LUMEN ET VIRTUS
ISSN: 2177-2789

TELETRABALHO E LGPD: DESAFIOS E BOAS PRÁTICAS NA PROTEÇÃO DE DADOS PESSOAIS

TELEWORKING AND LGPD: CHALLENGES AND GOOD PRACTICES IN THE PROTECTION OF PERSONAL DATA

TELETRABAJO Y LGPD: RETOS Y BUENAS PRÁCTICAS EN LA PROTECCIÓN DE DATOS PERSONALES

https://doi.org/10.56238/levv16n53-104

Data de submissão: 22/09/2025 **Data de publicação:** 22/10/2025

Demetrio Messias Costa
Graduando em Direito
Instituição: Faculdade Cesumar de Ponta Grossa
E-mail: demetriomessiascosta@gmail.com

João Paulo Vieira Deschk
Mestre em Direito Empresarial e Cidadania
Instituição: UNICURITIBA
E-mail: jp.deschk@gmail.com

RESUMO

Este trabalho teve como objetivo analisar os impactos da Lei Geral de Proteção de Dados (LGPD) nas relações de trabalho, com ênfase nas responsabilidades dos empregadores e empregados no tratamento de dados pessoais, especialmente diante do contexto do teletrabalho e do uso de dispositivos pessoais (BYOD). A metodologia adotada foi a pesquisa bibliográfica, fundamentada em autores contemporâneos e textos legais, com abordagem qualitativa e caráter exploratório, permitindo uma compreensão aprofundada dos aspectos jurídicos, técnicos e organizacionais envolvidos na proteção de dados no ambiente laboral. Os resultados demonstraram que o avanço das tecnologias da informação, aliado à expansão do teletrabalho, aumentou significativamente os riscos à segurança dos dados pessoais no ambiente doméstico. Observou-se que a ausência de políticas claras de segurança, o uso de redes públicas e o manuseio de informações sensíveis em dispositivos pessoais fragilizam o cumprimento das normas da LGPD. Além disso, evidenciou-se que tanto empregadores quanto empregados compartilham responsabilidades legais, sendo fundamental o desenvolvimento de estratégias conjuntas para assegurar a conformidade e prevenir violações. O estudo ainda destacou a importância do uso de ferramentas como VPNs, criptografia e autenticação multifator como medidas essenciais de proteção, mas que devem ser acompanhadas de treinamento, monitoramento e políticas institucionais adequadas. Concluiu-se que a proteção de dados no ambiente de trabalho depende não apenas da tecnologia, mas da adoção de uma cultura organizacional voltada à segurança da informação e à ética no tratamento de dados pessoais.

Palavras-chave: Cibersegurança. Compliance. Privacidade.

ABSTRACT

The aim of this work was to analyze the impacts of the General Data Protection Law (GDPR) on employment relationships, with an emphasis on the responsibilities of employers and employees in the

processing of personal data, especially in the context of teleworking and the use of personal devices (BYOD). The methodology adopted was bibliographical research, based on contemporary authors and legal texts, with a qualitative approach and exploratory nature, allowing an in-depth understanding of the legal, technical and organizational aspects involved in data protection in the workplace. The results showed that the advance of information technology, combined with the expansion of teleworking, has significantly increased the risks to the security of personal data in the domestic environment. It was observed that the absence of clear security policies, the use of public networks and the handling of sensitive information on personal devices weaken compliance with LGPD rules. It also showed that both employers and employees share legal responsibilities, and that it is essential to develop joint strategies to ensure compliance and prevent breaches. The study also highlighted the importance of using tools such as VPNs, encryption and multi-factor authentication as essential protection measures, but which must be accompanied by training, monitoring and appropriate institutional policies. It was concluded that data protection in the workplace depends not only on technology, but on the adoption of an organizational culture focused on information security and ethics in the handling of personal data.

Keywords: Cybersecurity. Compliance. Privacy.

RESUMEN

El objetivo de este trabajo fue analizar los impactos de la Ley General de Protección de Datos (RGPD) en las relaciones laborales, con énfasis en las responsabilidades de empleadores y empleados en el procesamiento de datos personales, especialmente en el contexto del teletrabajo y el uso de dispositivos personales (BYOD). La metodología adoptada fue una investigación bibliográfica, basada en autores contemporáneos y textos legales, con un enfoque cualitativo y de naturaleza exploratoria, que permitió una comprensión profunda de los aspectos legales, técnicos y organizativos involucrados en la protección de datos en el entorno laboral. Los resultados mostraron que el avance de las tecnologías de la información, combinado con la expansión del teletrabajo, ha incrementado significativamente los riesgos para la seguridad de los datos personales en el entorno doméstico. Se observó que la ausencia de políticas de seguridad claras, el uso de redes públicas y el manejo de información sensible en dispositivos personales debilitan el cumplimiento de las normas de la LGPD. También mostró que tanto empleadores como empleados comparten responsabilidades legales, y que es esencial desarrollar estrategias conjuntas para garantizar el cumplimiento y prevenir infracciones. El estudio también destacó la importancia de utilizar herramientas como las VPN, el cifrado y la autenticación multifactor como medidas esenciales de protección, que deben ir acompañadas de capacitación, supervisión y políticas institucionales adecuadas. Se concluyó que la protección de datos en el entorno laboral depende no solo de la tecnología, sino también de la adopción de una cultura organizacional centrada en la seguridad de la información y la ética en el manejo de datos personales.

Palabras clave: Ciberseguridad. Cumplimiento. Privacidad.

1 INTRODUÇÃO

A crescente digitalização das relações laborais e a intensificação do uso de tecnologias no ambiente corporativo, sobretudo após a consolidação do teletrabalho, tornaram o tratamento de dados pessoais um tema central nas dinâmicas entre empregadores e empregados. Nesse contexto, a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) inaugurou um novo paradigma normativo no Brasil, demandando não apenas adequações técnicas, mas também transformações na cultura organizacional quanto à privacidade e à segurança da informação. A realidade do trabalho remoto, o uso de dispositivos pessoais (BYOD), os riscos no ambiente doméstico e a responsabilidade compartilhada no tratamento de dados são elementos que evidenciam a complexidade desse cenário, exigindo análise crítica e aprofundada (Nogueira, 2024; Medeiros, 2022).

A justificativa para o desenvolvimento deste estudo reside na necessidade de compreender os múltiplos desafios impostos pela LGPD às relações de trabalho contemporâneas, especialmente no que se refere à proteção de dados no contexto do teletrabalho e do uso de tecnologias móveis. A descentralização do ambiente laboral, aliada ao uso intensivo de dispositivos conectados à internet, aumentou significativamente os riscos de violação de dados sensíveis, exigindo que empregadores adotem ferramentas como VPNs, sistemas de criptografia e autenticação multifatorial para garantir a integridade das informações (Nogueira, 2024; Medeiros, 2022).

Dessa forma, o objetivo geral deste trabalho é analisar os impactos da Lei Geral de Proteção de Dados nas relações de trabalho, com ênfase nas obrigações dos agentes de tratamento, nos riscos à proteção de dados no ambiente doméstico, na política de BYOD (Bring Your Own Device) e nas medidas tecnológicas de segurança. Os objetivos específicos incluem: discutir os direitos dos titulares de dados e os deveres dos controladores e operadores; examinar as responsabilidades do empregador e do empregado no tratamento de dados; identificar os riscos de vazamentos no contexto do trabalho remoto.

Para alcançar esses objetivos, será adotada uma metodologia de caráter qualitativo, com enfoque na revisão bibliográfica de autores contemporâneos e especialistas na área jurídica e tecnológica. As obras consultadas abrangem publicações acadêmicas, artigos científicos e capítulos de livros que tratam especificamente da LGPD e seus desdobramentos nas relações de trabalho e na segurança da informação.

2 DESENVOLVIMENTO

2.1 FUNDAMENTOS DO TELETRABALHO

O teletrabalho, também conhecido como trabalho remoto ou home office, é uma modalidade laboral caracterizada pela realização das atividades profissionais fora das dependências físicas da empresa, com apoio de tecnologias da informação e da comunicação. Embora frequentemente

associado à contemporaneidade, suas raízes remontam a mudanças progressivas na organização do trabalho ao longo da história. Fontana (2021) destaca que a evolução do trabalho esteve diretamente ligada aos avanços tecnológicos e às transformações sociais, sendo o teletrabalho uma resposta às novas demandas de flexibilidade, mobilidade e conectividade no mundo corporativo moderno.

A adoção do teletrabalho foi impulsionada inicialmente por fatores como a globalização, a digitalização dos processos e a busca por redução de custos operacionais. No entanto, conforme apontam Figueiredo et al. (2021), foi com a pandemia de COVID-19 que essa modalidade se consolidou como alternativa viável e urgente para garantir a continuidade das atividades econômicas e preservar a saúde dos trabalhadores. A emergência sanitária forçou empresas e instituições públicas a migrar rapidamente para o trabalho remoto, muitas vezes sem o preparo técnico ou estratégico necessário, o que evidenciou tanto suas potencialidades quanto suas fragilidades.

De acordo com Santos e Costa (2022), o chamado "novo normal" trouxe à tona não apenas o potencial do teletrabalho como modelo produtivo, mas também desafios relacionados ao equilíbrio entre vida profissional e pessoal, à saúde mental dos trabalhadores e às condições técnicas de trabalho domiciliar. A transformação abrupta, embora necessária, gerou um cenário de adaptação intensa e contínua, exigindo reconfigurações na cultura organizacional e nas práticas de gestão de pessoas.

Padilha e Bittencourt (2020) ressaltam que o teletrabalho, já contemplado na legislação brasileira com a reforma trabalhista de 2017, ganhou nova relevância após a pandemia, revelando a urgência de regulamentações mais específicas e de políticas internas que assegurem a produtividade e os direitos dos trabalhadores remotos. Complementando essa análise, Ferreira et al. (2021) identificam, por meio de pesquisa empírica, uma aceitação crescente do modelo home office por parte dos empregados, que valorizam a autonomia, a economia de tempo e a possibilidade de conciliação entre as esferas pessoal e profissional.

O teletrabalho, embora consolidado como uma alternativa viável à rotina tradicional de trabalho presencial, apresenta um conjunto de vantagens que o tornaram atrativo tanto para empregadores quanto para empregados. Dentre os principais benefícios, destaca-se a flexibilidade de horários, que permite ao trabalhador maior autonomia na gestão do tempo e da jornada laboral. Segundo Oliveira e Matheus (2022), essa autonomia contribui para o aumento da produtividade e da satisfação profissional, sobretudo quando acompanhada por metas bem definidas e autonomia para tomada de decisões. Além disso, a eliminação do tempo gasto com deslocamentos diários reduz o estresse e gera economia financeira para o colaborador.

Outro aspecto relevante refere-se à economia gerada pelas organizações. Com a redução da necessidade de estruturas físicas e consumo de recursos como energia elétrica, transporte e alimentação corporativa, empresas têm observado um significativo corte de custos operacionais. Filardi, Castro e Zanini (2020) observaram que, no caso da administração pública, experiências como as do Serpro e da

Receita Federal demonstraram que o teletrabalho pode representar ganhos em eficiência e otimização de recursos. Do ponto de vista institucional, há ainda ganhos relacionados à sustentabilidade e à imagem organizacional, que se fortalece diante de práticas modernas e alinhadas às novas dinâmicas de trabalho.

O teletrabalho também impõe desvantagens significativas, principalmente no que tange à saúde mental e ao bem-estar dos trabalhadores. A ausência de interação social, o isolamento prolongado e a dificuldade em delimitar os espaços entre o ambiente doméstico e profissional são elementos que afetam diretamente a qualidade de vida do trabalhador remoto. Vebber e Borges (2021) enfatizam que o teletrabalho pode intensificar sintomas de ansiedade, estresse e exaustão emocional, especialmente quando não há suporte psicológico ou estratégias organizacionais que promovam o equilíbrio entre trabalho e vida pessoal. O esgotamento digital e a sobrecarga de tarefas também são frequentemente relatados em estudos sobre a modalidade.

Além das questões psicossociais, o teletrabalho pode acentuar desigualdades estruturais, uma vez que nem todos os trabalhadores possuem acesso a condições adequadas para exercer suas funções remotamente. Conforme salientam Oliveira e Matheus (2022), problemas como a ausência de equipamentos, instabilidade de conexão à internet e espaços inadequados para o trabalho interferem diretamente na produtividade e no desempenho das atividades. Ademais, as dificuldades de monitoramento e avaliação por parte das chefias, aliadas à insegurança jurídica em torno da jornada de trabalho e do controle de resultados, representam desafios para a consolidação plena do teletrabalho como prática institucional estável e equitativa.

2.2 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 2018 por meio da Lei nº 13.709, representa um marco regulatório no ordenamento jurídico brasileiro quanto à proteção de dados pessoais, sendo fruto de um contexto internacional que exigia maior controle e segurança sobre as informações individuais. Inspirada principalmente no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD nasceu da necessidade de regulamentar o tratamento de dados no Brasil frente ao crescente uso de tecnologias digitais, redes sociais, serviços online e bancos de dados interconectados. Segundo Fernandes e Nuzzi (2022), a promulgação da LGPD preencheu uma lacuna jurídica existente e trouxe uma abordagem mais sistêmica e transparente sobre como os dados devem ser coletados, armazenados e utilizados por organizações públicas e privadas.

Os fundamentos da LGPD estão ancorados em princípios como a autodeterminação informativa, a proteção à privacidade e à intimidade, à inviolabilidade da honra e da imagem e a defesa dos direitos fundamentais dos cidadãos. De acordo com Joelsons (2022), esses princípios buscam garantir que o titular dos dados tenha conhecimento e controle sobre o uso de suas informações,

configurando uma mudança significativa no paradigma da proteção da privacidade. A autora enfatiza ainda que o "legítimo interesse", um dos fundamentos legais para o tratamento de dados, deve ser interpretado com cautela, de modo a não sobrepor os direitos fundamentais do titular.

Outro ponto importante é o contexto socioeconômico que impulsionou a criação da LGPD. A crescente digitalização dos processos empresariais e administrativos evidenciou a fragilidade das estruturas existentes para garantir a segurança das informações. Conforme Cruz, Passaroto e Junior (2021), a ausência de normas claras provocava insegurança jurídica tanto para os titulares de dados quanto para as instituições que os manipulavam. O setor contábil, por exemplo, sentiu fortemente essa mudança, tendo que rever práticas rotineiras de arquivamento, gestão de cadastros e comunicação com clientes, adequando-se a padrões mais rigorosos de compliance e segurança da informação.

Além dos aspectos normativos, a LGPD introduz um regime de responsabilidade civil específico em casos de vazamentos de dados ou de tratamento irregular de informações. Oliveira e Novais (2024) destacam que a responsabilização das organizações, inclusive com previsão de sanções administrativas e multas, fortalece a proteção do consumidor e amplia o alcance dos direitos individuais. A obrigatoriedade da implementação de medidas técnicas e administrativas, como políticas de segurança da informação, treinamentos e nomeação de encarregados pelo tratamento de dados (DPO), reforça a necessidade de uma cultura organizacional voltada à proteção da privacidade. Com isso, a LGPD se consolida como um instrumento jurídico imprescindível à governança digital e à consolidação de uma sociedade mais ética, transparente e centrada nos direitos do cidadão.

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, estabelece um conjunto de princípios fundamentais que orientam o tratamento de dados pessoais no Brasil. Tais princípios constituem o alicerce da normativa e asseguram a conformidade ética e jurídica no uso de informações pessoais, tanto no setor público quanto privado. Segundo Teffé e Viola (2020), os princípios da finalidade, necessidade, adequação, livre acesso, transparência, segurança, prevenção, não discriminação e responsabilização visam garantir que os dados sejam utilizados com respeito à dignidade, liberdade e privacidade do indivíduo.

No contexto das bases legais para o tratamento de dados, a LGPD prevê dez hipóteses autorizativas, sendo necessário que ao menos uma delas esteja presente para legitimar qualquer operação de coleta, armazenamento ou uso de dados pessoais. Entre essas bases estão o consentimento do titular, o cumprimento de obrigação legal, a execução de políticas públicas, a realização de estudos por órgão de pesquisa, e o legítimo interesse do controlador, entre outras. Xavier (2021) ressalta que a base do legítimo interesse, embora mais flexível, exige critérios objetivos e ponderação entre os interesses do controlador e os direitos do titular, sendo imprescindível a realização de uma avaliação de impacto à proteção de dados (DPIA).

Quando se trata do setor público, o tratamento de dados deve atender, prioritariamente, às bases legais relacionadas à execução de políticas públicas ou à obrigação legal e regulatória. De acordo com Botelho e Camargo (2021), a atuação do Estado está limitada pela finalidade pública do dado e pela necessidade de respeito aos direitos fundamentais. Ainda que o poder público não dependa de consentimento para grande parte de seus tratamentos, a LGPD exige que sejam observados os princípios da transparência e da minimização de dados. O uso indevido de informações por entes estatais pode configurar desvio de finalidade e gerar responsabilizações institucionais e administrativas, reafirmando o papel da norma como garantidora dos direitos dos cidadãos diante do poder de tratamento estatal.

A transparência e o fortalecimento do Estado Democrático de Direito são elementos centrais da LGPD, especialmente no que diz respeito à governança pública. Como apontam Blum e López (2020), a lei contribui para consolidar uma administração pública mais responsável, ética e participativa, na medida em que impõe deveres de clareza e acesso à informação sobre o uso de dados pelos órgãos públicos. Ao estabelecer que todo tratamento de dados deve ser informado e acessível ao titular, inclusive com possibilidade de revisão de decisões automatizadas, a LGPD se apresenta não apenas como uma norma técnica, mas como um instrumento de cidadania e controle democrático.

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece um conjunto de direitos fundamentais aos titulares de dados, conferindo-lhes maior controle sobre o uso de suas informações pessoais. Esses direitos incluem, entre outros, o acesso, a correção, a exclusão, a portabilidade dos dados, bem como a possibilidade de revogar o consentimento e de se opor ao tratamento de dados realizados com base em interesses legítimos. Conforme expõem Teffé e Viola (2020), esses direitos asseguram a autodeterminação informativa dos indivíduos, fortalecendo sua posição diante de empresas e instituições que processam dados, e reafirmam o compromisso da norma com a proteção da dignidade humana em um contexto de crescente digitalização.

Paralelamente aos direitos dos titulares, a LGPD impõe obrigações rigorosas aos agentes de tratamento, que são divididos entre o controlador e o operador. O controlador é responsável pelas decisões referentes ao tratamento de dados pessoais, enquanto o operador atua segundo as instruções do controlador, sem decidir autonomamente sobre o uso das informações. Kremer (2020) ressalta que ambos os agentes devem adotar medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados, perdas e vazamentos. Além disso, devem manter registros das operações realizadas e, em determinadas hipóteses, nomear um encarregado (DPO) para garantir a conformidade com a legislação e atuar como canal de comunicação entre o titular e a autoridade nacional.

A responsabilidade civil dos agentes de tratamento é um aspecto central da LGPD, sendo pautada pelo regime de responsabilidade objetiva para os controladores em casos de danos causados por falhas no tratamento. Como aponta Capanema (2020), a lei busca não apenas compensar o dano

sofrido pelo titular, mas também criar um mecanismo de prevenção e desestímulo a práticas negligentes por parte dos responsáveis. O operador, por sua vez, poderá ser responsabilizado de forma solidária caso descumpra as instruções do controlador ou atue com dolo ou culpa. Dessa maneira, a LGPD consolida um sistema de responsabilização que combina deveres de segurança, transparência e boa-fé, essencial para a proteção eficaz dos dados pessoais no Brasil.

2.3 APLICAÇÃO DA LGPD NO CONTEXTO DO TELETRABALHO

O teletrabalho consolidou-se como uma modalidade relevante no cenário contemporâneo, sobretudo após a pandemia da COVID-19, trazendo novos desafios ao ordenamento jurídico brasileiro. A Consolidação das Leis do Trabalho (CLT), em seus artigos 75-A a 75-E, já regulamenta o tema, mas a inserção da Lei Geral de Proteção de Dados (LGPD) trouxe novos contornos às relações laborais. A necessidade de compatibilizar o direito fundamental à privacidade do empregado com os deveres do empregador de organizar, fiscalizar e assegurar a segurança da informação ampliou o debate jurídico sobre o tema. O teletrabalho exige a construção de um equilíbrio entre proteção de dados pessoais e gestão eficiente da atividade laboral (Reis; Fernandes, 2023).

No campo do direito do trabalho, a pandemia acelerou a adoção do teletrabalho, revelando lacunas normativas quanto à proteção de dados pessoais. Silva et al. (2024) destacam que a intensificação do trabalho remoto ampliou a coleta de informações sobre o desempenho dos empregados, tornando necessário discutir os limites legais do monitoramento e da supervisão digital. Assim, a LGPD atua como instrumento essencial para delimitar até que ponto o empregador pode utilizar dados pessoais de seus colaboradores, reforçando a importância do princípio da finalidade e da proporcionalidade.

Outro aspecto relevante é o papel do compliance nas organizações, que passa a ser uma exigência no contexto do teletrabalho. De acordo com Soares (2022, p. 87), a ética empresarial deve incluir diretrizes claras sobre proteção de dados e práticas de monitoramento, a fim de evitar violações da privacidade e condutas abusivas. Esse alinhamento entre ética, direito e tecnologia fortalece a segurança jurídica das empresas e cria um ambiente laboral mais justo e equilibrado.

A responsabilidade civil do empregador é um ponto crítico quando se trata da proteção de dados no teletrabalho. Vazamentos de informações, quando decorrentes de falhas organizacionais, podem gerar não apenas sanções administrativas, mas também indenizações por danos morais e materiais. Reis e Fernandes (2023) salientam que a falta de medidas preventivas adequadas configura descumprimento dos deveres de segurança previstos na LGPD, o que reforça a importância da adoção de tecnologias e protocolos capazes de mitigar riscos jurídicos.

A expansão do teletrabalho, impulsionada principalmente pela pandemia da COVID-19, trouxe novos desafios à proteção de dados pessoais, especialmente no ambiente doméstico. A migração do

espaço corporativo para o lar diluiu as fronteiras entre os sistemas institucionais controlados e os dispositivos pessoais, muitas vezes desprovidos de infraestrutura adequada de segurança da informação. Segundo Moreira e Thaines (2023), essa realidade aumenta significativamente a exposição de dados sensíveis e confidenciais a riscos, como acessos indevidos, vazamentos, e ataques cibernéticos, uma vez que a maioria dos trabalhadores não possui treinamento específico nem ferramentas de proteção eficazes.

O ambiente doméstico, por sua natureza informal e privada, carece de mecanismos técnicos e organizacionais padronizados que garantam o cumprimento das diretrizes da LGPD. A ausência de redes criptografadas, a utilização de computadores compartilhados com familiares e a falta de controle de acessos são apenas alguns dos fatores que elevam a vulnerabilidade dos dados processados no teletrabalho. Mulholland (2020) aponta que essa precariedade de medidas preventivas pode configurar omissão culposa dos empregadores, que seguem responsáveis pelos dados mesmo quando o tratamento ocorre fora do ambiente empresarial. Assim, a responsabilização civil por eventuais danos deve considerar não apenas a existência do dano, mas também a ausência de cautelas proporcionais ao risco envolvido.

Moreira e Thaines (2023) observam que a aplicação da LGPD às relações de trabalho exige revisão contratual, adoção de políticas internas de proteção de dados e treinamentos contínuos. No entanto, tais medidas ainda são incipientes em muitas organizações, especialmente de pequeno e médio porte, que não dispõem de setores especializados em compliance digital. A negligência nesse cenário pode não apenas comprometer os dados dos clientes, mas também expor informações sensíveis dos próprios colaboradores, como dados médicos, bancários e familiares.

Dessa forma, a proteção de dados no contexto do teletrabalho demanda uma reconfiguração das práticas empresariais, aliando tecnologia, cultura organizacional e responsabilidade jurídica. Conforme destaca Mulholland (2020), é essencial que o empregador atue proativamente na prevenção de riscos, promovendo medidas compatíveis com a natureza dos dados tratados, sob pena de incorrer em responsabilidade civil objetiva. Além disso, a sensibilização do trabalhador quanto à importância da proteção de dados é crucial para a efetividade das normas. A LGPD, ao se aplicar plenamente ao ambiente doméstico no que tange ao teletrabalho, impõe um novo paradigma de proteção e vigilância, reafirmando a centralidade da dignidade da pessoa humana na era digital.

O uso de dispositivos pessoais no ambiente de trabalho, prática conhecida como *Bring Your Own Device* (BYOD), tem se tornado cada vez mais comum, especialmente com o avanço do trabalho remoto e da mobilidade corporativa. Essa tendência possibilita que os colaboradores utilizem seus próprios smartphones, laptops ou tablets para desempenhar atividades profissionais, promovendo economia de recursos e maior comodidade ao trabalhador. Contudo, conforme analisam Coto e Dias (2023), essa prática, embora vantajosa sob certas perspectivas, impõe desafios significativos às

organizações, sobretudo no que tange à segurança da informação e ao cumprimento da Lei Geral de Proteção de Dados (LGPD).

Do ponto de vista da proteção de dados pessoais e corporativos, o BYOD apresenta uma série de vulnerabilidades. O uso de dispositivos não gerenciados pela organização dificulta o controle e a rastreabilidade do tratamento de dados, favorecendo incidentes como acessos não autorizados, vazamentos e perda de informações sensíveis. Segundo Silva (2023), a integração entre mobilidade e segurança da informação exige políticas robustas de autenticação, criptografia e segmentação de redes, as quais muitas vezes são negligenciadas pelos usuários em dispositivos pessoais. Assim, o BYOD pode comprometer seriamente o cumprimento dos princípios da LGPD, como o da segurança, da prevenção e da responsabilização.

A questão se torna ainda mais complexa no contexto das relações laborais, pois envolve o equilíbrio entre a autonomia do trabalhador e a responsabilidade do empregador quanto ao tratamento dos dados. Gauriau (2021) destaca que, ao permitir o uso de dispositivos pessoais para fins profissionais, o empregador continua responsável pela proteção dos dados tratados, mesmo quando o processamento ocorre fora do ambiente corporativo. Esse entendimento, inspirado na jurisprudência europeia e nos princípios do RGPD, reforça a necessidade de cláusulas contratuais claras, treinamentos periódicos e implementação de medidas técnicas adequadas.

A responsabilidade pelo tratamento de dados pessoais no ambiente de trabalho é compartilhada entre empregador e empregado, exigindo o cumprimento rigoroso das diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD). O empregador, na condição de agente de tratamento, assume papel central no controle, proteção e uso adequado dos dados pessoais dos trabalhadores, sendo responsável por garantir a segurança da informação em todas as fases do vínculo contratual. Conforme destacam Yaegashi e Otero (2022), o empregador responde juridicamente por danos decorrentes do uso indevido ou do vazamento de dados, sendo-lhe imputável a obrigação de estabelecer políticas internas, realizar treinamentos e adotar medidas técnicas e administrativas adequadas.

De acordo com Tereza e Águila (2023), a empresa deve justificar a coleta desses dados com base em uma das hipóteses legais previstas na LGPD, como o cumprimento de obrigação legal ou regulatória. Caso ocorra um vazamento e fique caracterizada a negligência na adoção de mecanismos de proteção, a organização poderá ser responsabilizada por danos morais e materiais, devendo reparar os prejuízos sofridos pelo empregado. O risco jurídico é ainda maior diante da ausência de consentimento ou do uso de dados para finalidades distintas daquelas inicialmente previstas.

O empregado também possui deveres relacionados à proteção de dados no ambiente laboral. Ele deve agir de acordo com as normas internas da empresa, respeitando os princípios de confidencialidade, lealdade e finalidade, evitando o compartilhamento indevido de informações a que tenha acesso em razão do cargo. Conforme argumenta Coutinho (2020), o trabalhador tem o dever de

colaborar com a cultura de proteção de dados instituída pela empresa, especialmente quando atua em setores sensíveis, como recursos humanos ou tecnologia da informação. O descumprimento dessas obrigações pode ensejar sanções disciplinares, inclusive a demissão por justa causa, desde que haja previsão contratual ou regulamentar expressa.

2.4 O MONITORAMENTO DIGITAL DO EMPREGADO E OS LIMITES LEGAIS À PRIVACIDADE

O avanço das tecnologias de informação e comunicação transformou radicalmente as formas de controle empresarial, tornando o monitoramento digital dos empregados uma prática recorrente, especialmente após a consolidação do teletrabalho. Ferramentas capazes de registrar atividades em tempo real, como softwares de rastreamento, controle de produtividade e análise de desempenho, passaram a integrar a rotina das empresas que buscam otimizar processos e reduzir falhas operacionais. No entanto, essa realidade suscita preocupações jurídicas relacionadas à proteção da intimidade e à preservação da dignidade do trabalhador, direitos consagrados constitucionalmente no art. 5º, inciso X, da Constituição Federal. De acordo com Estêvão, Lima e Silva (2022), a utilização dessas ferramentas deve observar os princípios da finalidade, necessidade e proporcionalidade, assegurando que a coleta e o tratamento de dados não ultrapassem os limites éticos e legais estabelecidos pela Lei nº 13.709/2018. Assim, torna-se imprescindível a construção de uma política organizacional pautada pela transparência e pela boa-fé objetiva.

Além disso, a ampliação do trabalho remoto intensificou o debate sobre o alcance do poder diretivo do empregador diante do direito fundamental à privacidade do empregado. O controle digital do desempenho, embora legítimo, não pode converter-se em vigilância abusiva, capaz de gerar constrangimento ou invasão do ambiente pessoal do trabalhador. Conforme ressaltam Reis e Fernandes (2023), o teletrabalho impôs a necessidade de redefinir as fronteiras entre o espaço laboral e o espaço doméstico, uma vez que o ambiente virtual tende a confundir o tempo de trabalho com o tempo de descanso. Assim, a fiscalização constante e a ausência de limites temporais podem configurar violação à desconexão profissional, princípio cada vez mais reconhecido no direito comparado. Por isso, recomenda-se que os mecanismos de monitoramento sejam utilizados de modo equilibrado e comunicados previamente aos empregados, em consonância com as normas de proteção de dados e com o dever de informação previsto no art. 9º da LGPD.

> "Todavia, não se pode ignorar o fato de que o teletrabalho pode representar um risco à segurança dos dados pessoais, principalmente pela ausência de um preparo eficiente sobre a coleta, transferência e armazenamento dessas informações, visto que uma considerável parcela de empregados não possui as ferramentas e sistemas de proteção em seus equipamentos pessoais. A título de exemplo, é possível identificar alguns dados que merecem especial cuidado, como a própria documentação pessoal de identificação dos trabalhadores, as correspondências eletrônicas, as mensagens trocadas em aplicativos de comunicação, a captura

> de imagens dos trabalhadores, o registro de chamadas, o registro biométrico da jornada de trabalho, entre outros." (Estêvão, Lima e Silva, 2022, p.70)

A problemática do monitoramento digital exige uma reflexão sobre o princípio da dignidade da pessoa humana, que se sobrepõe a qualquer interesse econômico ou corporativo. A vigilância eletrônica, quando realizada de maneira indiscriminada, pode produzir impactos psicológicos relevantes, como ansiedade e sentimento de desconfiança, afetando diretamente o ambiente laboral. De acordo com Vebber e Borges (2021), o controle exacerbado e a sensação de constante observação geram riscos à saúde mental dos trabalhadores, especialmente em regimes de home office. Portanto, o desafio contemporâneo está em conciliar a eficiência produtiva com a integridade psicológica do empregado, evitando práticas que configurem assédio moral digital ou violação de direitos da personalidade. Essa ponderação encontra respaldo nos princípios da proporcionalidade e da razoabilidade, que orientam a interpretação constitucional e a aplicação da LGPD nas relações trabalhistas.

Sob a ótica da responsabilidade civil, eventuais abusos no uso de tecnologias de monitoramento podem ensejar reparação de danos morais, materiais e existenciais. Capanema (2020) explica que a Lei Geral de Proteção de Dados impõe ao empregador a obrigação de adotar medidas técnicas e administrativas adequadas à proteção das informações, sendo a omissão equiparada à culpa. Assim, a coleta e o armazenamento indevidos de dados pessoais ou sensíveis — como geolocalização, gravação de áudio e vídeo ou análise de comunicações — configuram violação direta à privacidade e à intimidade. É imprescindível, portanto, que as empresas implementem políticas de governança de dados e nomeiem encarregados responsáveis pela conformidade legal, a fim de mitigar riscos jurídicos e assegurar o tratamento ético das informações trabalhistas.

Do ponto de vista ético e organizacional, o monitoramento digital demanda uma cultura corporativa voltada à confiança e à corresponsabilidade. Souza e Tomei (2024) afirmam que a mera adoção de tecnologias não é suficiente para garantir a conformidade legal, sendo necessário o engajamento de todos os níveis hierárquicos na internalização de valores como respeito, transparência e integridade. Some-se a isso a importância da educação digital, que deve abranger não apenas o uso responsável de dados, mas também a conscientização dos trabalhadores sobre seus próprios direitos informacionais. O equilíbrio entre controle e autonomia, portanto, depende do reconhecimento da privacidade como um ativo organizacional que agrega valor à imagem institucional e reforça o compromisso com o bem-estar do colaborador.

Em outra perspectiva, a utilização de sistemas de monitoramento implica desafios técnicos significativos quanto à segurança da informação. Neves et al. (2021) observam que as empresas devem adotar medidas de segurança cibernética, como autenticação multifatorial, criptografia e auditorias periódicas, a fim de evitar o acesso não autorizado e o vazamento de dados. No ambiente do

teletrabalho, em que redes domésticas são frequentemente utilizadas para fins profissionais, os riscos se ampliam consideravelmente. Por isso, políticas claras de compliance e uso de VPNs tornam-se ferramentas essenciais para o cumprimento da LGPD e para a preservação da integridade dos sistemas corporativos. Assim, a responsabilidade pela proteção das informações deve ser compartilhada entre empregador e empregado, numa relação de confiança mútua que priorize a prevenção em detrimento da punição.

No contexto jurídico comparado, Gauriau (2021) ressalta que a legislação europeia, especialmente o Regulamento Geral de Proteção de Dados (RGPD), já reconhece limites expressos ao monitoramento laboral, condicionando-o ao consentimento e à proporcionalidade das medidas adotadas. O Brasil, ao inspirar-se nesse modelo, avança no sentido de consolidar um ordenamento jurídico capaz de compatibilizar a liberdade empresarial com os direitos fundamentais do trabalhador. Entretanto, persistem lacunas interpretativas, sobretudo no que se refere à fiscalização em ambientes híbridos e à delimitação das responsabilidades quando o tratamento de dados ocorre fora das dependências físicas da empresa. Nesses casos, a atuação do poder judiciário torna-se crucial para uniformizar entendimentos e assegurar a efetividade das garantias constitucionais de privacidade e proteção de dados pessoais.

Ainda que o monitoramento digital tenha o propósito de assegurar produtividade e prevenir fraudes, ele deve ser implementado de maneira transparente e previsível. Segundo Botelho e Camargo (2021), a transparência é condição indispensável à legitimidade do tratamento de dados, devendo o trabalhador ser informado sobre quais informações são coletadas, por que são coletadas e como serão utilizadas. O descumprimento desse dever de informação caracteriza violação direta à autodeterminação informativa, princípio central da LGPD. Ademais, a comunicação clara e objetiva fortalece a relação de confiança entre as partes, reduzindo litígios e promovendo uma cultura de governança digital responsável. Assim, o diálogo institucional torna-se o instrumento mais eficaz para harmonizar os interesses econômicos e os direitos individuais no ambiente corporativo digitalizado.

Do ponto de vista da governança e do compliance, Campos e Carreiro (2024) destacam que a gestão de riscos no ambiente digital deve ser proativa e adaptativa, acompanhando a velocidade das inovações tecnológicas. Isso implica revisar continuamente as políticas internas de monitoramento, de modo a garantir que estejam alinhadas às diretrizes legais e às boas práticas internacionais de proteção de dados. Ademais, o papel dos gestores é essencial para garantir que o controle de desempenho não se transforme em instrumento de coerção ou violação da intimidade. A ética corporativa, portanto, deve funcionar como o eixo orientador da implementação de tecnologias de vigilância, reforçando o compromisso da empresa com a proteção da dignidade humana e com a valorização do trabalho digno e seguro.

Em última análise, é importante reconhecer que a efetividade das normas de proteção de dados depende tanto da regulação estatal quanto da autorregulação empresarial. Blum e López (2020) afirmam que a transparência e a participação são pilares do Estado Democrático de Direito e devem se refletir nas práticas corporativas de coleta e uso de informações. Dessa forma, o monitoramento digital precisa ser compreendido não como um privilégio do empregador, mas como uma prerrogativa condicionada aos direitos fundamentais do empregado. Assim, conclui-se que o equilíbrio entre produtividade, segurança e privacidade é o caminho mais adequado para promover um ambiente laboral ético, eficiente e em conformidade com os valores constitucionais e com a Lei Geral de Proteção de Dados Pessoais.

Por fim, o monitoramento digital deve ser entendido como um fenômeno multidimensional que envolve aspectos jurídicos, técnicos, sociais e psicológicos. Amaral e Moreira (2024) argumentam que o fortalecimento da cultura de proteção de dados é uma necessidade inadiável para que o trabalho remoto e híbrido se desenvolvam de maneira sustentável. Portanto, é dever das organizações investir em políticas educativas, capacitação contínua e auditorias internas que assegurem a conformidade com a legislação vigente. De igual modo, cabe ao Estado, por meio de seus órgãos fiscalizadores, garantir que os direitos dos trabalhadores sejam efetivamente respeitados. Em síntese, a tecnologia deve ser utilizada como instrumento de progresso e não de vigilância opressiva, consolidando uma nova ética digital pautada no respeito à privacidade e na valorização do ser humano como sujeito de direitos e não como objeto de controle.

2.5 O PAPEL DO DPO (DATA PROTECTION OFFICER) NAS RELAÇÕES DE TRABALHO

O encarregado pelo tratamento de dados, conhecido internacionalmente como *Data Protection Officer* (DPO), constitui uma das figuras centrais para a efetividade da Lei Geral de Proteção de Dados Pessoais, atuando como elo estratégico entre os titulares das informações, as organizações e a Autoridade Nacional de Proteção de Dados. Sua função transcende o simples cumprimento de exigências legais, alcançando o campo da ética, da governança corporativa e da transparência institucional. Segundo Kremer (2020), o DPO deve assegurar que os processos de coleta, armazenamento e uso de dados pessoais ocorram em conformidade com os princípios da lei, desempenhando um papel de mediação e de orientação contínua dentro da estrutura organizacional. Assim, torna-se agente indispensável para a construção de um ambiente de trabalho compatível com as exigências da privacidade e da proteção informacional.

> "O controlador possui o dever de indicar o encarregado (semelhante ao Data Protection Officer – DPO – instituído no GDPR europeu) pelo tratamento de dados (Art. 41). Trata-se de pessoa natural indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD (Art. 5º, VIII). Ele age dentro de uma organização pública ou privada para garantir a conformidade com a LGPD ou para processar dados pessoais em nome da entidade. Quando indicado pelo controlador, suas atividades consistem em: (i) receber

> comunicações da ANPD; (ii) aceitar reclamações e comunicações dos titulares e lhes prestar esclarecimentos; (iii) orientar os colaboradores sobre observações das melhores práticas nas operações de processamento nos moldes na LGPD; (iv) executar outras atribuições determinadas pelo controlador (Art. 41, §2º).” (Kremer, 2020, p.8)

Além de promover o cumprimento técnico da legislação, o encarregado exerce uma função educativa ao fomentar a conscientização sobre a importância da proteção de dados entre gestores e colaboradores. Na visão de Souza e Tomei (2024), a efetividade das políticas de privacidade não depende apenas de normas escritas, mas do engajamento coletivo em torno de valores éticos compartilhados, o que exige uma liderança orientada para o exemplo e a coerência. Em outras palavras, a presença do DPO contribui para a formação de uma cultura organizacional em que o respeito aos direitos dos titulares de dados se torna parte integrante da identidade institucional. Esse aspecto pedagógico do encarregado é essencial para consolidar práticas duradouras de governança digital e para evitar que o cumprimento da LGPD se reduza à mera formalidade burocrática.

A complexidade crescente das relações laborais, impulsionada pela digitalização e pelo teletrabalho, amplia significativamente o campo de atuação do DPO. De acordo com Amaral e Moreira (2024), a descentralização do ambiente de trabalho e o uso de dispositivos pessoais para o desempenho de atividades profissionais exigem novas estratégias de controle e orientação. Nesse cenário, o DPO deve desenvolver protocolos de segurança adaptados à realidade do trabalho remoto, assegurando que a proteção de dados seja observada mesmo fora das instalações físicas da empresa. Essa postura proativa contribui para mitigar riscos jurídicos, técnicos e reputacionais, reforçando o papel do encarregado como guardião da conformidade e da confiança organizacional.

No contexto das relações de emprego, cabe ao DPO acompanhar de perto todas as etapas que envolvem o tratamento de informações de trabalhadores, desde o recrutamento até a rescisão contratual. Segundo Tereza e Águila (2023), dados sensíveis, como informações médicas, antecedentes criminais e dados bancários, exigem tratamento diferenciado, sob pena de violação da intimidade e da honra do empregado. Portanto, o encarregado deve atuar preventivamente na elaboração de relatórios de impacto à proteção de dados, conforme o artigo 38 da LGPD, e garantir que os princípios da finalidade e da minimização sejam observados em cada fase do vínculo trabalhista. Dessa forma, o DPO assume uma função de controle interno e de assessoramento jurídico-tecnológico, assegurando que as ações empresariais estejam em sintonia com o ordenamento vigente.

Outro aspecto relevante refere-se à necessidade de integração entre o encarregado e as demais áreas da organização. Para Campos e Carreiro (2024), a atuação eficaz do DPO depende de uma abordagem interdisciplinar que envolva os setores jurídico, tecnológico, de recursos humanos e de segurança da informação. Essa interação garante uma resposta mais ágil e coesa diante de incidentes de violação de dados, além de fortalecer a governança interna. O DPO, portanto, não deve ser visto como figura isolada, mas como parte de uma engrenagem organizacional que precisa operar de modo

sincronizado. Ao atuar em conjunto com o setor de compliance, o encarregado contribui para a criação de um sistema de integridade digital que antecipa riscos e fortalece a credibilidade institucional.

Ademais, o papel do DPO está diretamente vinculado à consolidação do compliance corporativo como instrumento de responsabilidade social e jurídica. Falangola e Ramalho (2025) afirmam que o encarregado é o principal responsável por integrar a proteção de dados aos programas de conformidade, de modo que a privacidade deixe de ser um tema restrito à área tecnológica e se transforme em valor transversal. A atuação do DPO, nesse sentido, deve garantir que a proteção informacional seja considerada em todas as decisões estratégicas da empresa, inclusive na definição de políticas de recursos humanos e nas práticas de monitoramento digital. Em síntese, o encarregado atua como o guardião da ética informacional, conciliando eficiência administrativa e respeito aos direitos fundamentais do trabalhador.

A relevância do DPO também se manifesta na gestão de incidentes de segurança, uma vez que o profissional é responsável por comunicar eventuais vazamentos à autoridade competente e aos titulares afetados. De acordo com Nogueira (2024), a adoção de protocolos de resposta rápida, aliada à criptografia e à autenticação multifatorial, constitui prática indispensável para conter danos e restaurar a confiança após um incidente. O encarregado, nesse contexto, exerce uma função de gerenciamento de crises, coordenando equipes técnicas e jurídicas para reduzir impactos operacionais e reputacionais. Assim, o papel do DPO vai além da prevenção: ele representa a linha de defesa que assegura a continuidade das operações e a transparência institucional diante de falhas inevitáveis em ambientes digitais complexos.

É importante ressaltar que o DPO também cumpre papel relevante na interface com a Autoridade Nacional de Proteção de Dados. Grotti (2021) observa que a atuação do encarregado é fundamental para viabilizar a comunicação entre a empresa e o órgão fiscalizador, garantindo que as orientações emitidas pela autoridade sejam compreendidas e aplicadas adequadamente. Essa interlocução contribui para uma relação de cooperação, em que o foco recai sobre a melhoria contínua das práticas de tratamento de dados, e não apenas sobre a punição. Dessa forma, o DPO funciona como mediador institucional, capaz de traduzir as exigências legais em políticas internas eficazes e adaptadas à realidade de cada organização.

Do ponto de vista jurídico, o DPO não se limita a funções administrativas, pois exerce também uma responsabilidade indireta na prevenção de litígios trabalhistas. Oliveira e Novais (2024) enfatizam que a omissão na nomeação de um encarregado ou a inexistência de políticas claras de proteção de dados podem caracterizar negligência patronal, sujeitando a empresa a sanções civis e administrativas. Assim, o DPO atua como instrumento de redução de passivos, assegurando a rastreabilidade e a legitimidade das operações de tratamento. A sua presença formaliza a boa-fé e a diligência da

organização perante a lei, fortalecendo a segurança jurídica e consolidando a imagem de responsabilidade institucional.

Por fim, é necessário compreender que a figura do DPO simboliza uma nova era na gestão corporativa, em que a proteção de dados pessoais se insere como componente essencial da governança e da sustentabilidade empresarial. Segundo Buogo, Fachinelli e Giacomello (2019), o conhecimento deve ser tratado como ativo estratégico, e sua gestão requer mecanismos de segurança e controle. O encarregado, ao zelar pelo uso responsável da informação, assegura não apenas a conformidade legal, mas também o desenvolvimento ético das organizações em um ambiente cada vez mais orientado pela tecnologia. Conclui-se, assim, que o DPO representa um agente de transformação institucional, capaz de articular o cumprimento normativo com a promoção de valores de cidadania digital, confiança e respeito à dignidade humana no contexto das relações de trabalho.

2.6 O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E A FISCALIZAÇÃO DO CUMPRIMENTO DA LGPD

A criação da Autoridade Nacional de Proteção de Dados (ANPD) representou um marco institucional fundamental para a efetividade da Lei Geral de Proteção de Dados Pessoais no Brasil. Seu papel vai muito além da simples fiscalização, abrangendo também a regulamentação, a orientação e a promoção de uma cultura de proteção de dados em todo o território nacional. De acordo com Grotti (2021), a ANPD atua como órgão técnico e regulador responsável por supervisionar a aplicação da legislação, aplicando sanções administrativas e promovendo a conscientização sobre o uso ético das informações. Assim, o surgimento da autoridade materializa o compromisso do Estado brasileiro com a transparência, a segurança digital e a defesa da privacidade enquanto direito fundamental.

> "É o caso do artigo 4º, III, Lei Geral de Proteção de Dados, que estabelece que a Lei 'não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais', para logo em seguida, em seu parágrafo terceiro, afirmar que a Autoridade Nacional emitirá opiniões técnicas ou recomendações sobre essas exceções e poderá solicitar relatório de impacto à proteção de dados pessoais (artigo 4º, §3º, Lei Geral de Proteção de Dados)" (Blum e López, 2020, p.173)

A atuação da ANPD é pautada por um equilíbrio entre a função pedagógica e a função coercitiva, devendo conciliar a educação corporativa com o poder sancionador. Segundo Damião e Novais (2024), a autoridade tem competência para instaurar processos administrativos, expedir relatórios técnicos e aplicar penalidades que podem alcançar até 2% do faturamento da empresa, limitadas a cinquenta milhões de reais por infração. Essas sanções possuem caráter educativo e preventivo, buscando estimular as organizações a adotarem mecanismos de governança e compliance

digital. Em outras palavras, a função fiscalizadora da ANPD deve ser compreendida como instrumento de aprimoramento institucional e não apenas como medida punitiva.

Além da função sancionatória, a ANPD desempenha papel essencial na construção de diretrizes e recomendações voltadas à proteção de dados nas relações de trabalho. Para Botelho e Camargo (2021), o órgão tem a responsabilidade de harmonizar o exercício do poder diretivo do empregador com os direitos de privacidade e de autodeterminação informativa do empregado. Ao emitir orientações sobre temas sensíveis, como o monitoramento digital, o armazenamento de dados biométricos e o uso de dispositivos pessoais, a autoridade contribui para uniformizar práticas e reduzir incertezas jurídicas. Dessa forma, a atuação regulatória da ANPD garante maior segurança e previsibilidade às empresas, ao mesmo tempo em que fortalece a proteção do trabalhador no ambiente digital.

A autoridade também exerce papel relevante no estímulo à cultura de segurança da informação e na capacitação das organizações quanto às boas práticas de tratamento de dados. De acordo com Cavalieri (2020), a ANPD atua como indutora de políticas públicas voltadas à integridade governamental e à transparência administrativa, promovendo uma mudança estrutural na forma como o Estado e o setor privado lidam com informações pessoais. Essa dimensão educativa é indispensável, pois consolida a ideia de que a proteção de dados deve ser tratada como um valor público, essencial à consolidação da cidadania digital e à confiança entre usuários e instituições. Assim, a ANPD funciona como catalisadora da ética informacional e da cultura de responsabilidade compartilhada.

No contexto do setor público, a atuação da autoridade assume importância ainda maior, visto que os órgãos governamentais lidam com grandes volumes de informações sensíveis. Segundo Blum e López (2020), a ANPD contribui para o fortalecimento do Estado Democrático de Direito ao exigir que o poder público adote práticas transparentes e respeite os direitos fundamentais dos cidadãos. A implementação de políticas de governança de dados no âmbito estatal, impulsionada pela atuação da autoridade, assegura maior controle social e accountability das ações governamentais. Em outras palavras, a ANPD atua como guardiã da legalidade e da moralidade administrativa na era digital.

A fiscalização exercida pela ANPD também é relevante para o fortalecimento da confiança entre empresas e consumidores. Amaral e Moreira (2024) afirmam que a existência de uma autoridade autônoma e técnica é fundamental para legitimar o tratamento de dados pessoais e para garantir que os titulares tenham seus direitos efetivamente protegidos. Ao atuar como mediadora de conflitos e como instância de apelação, a ANPD assegura equilíbrio entre os interesses econômicos e os direitos individuais, reforçando o princípio da proporcionalidade que permeia a Lei Geral de Proteção de Dados. Assim, o órgão contribui para a estabilidade jurídica e para o desenvolvimento sustentável da economia digital.

Outro aspecto essencial da atuação da ANPD está relacionado à sua capacidade de estabelecer cooperação internacional com outras entidades reguladoras. Segundo Fernandes e Nuzzi (2022), a

globalização dos fluxos de informação impõe a necessidade de alinhamento entre as normas brasileiras e os padrões internacionais de privacidade, como o Regulamento Geral de Proteção de Dados da União Europeia. Nesse sentido, a ANPD desempenha papel diplomático e técnico, promovendo o intercâmbio de informações, a harmonização de práticas e o fortalecimento da reputação do Brasil no cenário global de governança digital. Dessa forma, o órgão atua não apenas como fiscalizador interno, mas também como representante do país no diálogo internacional sobre privacidade e segurança informacional.

A responsabilidade da ANPD não se limita à aplicação de penalidades, mas se estende à orientação preventiva e ao incentivo à autorregulação. Segundo Campos e Carreiro (2024), a autoridade tem incentivado o desenvolvimento de programas de compliance digital e de mecanismos de certificação que atestam a conformidade das empresas com a LGPD. Essa estratégia estimula uma cultura de autorresponsabilidade e de amadurecimento institucional, reduzindo a necessidade de intervenção estatal direta. Ao promover a governança colaborativa, a ANPD reforça a corresponsabilidade entre poder público, setor privado e sociedade civil na proteção dos dados pessoais.

A atuação da autoridade também repercute diretamente nas relações trabalhistas, especialmente no tocante à proteção de dados de empregados e candidatos a vagas. Na visão de Reis e Fernandes (2023), a ANPD contribui para estabelecer parâmetros que impedem o uso discriminatório de informações pessoais, como histórico de saúde ou dados sensíveis, durante processos seletivos e avaliações de desempenho. Essas orientações funcionam como salvaguardas jurídicas contra práticas abusivas, garantindo a observância dos princípios da igualdade, da não discriminação e da boa-fé objetiva. Assim, a autoridade desempenha papel essencial na promoção da justiça social e da equidade nas relações de trabalho mediadas pela tecnologia.

Por fim, é importante compreender que o sucesso da ANPD depende de sua capacidade de dialogar com a sociedade e de manter sua independência institucional. Segundo Falangola e Ramalho (2025), a credibilidade da autoridade está diretamente vinculada à sua imparcialidade e à transparência de suas decisões, fatores indispensáveis para o fortalecimento da governança digital no país. Dessa forma, conclui-se que a ANPD não é apenas um órgão fiscalizador, mas uma instituição de Estado voltada à promoção da ética, da segurança e da confiança nas relações informacionais. Em síntese, sua atuação representa um avanço civilizatório na consolidação dos direitos fundamentais à privacidade e à proteção de dados pessoais, pilares indispensáveis de uma sociedade democrática e digitalmente sustentável.

3 APRESENTAÇÃO DOS DADOS (RESULTADOS)

3.1 BOAS PRÁTICAS PARA A PROTEÇÃO DE DADOS NO TELETRABALHO

As políticas internas de segurança da informação desempenham um papel essencial na proteção dos ativos digitais das organizações, especialmente diante da crescente exposição a riscos decorrentes de falhas humanas, ataques cibernéticos e vazamentos de dados. Tais políticas consistem em um conjunto de diretrizes, procedimentos e normas estabelecidos com o objetivo de garantir a confidencialidade, integridade e disponibilidade das informações. Segundo Neves et al. (2021), a conformidade com a Lei Geral de Proteção de Dados (LGPD) exige que as empresas implementem medidas técnicas e organizacionais robustas, dentre as quais as políticas internas ocupam posição central, sendo indispensáveis para a prevenção de incidentes e o atendimento aos princípios da proteção de dados.

É importante compreender que a efetividade dessas políticas depende diretamente da conscientização dos usuários, considerados o elo mais vulnerável do sistema. De acordo com Souza (2022), mesmo sistemas tecnologicamente avançados podem ser comprometidos por comportamentos negligentes, como o uso de senhas fracas, o compartilhamento indevido de credenciais ou a abertura de arquivos suspeitos. Nesse contexto, a educação continuada dos colaboradores torna-se fundamental para a construção de uma cultura organizacional voltada à segurança da informação. A realização de treinamentos, campanhas educativas e testes periódicos de vulnerabilidade são estratégias recomendadas para mitigar os riscos associados à ação humana.

Outro fator crítico na formulação de políticas internas é a proteção contra ataques de engenharia social, técnica que explora fragilidades comportamentais para obter acesso não autorizado a sistemas e dados sensíveis. Como apontam Pereira, Vicentine e Rizo (2022), esses ataques muitas vezes não dependem de brechas tecnológicas, mas sim da capacidade do atacante em manipular emocionalmente o usuário, fazendo com que este revele informações confidenciais. Assim, as políticas internas devem conter orientações claras sobre como identificar e reagir a situações suspeitas, como e-mails de phishing, ligações fraudulentas e solicitações de acesso não justificadas, fortalecendo a resiliência institucional.

A crescente digitalização dos processos organizacionais e a expansão do trabalho remoto intensificaram a necessidade de adoção de ferramentas e tecnologias voltadas à proteção de dados pessoais e corporativos. Nesse cenário, instrumentos como redes privadas virtuais (VPN), sistemas de criptografia e mecanismos de autenticação representam pilares fundamentais da segurança da informação. Conforme destaca Nogueira (2024), essas tecnologias atuam como barreiras técnicas para impedir acessos não autorizados, vazamentos e interceptações de dados, proporcionando maior controle sobre o tráfego e o armazenamento de informações sensíveis em redes corporativas e domésticas.

As VPNs (Virtual Private Networks) são ferramentas que criam túneis criptografados entre o dispositivo do usuário e a rede corporativa, garantindo a confidencialidade dos dados transmitidos mesmo em conexões públicas ou não seguras. De acordo com Medeiros (2022), a utilização de VPNs no Brasil se apresenta como uma medida legítima e recomendável para proteger informações em trânsito, especialmente diante das exigências legais impostas pela Lei Geral de Proteção de Dados (LGPD). Além de proteger contra interceptações externas, a VPN possibilita o mascaramento de endereços IP, dificultando a rastreabilidade e garantindo um nível adicional de anonimato e segurança.

Outra tecnologia indispensável no tratamento seguro de dados é a criptografia, que transforma informações legíveis em códigos ininteligíveis para usuários não autorizados. Nogueira (2024) ressalta que a criptografia deve ser aplicada tanto na transmissão quanto no armazenamento dos dados, de modo a prevenir que, mesmo em caso de invasão ou perda de dispositivos, as informações permaneçam inacessíveis. Existem diferentes métodos criptográficos e sua escolha depende do nível de segurança requerido, da sensibilidade dos dados e do desempenho esperado pelos sistemas de informação utilizados.

A governança de dados e o compliance digital configuram-se como elementos centrais na estruturação das organizações em um contexto cada vez mais orientado pela informação e pela transformação digital. A necessidade de estabelecer regras claras de gestão e proteção de dados tornou-se imprescindível após a vigência da Lei Geral de Proteção de Dados (LGPD), que impôs parâmetros normativos a todos os setores. Nesse sentido, a governança de dados surge como um mecanismo de controle e monitoramento, garantindo não apenas a conformidade legal, mas também a integridade organizacional (Cavalieri, 2020).

No âmbito da administração pública, a governança de dados assume uma relevância particular, uma vez que a gestão eficiente da informação é condição essencial para a prestação de serviços de qualidade e para a construção de uma cultura de transparência. Segundo Cavalieri (2020), a LGPD contribui diretamente para a integridade governamental, pois exige a implementação de mecanismos de proteção da privacidade que antes eram negligenciados. Dessa forma, a governança passa a ser compreendida como parte de um programa de integridade mais amplo, capaz de mitigar riscos de corrupção e de violações de direitos fundamentais.

Para Jesus, Brito e Reis (2022), a efetivação de programas de compliance digital vai além da simples observância da legislação, constituindo-se em uma prática de gestão positiva voltada à construção de confiança institucional. Ou seja, quando a organização internaliza a conformidade digital, ela fortalece sua imagem diante da sociedade e cria uma cultura interna que valoriza a proteção de dados como um ativo essencial.

A adoção de programas de compliance digital exige um olhar para os desafios impostos pela inovação tecnológica e pela disrupção dos modelos tradicionais de gestão. Campos e Carreiro (2024)

destacam que, em tempos de inovação acelerada, a conformidade precisa ser dinâmica, acompanhando as mudanças tecnológicas e jurídicas, isso significa que as organizações devem estabelecer mecanismos de monitoramento contínuo, utilizando práticas de gestão de riscos que possam antecipar problemas relacionados à segurança da informação e à privacidade dos titulares.

No setor privado, a governança de dados se conecta diretamente à competitividade das empresas, uma vez que a conformidade com a LGPD passa a ser diferencial no mercado. Conforme apontam Falangola e Ramalho (2025), o compliance em proteção de dados tornou-se parte do modelo de negócio, pois a não observância da lei pode acarretar multas, danos reputacionais e perda de confiança. Assim, o compliance digital não deve ser encarado como mero custo, mas como investimento estratégico, capaz de garantir a sustentabilidade e a credibilidade da instituição no longo prazo.

A segurança da informação tem se consolidado como um componente essencial para a sustentabilidade organizacional, especialmente em contextos marcados pela digitalização intensa e pelo teletrabalho, sua efetividade depende não apenas da implementação de tecnologias de proteção de dados, mas também da incorporação de práticas e procedimentos que permeiem toda a estrutura da organização. Assim, a cultura organizacional exerce papel determinante, pois influencia a forma como os colaboradores percebem e internalizam a importância da proteção de informações (Netto; Silveira, 2007).

A integração entre gestão da informação e cultura organizacional contribui para a minimização de riscos e para a prevenção de incidentes de segurança. Buogo, Fachinelli e Giacomello (2019) destacam que organizações que desenvolvem uma cultura de conscientização sobre o uso correto de dados e sistemas tecnológicos conseguem reduzir significativamente vulnerabilidades operacionais.

No contexto da Lei Geral de Proteção de Dados (LGPD), a cultura organizacional assume ainda mais relevância. Souza e Tomei (2024) ressaltam que a implementação de políticas de proteção de dados não deve se limitar à formalização de normas e regulamentos, mas sim envolver o engajamento de todos os níveis hierárquicos. Quando a organização internaliza valores de ética, transparência e responsabilidade no tratamento de informações, a adesão às práticas de segurança torna-se mais natural e consistente.

Silveira, Lunardi e Cerqueira (2023) argumentam que falhas recorrentes na proteção de dados podem estar diretamente ligadas a atitudes de improviso ou descuido, evidenciando a necessidade de uma cultura organizacional robusta, capaz de internalizar a disciplina e a conformidade como princípios centrais.

A implementação de programas de conscientização e treinamentos contínuos representa uma estratégia eficiente para fortalecer a cultura de segurança da informação. Silva Netto e Silveira (2007) destacam que o investimento em educação corporativa não apenas aumenta a capacidade técnica dos

colaboradores, mas também promove mudanças comportamentais, gerando um ambiente mais seguro e resiliente frente a incidentes de violação de dados.

A segurança da informação e a cultura organizacional são dimensões interdependentes e complementares. Souza e Tomei (2024) enfatizam que, sem a consolidação de valores e práticas de proteção de dados na cultura organizacional, qualquer medida tecnológica ou regulamentar pode se tornar insuficiente. Assim, a criação de uma cultura sólida, orientada por princípios de ética, responsabilidade e conscientização, configura-se como elemento central para a eficácia da proteção de informações e para o fortalecimento da confiabilidade institucional.

3.2 SANÇÕES ADMINISTRATIVAS E CONSEQUÊNCIAS DO DESCUMPRIMENTO DA LGPD

O descumprimento da Lei Geral de Proteção de Dados implica uma série de sanções administrativas que visam assegurar o cumprimento das normas e a proteção dos direitos dos titulares de dados. Grotti (2021) destaca que o sistema sancionatório previsto na LGPD é estruturado para aplicar penalidades proporcionais à gravidade da infração, abrangendo desde advertências até multas significativas, além de medidas complementares que obrigam a organização a adotar práticas corretivas imediatas.

Dentre as sanções previstas, as multas representam um dos instrumentos mais expressivos de repressão. Segundo Vilela e Lemos (2020), estas podem atingir até 2% do faturamento da empresa, limitadas a um teto de cinquenta milhões de reais por infração, demonstrando o caráter punitivo e pedagógico da legislação, essa estrutura busca não apenas punir, mas também incentivar a implementação de boas práticas de governança e de segurança da informação.

Além das multas, a LGPD prevê outras sanções, como publicização da infração e bloqueio ou eliminação de dados pessoais. Castro (2023) explica que tais medidas visam mitigar os danos causados aos titulares e sinalizar à sociedade a responsabilidade da organização, funcionando como mecanismo de transparência e de prevenção de reincidência.

As consequências do descumprimento da LGPD extrapolam o âmbito administrativo, podendo gerar responsabilização civil e, em casos extremos, repercussões criminais. Damião e Novais (2024) argumentam que falhas na proteção de dados podem resultar em ações judiciais por danos materiais e morais, afetando a imagem institucional e a confiabilidade do negócio perante clientes e parceiros.

Outro ponto relevante é que a aplicação de sanções depende da atuação da Autoridade Nacional de Proteção de Dados (ANPD), que tem poder para fiscalizar, notificar e aplicar penalidades. Grotti (2021) enfatiza que a ANPD atua como órgão regulador e fiscalizador, garantindo que as organizações mantenham práticas consistentes com a lei e adotem medidas corretivas quando necessário. A atuação da ANPD contribui para consolidar uma cultura de responsabilidade e diligência no tratamento de dados.

3.3 PERSPECTIVAS FUTURAS DO TELETRABALHO E DA PROTEÇÃO DE DADOS

O teletrabalho, consolidado durante o período de pandemia, continua a se expandir no cenário corporativo brasileiro e mundial, apresentando desafios e oportunidades para a proteção de dados pessoais. Amaral e Moreira (2024) destacam que a adoção crescente do trabalho remoto exige das organizações uma abordagem estratégica que integre governança digital, cultura de segurança da informação e conformidade com a Lei Geral de Proteção de Dados (LGPD), garantindo a proteção dos dados mesmo fora do ambiente físico da empresa.

Uma perspectiva futura relevante é o fortalecimento de políticas internas que promovam a responsabilização conjunta de empregadores e empregados. Reis e Fernandes (2023) apontam que a corresponsabilidade no tratamento de dados será cada vez mais exigida, com mecanismos de monitoramento, treinamentos periódicos e protocolos de segurança digital que acompanhem a evolução tecnológica e as novas modalidades de trabalho remoto.

A expansão do uso de tecnologias móveis e do modelo BYOD (Bring Your Own Device) também influencia as tendências futuras do teletrabalho. Fernandes (2024) observa que a utilização de dispositivos pessoais deve ser acompanhada de diretrizes claras sobre o uso seguro, políticas de criptografia, autenticação multifatorial e proteção contra vazamentos, configurando um novo paradigma de governança digital que se adapta à flexibilidade do trabalho remoto.

A integração de soluções tecnológicas avançadas, como inteligência artificial e plataformas de nuvem segura, tende a se tornar um elemento central na proteção de dados. Amaral e Moreira (2024) enfatizam que essas ferramentas permitem monitoramento contínuo, análise de riscos em tempo real e prevenção proativa de incidentes, fortalecendo a confiança dos trabalhadores e a conformidade legal das organizações.

Do ponto de vista jurídico, o teletrabalho e a proteção de dados deverão se consolidar como elementos interdependentes nas relações laborais. Reis e Fernandes (2023) destacam que a legislação e a jurisprudência evoluirão para regulamentar mais detalhadamente a responsabilidade do empregador em cenários remotos, equilibrando direitos do trabalhador com a necessidade de proteção de informações sensíveis, prevenindo conflitos e litígios trabalhistas.

As perspectivas futuras apontam para a construção de um ambiente laboral híbrido e digitalmente seguro, no qual a LGPD e boas práticas organizacionais atuam como pilares de confiança e eficiência. Fernandes (2024) ressalta que a conscientização, a educação contínua dos colaboradores e o investimento em tecnologia são estratégias essenciais para que o teletrabalho seja sustentável, ético e seguro, consolidando um modelo que integra inovação, proteção de dados e produtividade.

4 CONCLUSÃO

A análise desenvolvida ao longo deste trabalho permitiu compreender como a proteção de dados pessoais nas relações laborais se tornou um tema central diante das transformações tecnológicas e normativas recentes. A entrada em vigor da Lei Geral de Proteção de Dados representou um marco importante na tentativa de equilibrar o avanço digital com a preservação da privacidade, especialmente no contexto do teletrabalho e do uso de dispositivos pessoais. Fatores como a descentralização do ambiente de trabalho, a adoção do modelo BYOD e a mobilidade crescente do trabalhador demandam não apenas adequações técnicas, mas também mudanças estruturais e jurídicas nas organizações.

Verificou-se que os riscos à integridade dos dados no ambiente doméstico são significativos, sobretudo quando não existem delimitações claras quanto às responsabilidades de empregadores e empregados. Cabe às empresas a implementação de políticas de segurança da informação, capacitação dos colaboradores e disponibilização de infraestrutura adequada. Aos trabalhadores, por sua vez, compete a adoção de condutas diligentes, como o uso correto dos equipamentos, o sigilo das informações tratadas e o cumprimento das diretrizes internas de proteção de dados. A corresponsabilidade entre as partes é essencial para o cumprimento efetivo da legislação e para a prevenção de incidentes.

O estudo também evidenciou a importância de ferramentas tecnológicas como redes privadas virtuais, criptografia e autenticação multifator. Tais recursos, quando integrados às políticas organizacionais, auxiliam no controle e mitigação de vulnerabilidades, proporcionando um ambiente mais seguro para o tratamento de dados. Contudo, a simples adoção dessas tecnologias não é suficiente: é necessário garantir que todos os envolvidos compreendam seu funcionamento, suas finalidades e a importância de sua utilização no cotidiano profissional.

Conclui-se, assim, que a proteção de dados no contexto das relações de trabalho exige uma abordagem interdisciplinar, que envolva aspectos jurídicos, técnicos e administrativos. A LGPD traz não apenas desafios, mas também oportunidades de aprimoramento da cultura organizacional, baseada em ética, responsabilidade e transparência. Em um cenário de transformações digitais aceleradas, a consolidação de práticas seguras e conscientes no tratamento de dados pessoais é um passo fundamental para o fortalecimento das relações laborais e para a construção de um ambiente profissional mais confiável e resiliente.

REFERÊNCIAS

AMARAL, Beatriz; MOREIRA, Juarez Pinto. Garantia de proteção de dados frente ao trabalho remoto. REVISTA DELOS, v. 17, n. 61, p. e2915-e2915, 2024. Disponível em: https://ojs.revistadelos.com/ojs/index.php/delos/article/download/2915/1695

BLUM, Renato Opice; LÓPEZ, Nuria. Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito. Cadernos Jurídicos, São Paulo, v. 21, n. 53, p. 171-177, 2020. Disponível em: https://observatoriolgpd.com/wp-content/uploads/2020/05/ii_7_cadernos_juridicos_epm.pdf

BOTELHO, Marcos César; CAMARGO, Elimei Paleari. O tratamento de dados pessoais pelo poder público na LGPD. Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE), v. 9, n. 3, p. 549-580, 2021. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-Dir-Soc-Pol-Publicas_v.8_n.2.08.pdf

BUOGO, Mateus; FACHINELLI, Ana Cristina; GIACOMELLO, Cíntia Paese. Gestão do conhecimento e segurança da informação. Revista AtoZ, v. 8, n. 2, p. 39-59, 2019. Disponível em: https://www.academia.edu/download/116768913/41055.pdf

CAMPOS, Daniella; CARREIRO, Flavia. Compliance e gestão de riscos em tempos de inovação e disrupção digital. Revista de Gestão e Secretariado, v. 15, n. 4, p. e3743-e3743, 2024. Disponível em: https://ojs.revistagesec.org.br/secretariado/article/download/3743/2331

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. Cadernos Jurídicos, São Paulo, ano, v. 21, p. 163-170, 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf

CASTRO, Stella Crysthina Ferreira. A relação entre os mecanismos repressores constantes na lgpd e a sua efetividade. Portal de Trabalhos Acadêmicos, v. 15, n. 1, 2023. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/academico/article/download/2984/2312

CAVALIERI, Davi Valdetaro Gomes. Governança de dados e programa de compliance digital na administração pública: contribuições da LGPD para a integridade governamental. DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords.). LGPD & Administração Pública: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020. Disponível em: https://www.academia.edu/download/68715532/Artigo_Governanca_de_Dados_e_Programa_de_Compliance_Digital.pdf

COTO, Ideir; DIAS, Pedro Vinícius Rodrigues. Bring your own device (byod): quais as vantagens e desvantagens que podem ter nas organizações no contexto de segurança da informação. Educamazônia-Educação, Sociedade e Meio Ambiente, v. 16, n. 2, jul-dez, p. 497-510, 2023. Disponível em: https://periodicos.ufam.edu.br/index.php/educamazonia/article/download/11877/8377

COUTINHO, Aldacy Rachid. Proteção de dados do trabalhador e a questão do necessário consentimento: uma abordagem a partir da Lei n. 13.709/2018. FUTURO, p. 291, 2020. Disponível em: https://www.researchgate.net/profile/Rodrigo-Carelli/publication/346345624_Futuro_do_Trabalho_Os_efeitos_da_revolucao_digital_na_sociedade/links/5fbe90c492851c933f5c2498/Futuro-do-Trabalho-Os-efeitos-da-revolucao-digital-na-sociedade.pdf#page=292

CRUZ, Uniran Lemos; PASSAROTO, Matheus; JUNIOR, Nauro Thomaz. O Impacto da Lei Geral de Proteção de Dados Pessoais (LGPD) nos escritórios de contabilidade. ConTexto-Contabilidade em Texto, v. 21, n. 49, p. 30-39, 2021. Disponível em: https://seer.ufrgs.br/ConTexto/article/download/112561/pdf

DAMIÃO, Alisson Santana; NOVAIS, Thyara Gonçalves. Consequências jurídicas da lgpd para os crimes virtuais. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 11, p. 6590-6613, 2024. Disponível em: https://periodicorease.pro.br/rease/article/download/17054/9549

ESTÊVÃO, Luciana Costa; LIMA, Stephane Kelly; SILVA, Luanjir Luna. A Lei Geral de Proteção de Dados (LGPD) no âmbito das relações trabalhistas: conceitos, impactos e suas implicações. REVISTA BRASILEIRA DE DIREITO SOCIAL, v. 5, n. 2, p. 63-74, 2022. Disponível em: https://rbds.emnuvens.com.br/rbds/article/download/181/158

FALANGOLA, Tiago Veras; RAMALHO, Amanda Maia. Compliance e a lei geral de proteção de dados. Revista Jurídica do Cesupa, v. 6, n. 1, p. 121-140, 2025. Disponível em: https://periodicos.cesupa.br/index.php/RJCESUPA/article/download/423/206

FERNANDES, Gustavo Resende. A subordinação jurídica do empregado na modalidade de teletrabalho: desafios, perspectivas e equilíbrio. 2024. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/8349/1/ART%20GUSTAVO%20RESENDE.pdf

FERNANDES, Marcelo Eloy; NUZZI, Ana Paula Eloy. Fundamentos da Lei Geral de Proteção de Dados (LGPD): uma revisão narrativa. Research, Society and Development, v. 11, n. 12, p. e310111234247-e310111234247, 2022. Disponível em: https://rsdjournal.org/index.php/rsd/article/download/34247/29094

FERREIRA, André et al. As perspectivas do home office pós-pandemia na percepção do empregado: uma pesquisa de campo. Race: revista de administração, contabilidade e economia, v. 20, n. 3, p. 5, 2021. Disponível em: https://dialnet.unirioja.es/descarga/articulo/8442430.pdf

FIGUEIREDO, Elisabeth et al. Teletrabalho: Contributos e desafios para as organizações. Revista Psicologia: Organizações e Trabalho, v. 21, n. 2, p. 1427-1438, 2021. Disponível em: https://www.repository.utl.pt/bitstream/10400.5/28588/1/Teletrabalho%20Contributos%20e%20Desafios%20para%20as%20Organiza%C3%A7%C3%B5es.pdf

FILARDI, Fernando; CASTRO, Rachel Mercedes P.; ZANINI, Marco Tulio Fundão. Vantagens e desvantagens do teletrabalho na administração pública: análise das experiências do Serpro e da Receita Federal. Cadernos Ebape. br, v. 18, p. 28-46, 2020. Disponível em: https://www.scielo.br/j/cebape/a/pJSWmhnCPvz6fGwdkcFyvLc/?lan

FONTANA, Clarissa Peres. A evolução do trabalho: da pré-história até ao teletrabalho. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 7, n. 7, p. 1155-1168, 2021. Disponível em: https://periodicorease.pro.br/rease/article/download/1759/736

GAURIAU, Rosane. Tratamento de dados pessoais e relação laboral: contribuições do RGPD e do direito do trabalho francês. Revista do Tribunal Regional do Trabalho da 18ª Região, 2021. Disponível em: https://revista.trt18.jus.br/index.php/revista/article/download/46/50

GROTTI, Dinorá Adelaide Musetti. As sanções administrativas na lei geral de proteção de dados. O direito administrativo do pós-crise, p. 179, 2021. Disponível em:

https://www.academia.edu/download/74027766/77_Reforma_Administrativa_criticas_e_caminhos.pdf#page=179

JESUS, Orlando Alves Lopes; BRITO, Cibele Guimarães; REIS, Laine. Compliance digital: ferramenta estratégica na gestão de uma governança positiva. Graduação em Movimento-Ciências Jurídicas, v. 1, n. 2, p. 166-166, 2022. Disponível em: https://periodicos.uniftc.edu.br/index.php/gdmdireito/article/download/514/168

JOELSONS, Marcela. Lei geral de proteção de dados: fronteiras do legítimo interesse. Editora Foco, 2022.

KREMER, Bianca. Os agentes de tratamento de dados pessoais. A LGPD e o novo marco normativo do Brasil. Porto Alegre: Arquipélago, p. 289-318, 2020. Disponível em: https://www.academia.edu/download/63498490/Os_agentes_de_tratamento_de_dados_pessoais_BKREMER_LivroLGPD20200601-95532-9b28nq.pdf

MEDEIROS, Samuel Andreatta. Proteção de Dados: VPNS e o ordenamento jurídico brasileiro. Revista Eletrônica da PGE-RJ, v. 5, n. 2, 2022. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/download/268/236

MOREIRA, Camila Macedo Thomaz; THAINES, Aleteia Hummes Thaines. A Lei Geral de Proteção de Dados Pessoais e as suas repercussões nas relações trabalhistas. Revista Eletrônica de Ciências Contábeis, v. 12, n. 3, p. 1-19, 2023. Disponível em: https://seer.faccat.br/index.php/contabeis/article/view/3096/1873

MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018). MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coords.). Responsabilidade civil e novas tecnologias. Indaiatuba, SP. Editora Foco, 2020. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf

NEVES, Denise Lemes Fernandes et al. A segurança da informação de encontro às conformidades da LGPD. Revista Processando o Saber, v. 13, p. 186-198, 2021. Disponível em: https://fatecpg.edu.br/revista/index.php/ps/article/download/171/146

NOGUEIRA, Michele. Segurança na Conectividade: Protegendo Redes e Conexões. Computação Brasil, n. 52, p. 30-34, 2024. Disponível em: https://journals-sol.sbc.org.br/index.php/comp-br/article/download/4600/2742

OLIVEIRA, Bárbara Francis; MATHEUS, Felipe Morita. Teletrabalho: a existência de vantagens e desvantagens. Revista Juris UniToledo, v. 7, n. 01, p. 83-98, 2022. Disponível em: https://wyden.periodicoscientificos.com.br/index.php/jurisunitoledo/article/download/268/243

OLIVEIRA, Larissa; NOVAIS, Thyara Gonçalves. Lei Geral De Proteção De Dados Pessoais: Responsabilidade civil no vazamento de informações. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 5, p. 1614-1631, 2024. Disponível em: https://periodicorease.pro.br/rease/article/download/13668/6892

PADILHA, Cleverton Luiz; BITTENCOURT, Maurício. Teletrabalho: home office e os impactos após a reforma trabalhista. Revista Gestão e Conhecimento, v. 14, n. 1, 2020. Disponível em: https://revistagc.com.br/ojs/index.php/rgc/article/download/134/139

PEREIRA, Lucas Avanci; VICENTINE, Augusto Luciano; RIZO, Andre Castro. Impactos da Engenharia Social na Segurança da Informação. Revista Brasileira em Tecnologia da Informação, v. 4, n. 1, p. 48-58, 2022. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/download/75/34

REIS, Nathalya Aparecida Lemes; FERNANDES, Suzidarly Ribeiro Teixeira. Privacidade e Proteção de Dados do Empregado: A Incidência da Lei Geral de Proteção de Dados no Teletrabalho. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 5, p. 269-290, 2023. Disponível em: https://periodicorease.pro.br/rease/article/download/9662/3759

SANTOS, Leticia Aparecida; COSTA, Denis Honorato. O novo normal: A evolução do trabalho home-office e hibrido após pico da crise pandêmica SARS-CoV-2. E-Acadêmica, v. 3, n. 2, p. e1632151-e1632151, 2022. Disponível em: https://mail.eacademica.org/eacademica/article/download/151/133

SILVA NETTO, Abner da; SILVEIRA, Marco Antonio Pinheiro da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. JISTEM-Journal of Information Systems and Technology Management, v. 4, p. 375-397, 2007. Disponível em: https://www.scielo.br/j/jistm/a/Vx8Ypv6mDjxdYkKKrfYVgqz/?format=html&lang=pt&stop=next

SILVA, Adriana de Andrade Freitas et al. Teletrabalho e pandemia de covid-19: aspectos jurídicos e repercussões no direito trabalhista brasileiro. International Contemporary Management Review, v. 5, n. 3, p. e200-e200, 2024. Disponível em: https://www.icmreview.com/icmr/article/download/200/121

SILVA, Eduardo. Cloud Security & BYOD-Como ter mobilidade mantendo a segurança da informação. Eduardo Silva, 2023.

SILVEIRA, Jonas Rafael; LUNARDI, Guilherme Lerch; CERQUEIRA, Lucas Santos. Relação entre cultura e segurança da informação: como evitar falhas decorrentes do “jeitinho brasileiro”?. REAd. Revista Eletrônica de Administração (Porto Alegre), v. 29, n. 01, p. 143-170, 2023. Disponível em: https://www.scielo.br/j/read/a/mXzJBPHSXLkxTFPBVGMhkqs/?format=pdf&lang=pt

SOARES, Paloma Medrado Lopes. Ética empresarial e teletrabalho: o compliance quanto ao assédio moral, proteção de dados e desconexão-aspectos do direito comparado. Editora Thoth, pág. 87. 2022.

SOUZA, Fabio Benedito. Usuário, o elo mais fraco da segurança da informação. Revista Scientia Alpha, v. 1, n. 1, 2022. Disponível em: https://revista.alfaumuarama.edu.br/index.php/rsa/article/download/34/33

SOUZA, Thaís Soares; TOMEI, Patrícia Amélia. Cultura organizacional e lei geral de proteção de dados (LGPD). Revista Pensamento Contemporâneo em Administração, v. 18, n. 4, p. 106-130, 2024. Disponível em: https://www.redalyc.org/journal/4417/441780117008/441780117008.pdf

TEFFÉ, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica. com, v. 9, n. 1, p. 1-38, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/download/510/384

TEREZA, Ana Carolina Faria; ÁGUILA, Iara Marthos. A lei geral de proteção de dados nas relações de trabalho: uma análise da responsabilidade da empresa no caso de vazamento de dados pessoais e sensíveis do empregado. Revista de Iniciação Científica e Extensão da Faculdade de Direito de Franca, v. 8, n. 1, 2023. Disponível em: https://revista.direitofranca.br/index.php/icfdf/article/download/1566/1007

VEBBER, Thailini; BORGES, Silvana Maia. Impactos do teletrabalho na saúde mental do trabalhador. Revista sobre Excelência em Gestão e Qualidade, v. 3, n. 2, p. 1-17, 2021. Disponível em: https://www.fismaead.edu.br/seer/index.php/jemq/article/download/35/15

VILELA, Camila Maria; LEMOS, Christine Mattos Albiani. A responsabilização decorrente do tratamento de dados pessoais e o sistema sancionatório da lei geral de proteção de dados pessoais ("LGPD"). Revista Ilustração, v. 1, n. 2, p. 57-67, 2020. Disponível em: https://journal.editorailustracao.com.br/index.php/ilustracao/article/download/17/17

XAVIER, Fabio Correa. LGPD: Uso do legítimo interesse como base legal para tratamento de dados pessoais. TCE São Paulo, v. 16, 2021. Disponível em: https://atricon.org.br/wp-content/uploads/2023/09/LGPD-Uso-do-legitimo-interesse-como-base-legal-para-tratamento-de-dados-pessoais.pdf

YAEGASHI, João Gabriel; OTERO, Cleber Sanfelici. A responsabilidade do empregador pela proteção de dados no meio ambiente de trabalho: consequências jurídicas. Meritum, Revista de Direito da Universidade FUMEC, 2022. Disponível em: https://revista.fumec.br/index.php/meritum/article/view/8807/4692