que os documentos digitais permaneçam íntegros e autênticos ao longo do tempo. Além disso, é importante que as organizações adotem políticas e procedimentos claros para o manuseio e armazenamento de documentos digitais, definindo responsabilidades e estabelecendo controles para evitar alterações não autorizadas.

A interrupção da cadeia de custódia pode ter consequências graves, especialmente em contextos legais, onde a validade dos documentos digitais pode ser questionada. Em casos de litígios, por exemplo, a falta de evidências que comprovem a integridade e a autenticidade dos documentos digitais pode levar à sua desconsideração como prova. Portanto, investir em ferramentas tecnológicas e adotar práticas de gestão de documentos digitais que garantam a manutenção da cadeia de custódia é fundamental para proteger a integridade e a validade dos documentos digitais, assegurando sua confiabilidade em todas as fases do seu ciclo de vida.

A dinâmica das relações entre indivíduos e empresas exige a formulação de novas normas, princípios e regulamentações, a fim de adaptar os princípios contratuais tradicionais do Direito ao contexto contemporâneo, preservando sua essência. É imprescindível compreender o funcionamento das novas tecnologias de comunicação e contratação, como a Internet, e sua evolução no cenário de convergência, uma vez que o Direito está intrinsecamente ligado ao comportamento social e à linguagem (Rubini, Gehelen; 2023).

A transformação digital impulsionou uma reconfiguração das interações sociais e comerciais, tornando imperativa a adaptação do arcabouço jurídico. A necessidade de novas regras, princípios e regulamentações surge da inadequação dos modelos tradicionais para lidar com as complexidades das relações mediadas por tecnologia. A aplicação dos antigos princípios contratuais, embora fundamental para a manutenção da coerência e da segurança jurídica, exige uma releitura à luz das novas realidades, preservando a essência do Direito enquanto se adapta às demandas contemporâneas.

A compreensão do funcionamento das novas tecnologias de comunicação e contratação, como a Internet, é essencial para a construção de um Direito que acompanhe a evolução social. A convergência tecnológica, caracterizada pela integração de diferentes mídias e plataformas, exige uma abordagem multidisciplinar e flexível, capaz de lidar com a rápida obsolescência das tecnologias e a emergência de novos paradigmas. O Direito, enquanto expressão do comportamento social e da linguagem, deve ser capaz de captar as nuances dessas transformações, incorporando-as em suas normas e princípios.

A dinâmica das relações na era digital exige um Direito que seja capaz de equilibrar a proteção dos direitos individuais com a promoção da inovação e do desenvolvimento tecnológico. A busca por esse equilíbrio passa pela construção de um arcabouço jurídico que seja capaz de garantir a segurança jurídica, a previsibilidade e a confiança nas relações mediadas por tecnologia, ao mesmo tempo em que estimula a criação de novas soluções e modelos de negócio. A adaptação do Direito à era digital é um processo contínuo e desafiador, que exige a participação de diversos atores, como legisladores, juristas, empresas, sociedade civil e academia.

Devido à natureza efêmera dos recursos digitais e à rápida obsolescência tecnológica inerente a esse ambiente, é essencial reunir informações que assegurem, ou pelo menos busquem um grau razoável de segurança, a capacidade de reproduzir o ambiente computacional original ao longo do tempo. Isso garante que os registros permaneçam acessíveis, independentemente do formato e das condições técnicas iniciais. Os metadados, conjunto de atributos que descrevem os dados, desempenham um papel crucial nesse processo. Eles permitem que os dados contidos em um documento digital se transformem em um documento manifestado e acessível ao usuário no futuro. Isso se dá pela associação do conteúdo fundamental do documento com as transações e requisitos que o validam. Essa combinação constitui um registro digital que, quando criado para evidenciar e servir como prova das atividades de uma pessoa ou instituição, torna-se um registro digital arquivístico (Silva; Araújo, 2024).

Ou seja, a garantia da preservação e acessibilidade de registros digitais ao longo do tempo depende da capacidade de reproduzir o ambiente computacional original, o que exige a captura e o armazenamento de metadados abrangentes. Esses metadados devem incluir informações sobre o software, hardware, sistema operacional e outros componentes tecnológicos utilizados na criação e no manuseio dos registros. A falta de metadados adequados pode levar à perda de acesso aos registros digitais, especialmente quando as tecnologias originais se tornam obsoletas ou incompatíveis com os sistemas atuais.

A implementação de contratos inteligentes representa uma inovação disruptiva no cenário das transações comerciais, ao automatizar e garantir a execução de acordos sem a necessidade de intermediários. Essa tecnologia, baseada em blockchain, confere transparência e segurança às transações, uma vez que todas as informações e ações são registradas de forma imutável e acessível a todas as partes envolvidas (Goulart, 2021).

A natureza autoexecutável dos contratos inteligentes elimina a possibilidade de manipulação ou descumprimento dos termos acordados, uma vez que as ações são executadas automaticamente quando as condições predefinidas são atendidas. Essa característica confere maior agilidade e eficiência às transações, além de reduzir os custos e riscos associados à intermediação de terceiros.

A utilização de contratos inteligentes abrange diversas áreas, desde transações financeiras e imobiliárias até a gestão de cadeias de suprimentos e o registro de propriedade intelectual. A capacidade de automatizar e garantir a execução de acordos de forma segura e transparente torna essa tecnologia uma ferramenta poderosa para a construção de relações comerciais mais eficientes e confiáveis.

Aduz Sousa (2022), que, considerando que o conhecimento se materializa em documentos de inteligência digital, é fundamental revisitar o conceito de documento e compreender o papel das ferramentas de automação na gestão documental e arquivística. A evolução da inteligência em documentos digitais exige uma revisão do conceito tradicional de documento, expandindo-o para abranger a natureza dinâmica e interativa dos registros digitais. Nesse contexto, a inteligência materializa-se em documentos que não apenas armazenam informações, mas também as processam, analisam e compartilham, transformando dados brutos em conhecimento acionável. A compreensão dessa nova realidade documental é fundamental para a gestão eficaz da informação na era digital.

As ferramentas de automação desempenham um papel crucial na gestão de documentos de inteligência digital, permitindo a coleta, o processamento, a análise e a disseminação de informações de forma eficiente e segura. Essas ferramentas incluem sistemas

de gestão documental (SGD), softwares de reconhecimento óptico de caracteres (OCR), plataformas de análise de dados e soluções de inteligência artificial (IA) para automação de fluxos de trabalho. A utilização dessas tecnologias permite a criação de um ambiente de gestão documental ágil, flexível e adaptado às necessidades específicas de cada organização.

A automação da gestão documental e arquivística possibilita a otimização de processos, a redução de custos, o aumento da segurança da informação e a melhoria da tomada de decisões. Ao automatizar tarefas como a indexação, a classificação, o arquivamento e a recuperação de documentos, as organizações podem liberar recursos para atividades mais estratégicas, reduzir o risco de erros humanos e garantir a conformidade com as normas e regulamentações aplicáveis. Além disso, a utilização de ferramentas de IA para análise de dados permite a extração de insights valiosos a partir dos documentos, transformando a informação em conhecimento estratégico para a organização.

A LGPD impõe aos empregadores uma série de obrigações em relação ao tratamento de dados pessoais, gerando um conflito entre a proteção da privacidade dos empregados e a necessidade de o empregador preservar provas e cumprir obrigações legais. O eSocial, sistema unificado de informações trabalhistas, previdenciárias e fiscais, representa um marco na digitalização das relações de trabalho, com impactos significativos para empregadores e trabalhadores.

A questão do tratamento de dados dos empregados após o término do contrato de trabalho é outro ponto relevante, destacando a falta de regulamentação específica sobre o tema. A garantia da preservação e acessibilidade de registros digitais ao longo do tempo depende da capacidade de reproduzir o ambiente computacional original, o que exige a captura e o armazenamento de metadados abrangentes.

A implementação de contratos inteligentes representa uma inovação disruptiva no cenário das transações comerciais, ao automatizar e garantir a execução de acordos sem a necessidade de intermediários. A evolução da inteligência em documentos digitais exige uma revisão do conceito tradicional de documento, expandindo-o para abranger a natureza dinâmica e interativa dos registros digitais.

A coletânea de modificações apresentada constitui uma nova realidade automatizada no que se trata da relação empregatícia, a qual demanda aplicação cuidadosa dos princípios de responsabilidade civil listados, dada a natureza delicada do processo de tratamento de dados pelo responsável em tela, qual seja o empregador.

## 5 CONSIDERAÇÕES FINAIS

A proteção de dados é uma questão crítica à luz do desenvolvimento de inovações tecnológicas que facilitam nosso trabalho e interações pessoais. Assim, a LGPD aparece como um marco regulatório destinado a estabelecer normas para garantir a autodeterminação informacional dos indivíduos, bem como a integridade do tratamento dos dados para assegurar a privacidade dos indivíduos.

Nesse sentido, a responsabilidade civil não é apenas um mecanismo de reparação de danos, mas também uma ferramenta importante para o incentivo de boas práticas por parte dos agentes de tratamento de dados. O conhecimento dessas diferenças é extremamente relevante, pois orienta as práticas que os atores jurídicos e organizações devem adotar, especialmente ao considerar legislações muito específicas como o Código de Defesa do Consumidor.

Uma área de grande relevância é o gerenciamento de dados de funcionários pelo empregador. O argumento para a adoção de práticas que honrem os direitos dos trabalhadores deve ser congruente com uma cultura organizacional de prevenção e proteção, incluindo transparência e consentimento informado. Além disso, diferentes problemas surgem na fase pós-contratual que necessitam de um esforço particular, à medida que controlar e gerenciar dados mostra o cruzamento entre direitos trabalhistas e proteção da privacidade.

No final, esse debate não apenas destaca a importância de seguir rigorosamente a LGPD, mas também cria um senso de urgência em torno do fato de que as organizações precisam estar em constante evolução e adaptação em resposta aos riscos trazidos pela tecnologia. Com base nesses fundamentos, a responsabilidade civil não deve ser entendida como uma imposição normativa, mas sim como uma oportunidade de transformação e melhoria das relações de confiança entre empresas e a sociedade em geral, como os empregados. Todas as partes devem trabalhar em prol de um diálogo aberto e cooperativo que busque não meramente estar dentro dos limites da lei, mas fomentar um espaço social digital mais seguro e respeitoso.

# REFERÊNCIAS

ACIOLY, Luis Henrique de Menezes; SILVA, Matheus Fernandes da; MONTEIRO NETO, João Araújo. A Emenda Constitucional nº 115 de 10 de fevereiro de 2022 e o *enforcement* da proteção de dados pessoais no Brasil. **Revista de Investigações Constitucionais**, [S.L.], v. 11, n. 3, p. 1-28, 30 out. 2024. Universidade Federal do Paraná. http://dx.doi.org/10.5380/rinc.v11i3.92117. Disponível em: https://revistas.ufpr.br/rinc/article/view/92117/73925. Acesso em: 15 jan. 2

ALCÂNTARA, Clayton Deodoro Gonçalves de. **Impactos da Lei Geral de Proteção de Dados nas relações de trabalho**. 2021. 28 f. TCC (Graduação) - Curso de Direito, Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1472. Acesso em: 09 fev. 2025.

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital**. Perspectivas em Ciência da Informação**, [S.L.], v. 27, n. 3, p. 26-45, set. 2022. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/1981-5344/25905. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/?lang=pt. Acesso em: 07 fev. 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, v. 9, n. 3, p. 1–23, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662. Acesso em: 4 fev. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 fev. 2025.

BUIM JUNIOR, Wladir Muzati. **A Lei Geral de Proteção de Dados considerados como fundamentais e os impactos nas relações de trabalho: boas práticas como vetor de mitigação de riscos impostos pela lei**. 2020. 110 f. Dissertação (Mestrado) - Curso de Direito, Fundação de Ensino "Eurípides Soares da Rocha" – Feesr, Marília, 2020. Disponível em: https://aberto.univem.edu.br/bitstream/handle/11077/1964. Acesso em: 09 fev. 2025.

CALDAS, Roberto Correia da Silva Gomes; SOARES, Paulo Vinicius de Carvalho; MARTINS, José Alberto Monteiro. Análises preliminares sobre a responsabilidade civil na Lei Geral de Proteção de Dados Pessoais – arts. 42 a 45 da Lei Federal nº. 13.709, de 14 de agosto de 2018. **Administração de Empresas em Revista**, Curitiba, v. 2, n. 28/2022, p. 414-461, 2022. Disponível em: https://revista.unicuritiba.edu.br/index.php/admrevista/article/view/6040. Acesso em: 14 jan. 2025.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos:** direito digital e proteção de dados pessoais, São Paulo, ano 21, v. 53, p. 163-170, mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilida

de_civil.pdf. Acesso em: 14 jan. 2025.

CAVALIERI FILHO, Sergio. Responsabilidade Civil no Novo Código Civil. **Revista da Emerj**, Rio de Janeiro, v. 6, n. 24, p. 31-47, mar. 2003. Disponível em: https://core.ac.uk/download/pdf/18336057.pdf. Acesso em: 08 mar. 2025.

CUNHA, Luana Carolina Bonavina da; NASCIMENTO, Vitória Rodrigues do.; DIAS, Andreza Silva. CTPS DIGITAL: os desafios da implantação em empresas privadas na região de São Carlos-SP. **Revista Interface Tecnológica**, Taquaritinga, SP, v. 20, n. 1, p. 288–299, 2023. DOI: 10.31510/infa.v20i1.1611. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/1611. Acesso em: 9 fev. 2025.

D'OLIVEIRA, Nadine Passos Conceição; CUNHA, Francisco José Aragão Pedroza. Lei Geral de Proteção de Dados (LGPD): a relação entre as políticas e os regimes de informação. **Rdbci: Revista Digital de Biblioteconomia e Ciência da Informação**, [S.L.], v. 22, p. 1-21, 18 jun. 2024. Universidade Estadual de Campinas. http://dx.doi.org/10.20396/rdbci.v22i00.8675749. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/8675749/34085. Acesso em: 15 jan. 2025.

DE TEFFÉ, Chiara Spadaccini; DE MORAES, Maria Celina Bodin. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet**. Pensar-Revista de Ciências Jurídicas**, v. 22, n. 1, p. 108-146, 2017.

FERNANDES, Ana Lívia Silva; PEREIRA, Letícia Fernandes; PEDROSA, Jussara de Melo. **Responsabilidade civil por vazamento de dados pessoais: uma análise sob a luz da LGPD**. 2024. 17 f. TCC (Graduação) - Curso de Direito, Universidade de Uberaba, Uberaba, 2024. Disponível em: https://dspace.uniube.br:8443/bitstream/123456789/2711/1/TCC%20Ana%20L%c3%advia%20e%20Let%c3%adcia%20Fernandes.pdf. Acesso em: 14 jan. 2025.

FERREIRA, Vanessa Rocha; FALCÃO, Beatriz Normando; BIZZOCCHI, Lucas Jorge João. Sociedade digital, privacidade e proteção de dados: uma análise dos impactos da lgpd no direito do trabalho. **Conjecturas**, [S.L.], v. 22, n. 2, p. 219-241, 24 fev. 2022. Uniao Atlantica de Pesquisadores. http://dx.doi.org/10.53660/conj-645-614. Disponível em: https://scholar.google.com/scholar?hl=pt-BR&as_sdt=0%2C5&q=Digital%2C+Privacidade+e+Prote%C3%A7%C3%A3o+de+Dados%3A+uma+an%C3%A1lise+dos+impactos+da++LGPD+no+Direito+do+Trabalho&btnG=. Acesso em: 14 fev. 2025.

FIDELIS, Isabela Cristine. **Abusividade contratual na era digital: aspectos jurídicos e reflexos da LGPD**. 2023. 63 f. TCC (Graduação) - Curso de Direito, Universidade de Santa Cruz do Sul – Unisc, Capão da Canoa, 2023. Disponível em: https://repositorio.unisc.br/jspui/handle/11624/3670. Acesso em: 09 fev. 2025.

GOMES, Matheus Machado. **Impactos da "LGPD" nos processos seletivos de emprego**. 2022. 30 f. TCC (Graduação) - Curso de Direito, Universidade Presbiteriana Mackenzie, São Paulo, 2022. Disponível em: https://dspace.mackenzie.br/items/1b6d7123-0c3e-4599-8bc5-0cf7630f6c95. Acesso em: 09 fev. 2025.

GOULART, Bruno Brigido. **Aplicação da tecnologia blockchain no armazenamento de**

**documentos**. 2021. 17 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense, Criciúma, 2021. Disponível em: http://repositorio.unesc.net/handle/1/9140. Acesso em: 22 fev. 2025

LEAL JUNIOR, Wilmar Borges; CORDEIRO, Suzane Aparecida; LEAL, Alexis Vinícius de Aquino. Proteção dos dados pessoais: impactos da Nova Lei Geral de Proteção de Dados no Instituto Federal do Tocantins. **Revista Sítio Novo**, Palmas, v. 6, n. 4, p. 16-30, dez. 2022. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/94887289/1158_5061_1_PB-libre.pdf?1669515621=&response-content-disposition=inline%3B+filename%3DProtecao_dos_dados_pessoais_impactos_da.pdf&Expires=1738973472&Signature=f6--eRnWtV-bvQrmSrK9Dc5IBjDZsKzjbJzopZO2nlXPTAZlKZMQ9KLHmnIt2tVVpG9KUixx0xfHq62QQwYe~FKm6tewOwH0AeDh8d50x9NcKFRoYgAntW3VCCEijnMIWx09jVZVV3JFelhYG-J2b9A7bzIXunlUc4tjTRASZ7ftf159WTBGTV5WB5qH~z-D2Eq0Krk9vkdoyJQv1d5lJ-El3pu9b1atLBW-S1YRb2gKiqs6B3ISD0p3VxhijruLw33H~aefn60hhwh97dY9kcDwJeyGMC3kKq6GshxPs1NfAAILzrdT4hKJH44cup59N7eaJfc-cvaWYlp7Q3oIbA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em: 07 fev. 2025.

LIMA, Victtor Henrique Pereira. **LGPD análise dos impactos da implementação em ambientes corporativos: estudo de caso**. 2020. 43 f. Tese (Doutorado) - Curso de Ciência da Computação, Pontifícia Universidade Católica de Goiás, Goiânia, 2020. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/108/1/LGPD%20-%20ANALISE%20DOS%20IMPACTOS%20DA%20IMPLEMENTAC%CC%A7A%CC%83O%20-%2003-12%20-%20final.pdf. Acesso em: 07 fev. 2025.

LOPEZ, Teresa Ancona. Responsabilidade civil na sociedade de risco. **Revista da Faculdade de Direito, Universidade de São Paulo**, v. 105, p. 1223-1234, 2010.

MACHADO, Luciana Cristina Pinto; MARCONI, Licia Pimentel. Estudos preliminares sobre os princípios aplicados ao tratamento de dados pessoais na Lei nº 13.709/2018 - LGPD. **Anais Enepe 2020**, Presidente Prudente, v. 25, n. 1, p. 2603-2613, out. 2020. Disponível em: https://www.unoeste.br/Areas/Eventos/Content/documentos/EventosAnais/564/anais/Sociai %20Aplicadas/Direito.pdf#page=190. Acesso em: 07 fev. 2025.

MACIEL, Roberta Araújo de Carvalho. Considerações sobre a Lei Geral de Proteção de Dados Pessoais – LGPD, sua aplicação ao poder público e o compartilhamento de dados pessoais pelos órgãos públicos. **Revista Judicial Brasileira**, [S.L.], v. 3, p. 257-284, 27 nov. 2023. Escola Nacional de Formação e Aperfeiçoamento de Magistrados. http://dx.doi.org/10.54795/rejubesp.dirdig.226. Disponível em: https://revistadaenfam.emnuvens.com.br/renfam/article/view/226/76. Acesso em: 14 jan. 2025.

MATOS, Liliane Gonçalves; MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Limites à implantação de chips subcutâneos: a tutela da privacidade como instrumento de proteção da pessoa na sociedade da informação. **Revista de Direitos e Garantias Fundamentais,** v. 18, n. 3, p. 267-300, 2017.

NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe dal Farra. Responsabilidade civil na LGPD: problemas e soluções. **Conpedi Law Review,** [S.L.], v. 6, n. 1, p. 158-174, 24 dez. 2020. Conselho Nacional de Pesquisa e Pos-Graduacao em Direito - CONPEDI.

http://dx.doi.org/10.26668/2448-3931_conpedilawreview/2020.v6i1.7024. Disponível em: https://core.ac.uk/download/382457955.pdf. Acesso em: 04 fev. 2025.

OTTONI, Mara Ruth Ferraz; FARIAS, Paulo José Leite. Lei Geral de Proteção de Dados, as relações de trabalho à luz do desenvolvimento sustentável. **Revista de Direito - Trabalho, Sociedade e Cidadania**, [S.L.], v. 12, n. 12, p. 60-76, 13 dez. 2023. Centro Universitário Instituto de Educação Superior de Brasília. http://dx.doi.org/10.61541/c9mkg257. Disponível em: https://revista.iesb.br/revista/index.php/ojsiesb/article/view/106. Acesso em: 07 fev. 2025.

PAMPLONA FILHO, Rodolfo; CONI JUNIOR, Vicente Vasconcelos. A Lei Geral de Proteção de Dados Pessoais e seus impactos no direito do trabalho. **Revista Direito Unifacs** - Qualis A2 Classificada Pela Capes, [S.L], n. 249, p. 1-42, mar. 2021. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/7108. Acesso em: 09 fev. 2025.

PAULA, Sabrina Cordeiro de. **A proteção de dados na Era Digital: uma revisão narrativa das legislações da União Europeia, Estados Unidos e Brasil**. 2024. 75 f. TCC (Graduação) - Curso de Relações Internacionais, Universidade Federal de Santa Maria, Santa Maria, 2024. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/32890/Paula_Sabrina_Cordeiro_de_2024_TCC pdf?sequence=1&isAllowed=y. Acesso em: 15 jan. 2025.

PINTO, Danielle Jacon Ayres; MOTA, Rafael Gonçalves. A guerra cibernética como a quinta dimensão da guerra moderna e o seu enfrentamento constitucional no Brasil. in: xxix Congresso Nacional do Conpedi Balneário Camboriú - sc, 29., 2022, Balneário Camboriú. **Internet: dinâmicas da segurança pública e internacional.** Balneário Camboriú: Conpedi, 2022. p. 210-226. disponível em: https://site.conpedi.org.br/publicacoes/906terzx/n61yy6o8/cz807686ijh307tu.pdf. acesso em: 28 fev. 2025.

PIRES, Mariana Silva. **Proletariado digital e regulação jurídica: parâmetros normativos para a (re)significação da relação de trabalho Uberizada no brasil**. 2023. 128 f. Dissertação (Mestrado) - Curso de Direito, Universidade Federal da Paraíba, João Pessoa, 2023. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/31804. Acesso em: 13 fev. 2025.

REYMÃO, Ana Elizabeth Neirão; OLIVEIRA, Lis Arrais; KOURY, Suzy Elizabeth Cavalcante. A ANPD e a fiscalização da governança corporativa de proteção de dados. **Revista do Direito Público**, [S.L.], v. 18, n. 2, p. 30-47, 3 set. 2023. Universidade Estadual de Londrina. http://dx.doi.org/10.5433/1980-511x.2023v18n2p30. Disponível em: https://ojs.uel.br/revistas/uel/index.php/direitopub/article/view/46105. Acesso em: 07 fev. 2025.

RUBINI, Luana Zagonel; GEHELEN, Maristela Heinen. Contrato eletrônico. **Academia de Direito**, [S.L.], v. 5, p. 27-45, 24 mar. 2023. Universidade do Contestado - UnC. http://dx.doi.org/10.24302/acaddir.v5.3372. Disponível em: https://www.periodicos.unc.br/index.php/acaddir/article/view/3372. Acesso em: 22 fev. 2025.

SANDEN, Ana Francisca Moreira de Souza. **A proteção de dados pessoais do empregado no direito brasileiro**. 2012. 264 f. Tese (Doutorado) - Curso de Faculdade de Direito, Departamento de Direito do Trabalho e de Seguridade Social, Universidade de São Paulo, São Paulo, 264. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2138/tde-05082013-

165006/publico/TESE_AnaFranciscaMoreiradeSouzaSANDEN.pdf. Acesso em: 07 fev. 2025.

SANTOS, Rômulo Marcel Souto dos; LEITÃO, André Studart; WOLKART, Erik Navarro. A responsabilidade civil na Lei Geral de Proteção de Dados Pessoais e a Regra de Hand. **Revista Opinião Jurídica (Fortaleza)**, [S.L.], ano 20, n. 34, p. 60-84, 17 mar. 2022. Instituto para o Desenvolvimento da Educação. http://dx.doi.org/10.12662/2447-6641oj.v20i34.p60-84.2022. Disponível em: https://periodicos.unichristus.edu.br/opiniaojuridica/article/download/4179/1556/16187. Acesso em: 14 jan. 2025.

SANTOS, Camila Ferrão dos; SILVA, Jeniffer Gomes da; PADRÃO, Vinícius. Responsabilidade civil pelo tratamento de dados pessoais na Lei Geral de Proteção de Dados. **Revista Eletrônica da Pge-Rj**, [S.L.], v. 4, n. 3, 30 dez. 2021. Centro de Estudos Jurídicos da Procuradoria Geral do Estado do Rio de Janeiro. http://dx.doi.org/10.46818/pge.v4i3.256. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/256. Acesso em: 14 jan. 2025.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020. Disponível em: https://repositorio.pucrs.br/dspace/bitstream/10923/18868/2/O_Direito_Fundamental_Proteo de_Dados_Pessoais_na_Constituio_Federal_Brasileira_de_1988.pdf. Acesso em: 15 jan. 2025.

SILVA, Faysa de Maria Oliveira e; SIEBRA, Sandra de Albuquerque; SANTOS, Thais Helen do Nascimento. Preservação digital na Arquivologia. **Revista Brasileira de Preservação Digital**, [S.L.], v. 4, p. 1-30, 10 jun. 2023. Universidade Estadual de Campinas. http://dx.doi.org/10.20396/rebpred.v4i00.17937. Disponível em: https://econtents.bc.unicamp.br/inpec/index.php/rebpred/article/view/17937. Acesso em: 22 fev. 2025.

SILVA, Pedro Felipy Cunha da; ARAÚJO, Wagner Junqueira de. Registros digitais arquivísticos do SIPAC Protocolo. **Revista Brasileira de Preservação Digital**, [S.L.], v. 5, n. 024001, p. 1-26, 4 mar. 2024. Universidade Estadual de Campinas. http://dx.doi.org/10.20396/rebpred.v5i00.17908. Disponível em: https://econtents.bc.unicamp.br/inpec/index.php/rebpred/article/view/17908. Acesso em: 22 fev. 2025.

SOUSA, Francisco Luziaro de. **Transformação Digital no Contexo da Inteligência de Estado: Análise e Mitigação das Vulnerabilidades do Documento Digital**. 2022. 50 f. Tese (Doutorado) - Curso de Engenharia Elétrica, Universidade de Brasília, Brasília, 2022. Disponível em: http://repositorio.unb.br/handle/10482/46230. Acesso em: 22 fev. 2025.

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos: Direito Digital e Proteção de Dados Pessoais**, São Paulo, ano 21, v. 53, p. 97-115, mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_1_interface_entre_

_lgpd.pdf?d=637250344175953621. Acesso em: 14 jan. 2025.

YAEGASHI, João Gabriel; OTERO, Cleber Sanfelici. A responsabilidade do empregador pela proteção de dados no meio ambiente de trabalho: consequências jurídicas. **Revista Meritum**, Belo Horizonte, v. 17, n. 3, p. 284-299, 2022. DOI: https://doi.org/10.46560/ meritum, v17i3.8807. Disponível em: https://revista.fumec.br/index.php/meritum/article/view/8807. Acesso em: 09 fev. 2025.