

47 PROTEÇÃO VS. PRODUTIVIDADE: AS BARREIRAS DA LEI GERAL DE PROTEÇÃO DE DADOS PARA OS MICROEMPREENDEDORES NO BRASIL

Moriah Bandeira Henequim Costa¹, Andryelle Vanessa Camilo Pomin²

¹ Acadêmica do curso de Direito, Universidade Cesumar - UniCesumar, Campus Maringá-Pr, Trabalho de Conclusão de Curso.

² Orientadora. Doutora (2025) pela UniCesumar. Docente do Curso de Direito da Universidade Cesumar – UniCesumar, na linha Efetividade da Justiça e Direitos da Personalidade.

RESUMO

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) representou um marco para a consolidação da privacidade e da autodeterminação informativa no Brasil, contudo sua implementação tem imposto desafios significativos ao setor empresarial, especialmente às micro e pequenas empresas, que frequentemente carecem de recursos jurídicos, tecnológicos e financeiros para atender às exigências legais. Este artigo tem como objetivos identificar as exigências centrais da LGPD aplicáveis a esses empreendimentos, analisar os principais obstáculos à sua implementação, avaliar os impactos dessas dificuldades sobre a efetividade do direito à autodeterminação informativa, à liberdade de iniciativa e à função social da empresa bem como sugerir medidas que possibilitem conciliar a proteção de dados pessoais com a viabilidade econômica e operacional das micro e pequenas empresas. A pesquisa adota metodologia bibliográfica e abordagem hipotético-dedutiva, buscando compreender em que medida as dificuldades práticas de adequação à LGPD revelam descompasso entre a elaboração normativa e a realidade operacional das empresas de menor porte. Os resultados indicam que, embora a norma imponha encargos onerosos, sua correta implementação pode proporcionar ganhos institucionais relevantes, como maior confiança dos consumidores, fortalecimento da governança corporativa e diferenciação competitiva no mercado digital contemporâneo. Conclui-se que a LGPD, apesar dos desafios que impõe, pode ser compreendida não apenas como um mecanismo de proteção de direitos fundamentais, mas também como oportunidade de aprimoramento da gestão empresarial e de fortalecimento da economia digital.

Palavras-chave: Governança corporativa; Modernização digital; Privacidade informacional; Riscos regulatórios.

1 INTRODUÇÃO

A sociedade contemporânea vivencia um processo acelerado de digitalização, no qual os dados pessoais assumiram posição de ativo estratégico para organizações públicas e privadas. A coleta, o armazenamento e o uso dessas informações tornaram-se indispensáveis à atividade econômica, mas também suscitaram preocupações quanto à privacidade e à segurança informacional. No Brasil, esse cenário levou à promulgação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), posteriormente fortalecida pela Emenda Constitucional nº 115/2022, que consagrou a proteção de dados como direito fundamental, assegurando que “é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais” (BRASIL, 1988, art. 5, LXXIX).



A LGPD representa um marco jurídico essencial para a tutela da privacidade e da autodeterminação informativa, contudo a sua implementação tem revelado descompasso entre a elaboração normativa e a realidade prática das empresas, sobretudo das micro e pequenas, que frequentemente carecem de estruturas tecnológica, jurídica e financeira para atender às exigências legais. Esse descompasso constitui o eixo central da presente pesquisa, que busca analisar como a norma, embora indispensável à proteção dos titulares, impõe desafios que afetam diretamente a viabilidade e a produtividade empresarial.

O objetivo geral deste estudo é examinar justamente os obstáculos enfrentados pelas empresas brasileiras no processo de adequação à LGPD, considerando seus aspectos jurídicos, operacionais e econômicos. De forma específica, pretende-se (i) identificar as exigências centrais da legislação; (ii) avaliar os impactos das dificuldades sobre a efetividade da proteção de dados e os direitos da personalidade abrangidos; e (iii) propor medidas que conciliem a conformidade normativa com a viabilidade das atividades empresariais.

A relevância do tema se justifica tanto no plano jurídico, pela consolidação de um direito personalíssimo, quanto nos planos social e econômico, diante do impacto direto da proteção de dados na competitividade empresarial e na relação de confiança com os consumidores.

Metodologicamente, a pesquisa adota caráter bibliográfico e abordagem hipotético-dedutiva, possibilitando a análise crítica da legislação e da doutrina especializada bem como a proposição de alternativas aplicáveis.

Por fim, o artigo organiza-se em três seções principais: a primeira apresenta a LGPD e seus fundamentos; a segunda analisa os desafios práticos enfrentados pelas empresas, inclusive no tocante aos direitos da personalidade que podem ser afetados; e a terceira propõe estratégias de superação, destacando o papel da capacitação, do compliance e da cooperação com a Autoridade Nacional de Proteção de Dados (ANPD). Portanto, consiste como um dos objetivos principais desse artigo compreender até que ponto a adequação da LGPD, diante das flexibilizações propostas para microempresas, não compromete a essência da proteção de dados como direito fundamental.



2 EXIGÊNCIAS CENTRAIS DA LGPD PARA MICRO E PEQUENAS EMPRESAS

A transformação digital impactou profundamente a dinâmica empresarial, tornando o tratamento de dados pessoais uma etapa essencial da atividade econômica moderna. Com a ascensão do comércio eletrônico, da automação e da análise preditiva, os dados passaram a ser considerados ativos estratégicos. Lisboa (2019, p. 17) reconhece que a internet, hoje, é considerada uma ferramenta inerente à atividade empresarial, fundamental para o empresário ampliar suas vendas e compras e administrar sua empresa, evidenciando os dados de clientes, colaboradores e parceiros na operacionalização do negócio.

O cenário de coleta massiva e automatizada de informações pessoais gerou a necessidade de um regramento uniforme para todas as etapas do tratamento, abrangendo a identificação, a categorização, a coleta, o uso, o armazenamento e o descarte. Inspirada nas normas estadunidenses e europeias, especialmente no Regulamento Geral de Proteção de Dados da União Europeia (RGPD), de 14 de abril de 2016, bem como nas diretrizes da OCDE, após as repercussões mundiais sobre vazamento de dados e ciberataques, a LGPD representa um divisor de águas ao conferir maior controle aos titulares dos dados e impor responsabilidades objetivas às organizações (Lisboa, 2019, p. 30).

A LGPD define como dado pessoal “toda informação relacionada a pessoa natural identificada ou identificável” (Brasil, 2018, art. 5º, I). A classificação compreende ainda os dados pessoais sensíveis, aqueles que dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, entre outros, os quais exigem maior grau de proteção jurídica. A coleta de dados, etapa particularmente delicada, pode ocorrer por formulários digitais, cadastros presenciais, cookies, sistemas de CRM ou durante a contratação de funcionários, a multiplicidade de bases legais aumenta a complexidade para pequenos negócios, que carecem de orientação para identificar a mais adequada

Além disso, o artigo 6º estabelece os princípios que orientam a atividade de tratamento como a finalidade, a adequação, a necessidade, a transparência, a segurança, a prevenção e a responsabilização (Brasil, 2018, art. 6º). Para o tratamento de dados de crianças e adolescentes, a exigência é ainda mais rigorosa:



o artigo 14 impõe que, em regra, a coleta e o uso dependem do consentimento expresso de pelo menos um dos pais ou responsável legal (Brasil, 2018, art. 14).

O dever de transparência, disciplinado nos artigos 9º e 18, impõe, às empresas, a obrigação de informar de forma clara as finalidades do tratamento, a duração do armazenamento e a identidade dos responsáveis, além de assegurar, aos titulares, direitos como acesso, correção, exclusão e contestação de dados (Brasil, 2018, art. 9º e 18). Vinculado a isso, o artigo 46 determina a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados contra acessos não autorizados, perda ou destruição ilícita (Brasil, 2018, art. 46).

As relações contratuais também são objeto de atenção. O artigo 39 prevê que operadores só podem tratar dados conforme instruções do controlador, o que exige contratos claros com cláusulas de confidencialidade e de segurança da informação, sobretudo em pequenas empresas que terceirizam serviços de contabilidade, tecnologia da informação ou logística (Brasil, 2018, art. 39).

Outro aspecto relevante refere-se ao descarte das informações. O artigo 16, da LGPD, impõe que, encerrado o tratamento, os dados pessoais sejam eliminados, ressalvadas hipóteses legais de guarda mínima (Brasil, 2018, art. 16). Guedes e Meireles (2021, p. 253-254) destacam a importância do descarte dos dados coletados, que, além de ser uma prerrogativa do usuário para a exclusão definitiva de suas informações, pode ocorrer por esgotamento funcional, ilegalidade ou decurso de prazo. As autoras afirmam que

A regra geral é a completa eliminação dos dados pessoais pelo controlador quando o tratamento se encerra, nos moldes do art. 16 da LGPD. Trata-se de modelo que visa a diminuir os riscos do uso não autorizado ou indevido das informações pessoais, buscando uma maior tutela do seu titular.

Essa imposição de cuidados no descarte dos dados do usuário deve ser observada pelos empresários, para que não cometam erros desnecessários e sancionatórios.

3 IMPACTOS NO DIREITO À AUTODETERMINAÇÃO INFORMATIVA, À LIBERDADE DE INICIATIVA E À FUNÇÃO SOCIAL DA EMPRESA



Apesar dos avanços, a implementação da LGPD impôs desafios significativos ao setor empresarial. As empresas brasileiras, sobretudo as de pequeno e médio porte, enfrentam barreiras jurídicas, regulatórias, operacionais e tecnológicas para se adequarem plenamente, já que muitas carecem de estrutura jurídica robusta para atenderem às exigências legais.

Nesse contexto digitalizado, os dados pessoais constituem insumos essenciais à atividade econômica. Sendo assim, o desafio central está em conciliar inovação e crescimento com a conformidade regulatória. Tal constatação evidencia que o tratamento de dados está diretamente ligado à liberdade de iniciativa e ao desenvolvimento econômico.

A regulamentação tem imposto mudanças estruturais nas rotinas internas das empresas, que passaram a lidar com novos instrumentos jurídicos como termos de consentimento, contratos de operação de dados e políticas de privacidade. No entanto, essa transição esbarra na carência de recursos e de profissionais qualificados, especialmente entre as microempresas.

Por exemplo, o Eletronic Data Interchange (EDI), uma ferramenta que serve para automatizar o comércio eletrônico interempresarial que engloba a produção, distribuição, comercialização, venda ou entrega de bens e serviços por meios eletrônicos. O uso do EDI permite a automação de transações comerciais entre empresas e é uma alternativa eficiente para grandes corporações, mas altamente desafiadora para pequenos empreendimentos. O EDI beneficia grandes empresas, reduzindo bastante o tempo e o custo do processamento manual de dados. No entanto, o EDI é complexo e difícil de implementar. Para pequenas e médias empresas, a infraestrutura de rede e o software necessários para implementação do EDI são proibitivamente caros. Além disso, os padrões de EDI em diferentes países variam, tornando as transações internacionais complexas, mesmo que estejam usando o mesmo padrão – tenham suas próprias implementações (EDI basics, 2025)

Somados a isso, os altos custos de conformidade e o risco de penalidades por descumprimento — como multas de até 2% do faturamento, limitadas a R\$ 50 milhões (BRASIL, 2018, art. 52) — elevam ainda mais o grau de complexidade da adaptação.

Atualmente, os empreendimentos enfrentam grande dificuldade na interpretação e aplicação das exigências normativas, o que pode levar a lacunas de



conformidade. A complexidade das medidas exigidas, a escassez de profissionais especializados e o desconhecimento dos dispositivos legais como entraves centrais dificultam ou impossibilitam os empresários de fazerem as alterações necessárias para a implementação da Lei Geral de Proteção de Dados. Assim, há uma percepção generalizada que a regulação é excessivamente complexa e onerosa.

Consequentemente, a inexistência de contratos específicos de processamento de dados com terceiros impede a responsabilização clara e dificulta a governança corporativa. Dos Santos, Evangelista e Oliveira (2023, p. 7-8) corroboram a ideia de que a ausência de cultura de proteção de dados, aliada à falta de investimento e de capacitação dos profissionais, é uma barreira para a adoção das novas regras, e, assim, eles expõem que

somente 35% das microempresas dizem não ter política estabelecida de segurança de dados e afirmam que vão ter que começar do zero (...) cerca de 28% planejam alocar menos de R\$ 10 mil, enquanto quase 40% das companhias pesquisadas ainda não sabem responder o quanto deverão desembolsar. Ainda com números 14% dizem não ter problemas para se adequar até o momento, 30% reclamam da complexidade das medidas e volume de trabalho necessário, 27% relatam a inexistência de uma área dedicada à informação e tratamento de dados na companhia, 26% da falta de conhecimento suficiente sobre a LGPD, 17% têm pouco tempo disponível para se dedicar à lei, 13% informam da falta de verba para a contratação de uma consultoria especializada e 20% não souberam informar.

Consoante a esses dados, Costa Júnior (2023, p. 46) destaca que “87% dos usuários já deixaram de realizar alguma atividade por preocupações com seus dados pessoais”.

Outrossim, além da multa mencionada, outras consequências são a publicidade da infração, o bloqueio dos dados pessoais até a sua regulamentação, a suspensão parcial por até seis meses do banco de dados envolvido ou, ainda, a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (SEBRAE-SC, 2022, p. 17-18). Dessa forma, as empresas que não se adequam correm ainda o risco de enfrentar ações judiciais e danos irreversíveis à sua reputação institucional.



Além disso, a implementação da LGPD trouxe impactos diretos sobre os direitos da personalidade, notadamente à autodeterminação informativa, à liberdade de iniciativa e à função social da empresa.

A autodeterminação informativa, constitucionalizada pela Emenda Constitucional nº 115/2022, assegura ao titular dos dados o poder de controlar suas informações pessoais. Trata-se de uma prerrogativa do livre desenvolvimento, que garante ao indivíduo decidir sobre o uso e a circulação de seus dados. A ausência de políticas claras de segurança e a coleta de dados sem transparência minam o exercício efetivo desse direito, transformando-o, em muitos casos, em uma garantia meramente formal.

Como ressalta Bittar (2015, p. 82-84), o uso de figuras humanas em publicidade e o uso maciço de criações intelectuais e artísticas ampliaram o leque de aparições públicas das pessoas, mesmo que já fossem extensos em função dos reflexos que a diversidade de meios de comunicação e de circulação propicia, inclusive no sistema de transportes, expondo-as intensamente ao meio social, em especial nos grandes centros urbanos.

Nesse sentido, observa-se que não apenas os empresários, mas também os próprios titulares, muitas vezes se expõem de maneira descuidada, compartilhando voluntariamente seus dados em ambientes digitais. Assim, não é razoável que as consequências recaiam unicamente sobre os agentes econômicos, sendo necessário reconhecer a corresponsabilidade dos indivíduos na preservação de sua privacidade.

Nesse cenário, a jurisprudência tem desempenhado papel fundamental na consolidação da LGPD. Em recente julgamento, o Superior Tribunal de Justiça reconheceu que, em contrato de seguro de vida, o vazamento de dados sensíveis enseja responsabilidade objetiva e gera dano moral presumido, independentemente de comprovação de prejuízo concreto, dada a gravidade da violação à intimidade e à autodeterminação informativa (REsp n. 2.121.904/SP, rel. Min. Nancy Andrighi, Terceira Turma, j. 11 fev. 2025, DJEN 17 fev. 2025).

Ao mesmo tempo, a lei repercute no direito à liberdade de iniciativa, também protegido constitucionalmente (BRASIL, 1988, art. 170). O princípio, que assegura, ao empresário, a livre atuação no mercado, acaba limitado pelo alto custo de conformidade e pela complexidade técnica das exigências legais. Assim, impor



requisitos onerosos sem o devido suporte normativo e institucional pode restringir o exercício da atividade econômica, criando barreiras de entrada e reduzindo a competitividade, sobretudo entre os pequenos empreendedores.

O próprio nome empresarial também goza dessa tutela, seja no campo da propriedade industrial, seja na teoria da concorrência desleal, evitando que concorrentes utilizem indevidamente denominações semelhantes com o intuito de confundir o consumidor e captar clientela de forma ilícita. Nas palavras de Bittar (2015, p. 199),

Também o nome de pessoa jurídica desfruta de instrumental de amparo específico, tanto na lei citada como na da propriedade industrial e, em particular, no âmbito da teoria da concorrência desleal, em que se pode obviar o uso indevido por concorrente, destinada a criar confusão com sua empresa, para a captação de clientela.

Por sua vez, a função social da empresa — que exige a harmonização entre o interesse privado e a preservação de direitos coletivos — assume nova centralidade no contexto da proteção de dados. A adequação à LGPD não é apenas uma obrigação legal, mas um dever de responsabilidade social. Isso porque a função social significa a superação de uma visão individualista do direito, sendo critério de valoração de situações jurídicas ligadas ao desenvolvimento da ordem econômica. Seus objetivos são o bem comum e o bem-estar coletivo. Conforme leciona a doutrina de Amaral (2018, p. 141),

A tensão entre proteção de direitos fundamentais e liberdade econômica exige, portanto, interpretação equilibrada: flexibilizações excessivas podem comprometer a essência da tutela da privacidade, ao passo que rigidez absoluta pode inviabilizar pequenos negócios. O desafio é encontrar um ponto de convergência que garanta a efetividade da norma sem sufocar a competitividade empresarial.

4 MEDIDAS DE PROTEÇÃO DE DADOS PESSOAIS VIÁVEIS ÀS MICRO E PEQUENAS EMPRESAS

Levando-se em consideração que a implementação da LGPD é necessária tanto para a proteção jurídica da própria empresa quanto de seus clientes, torna-se essencial apresentar, aos empresários, — especialmente aqueles de micro e



pequenas empresas — formas que, sem serem excessivamente onerosas, sejam suficientemente eficazes para o cumprimento efetivo da legislação.

A *priori*, embora existam programas voltados à adequação das medidas exigidas pela LGPD, como o exemplo já mencionado do *Electronic Data Interchange* (EDI), segundo Lisboa (2019, p. 182) e outros autores, apesar de serem soluções benéficas, para pequenas e médias empresas não se mostram opções viáveis, uma vez que, além de complexas, são proibitivamente caras. Em outras palavras, o investimento em infraestrutura de TI e em sistemas de gestão da segurança da informação (SGSI) costuma onerar especialmente as micro e pequenas empresas.

Esse exemplo ilustra que, além dos custos iniciais, a manutenção contínua de controles técnicos e auditorias representa um desafio sobretudo porque muitos empresários não percebem retorno imediato no investimento, o que gera resistência e atrasos no processo de adequação.

Nesse sentido, buscando as melhores estratégias, as autoras Guedes e Meireles (2021, p. 246) sustentam que os programas de “compliance” constituem mecanismos relevantes para alinhar as práticas e rotinas organizacionais às exigências da LGPD e, por consequência, à ordem constitucional. Esses programas abrangem todas as etapas do tratamento de dados, desde a coleta até a sua exclusão definitiva.

Além disso, o tema central de Guedes e Meireles (2021, p. 259) é quanto à importância do *compliance* para o descarte dos dados pessoais, portanto as autoras exploram que,

No que tange ao término de dados pessoais, como visto acima, há de se verificar as quatro hipóteses previstas na lei: i) o esgotamento da finalidade; ii) a observância do período; iii) a revogação do consentimento; iv) a determinação da autoridade nacional, por violação à LGPD. O desenvolvimento das regras de compliance deve pautar-se, portanto, nessa linha. Vale dizer, estabelecer os processos e os meios de controle adequados para definir quando ocorre o término do tratamento de dados naquela dada atividade e como acontecerá a sua eliminação, isto é, a exclusão de dado ou de conjunto de dados armazenados.

Ademais, as pesquisadoras ressaltam que essa medida, quando integrada ao Código de Conduta empresarial, deixa de ser uma prática meramente formal e passa a consolidar uma verdadeira mudança cultural, combinando tecnologia e governança.



A tecnologia, portanto, não deve ser vista isoladamente, mas como parte de uma transformação mais ampla e integrada.

Consoante com tal conclusão, o pesquisador Costa Júnior (2023, p. 87-89) enfatiza que a adequação das micro e pequenas empresas à LGPD exige, antes de tudo, uma mudança de mentalidade por parte dos gestores, que devem assumir o papel de estrategistas. Isto é, o planejamento é central para a empresa, compreender a estrutura, o funcionamento, os objetivos e colocar no papel as formas de alcançar as metas. Em suas palavras, algumas ferramentas de gestão da qualidade com o objetivo de sustentar o planejamento e os esforços de adaptação são

a análise SWOT, o fluxograma, a matriz 5W2H e o ciclo PDCA, respectivamente, contribuem com os processos de verificação e diagnóstico do ambiente; com o mapeamento dos processos executados atualmente; com o direcionamento do plano de ação para concretização das estratégias de adequação; e, com o controle e melhoria contínua de todas essas soluções

Sob essa perspectiva, Costa Júnior (2023, p. 88-92) ainda reconhece a necessidade de se estabelecer um relacionamento transparente com os clientes e principalmente com colaboradores e parceiros comerciais, visto que, assim como o empresário, eles devem tomar uma série de preocupações.

Ademais, outra estratégia é a capacitação contínua de gestores e colaboradores. Programas de treinamento são fundamentais para fomentar uma cultura organizacional de proteção de dados e garantir o cumprimento interno da LGPD, de maneira que é menos custoso ao empresário dispor de algumas horas mensalmente para preparar sua equipe para lidar com as mais diversas situações, não se limitando apenas aos desdobramentos da LGPD. De acordo com o demonstrado pela pesquisa de Ribeiro e Moreira (2021, p.129), essa preocupação já tem histórico nas empresas:

Todas as organizações que processam ou armazenam dados pessoais devem ter uma equipe bem treinada e dedicada à segurança de dados. Entretanto, 75 dos profissionais (72%) possuem equipes de TI treinadas para garantir a segurança dos dados, porém 29 profissionais (28%) afirmaram que não possuem equipe de TI pela situação financeira para garantir um investimento na segurança ou por não achar tão importante.



Nesse cenário, a Autoridade Nacional de Proteção de Dados (ANPD) surgiu com o papel central na implementação da LGPD, não atuando apenas como órgão fiscalizador, mas também como agente orientador. Dessa forma, sua atuação deve ser compreendida como uma parceria estratégica para o empresariado, especialmente para aqueles que não têm os recursos financeiros e jurídicos das empresas de grande porte.

Segundo Lisboa (2019, p. 232), cabe à ANPD editar normas, requisitar informações, fiscalizar, aplicar sanções, promover consultas públicas e difundir boas práticas, entre outras atribuições.

Para enfrentar esses desafios, a ANPD e o Sebrae têm sugerido medidas simplificadas e acessíveis, compatíveis com a realidade das empresas de pequeno porte. O Guia Orientativo para Agentes de Tratamento de Pequeno Porte da ANPD (2021, p. 6-18), por exemplo, recomenda a adoção de políticas de segurança simplificadas, como o uso de senhas fortes, o controle de acesso, a realização de backups periódicos e a proteção física de dispositivos. Também indica a realização de treinamentos periódicos para gestores e colaboradores, reforçando responsabilidades e boas práticas, a utilização de contratos claros com cláusulas de proteção de dados nas relações com fornecedores e parceiros e cuidados no uso de serviços em nuvem, incluindo autenticação multifator e acordos que garantam níveis mínimos de proteção.

De forma convergente, a Resolução CD/ANPD nº 2/2022 também trouxe flexibilizações, como no artigo 11: a dispensa da obrigatoriedade de nomeação de um encarregado pelo tratamento de dados, mas deve-se disponibilizar um canal de comunicação com o titular de dados. Ou, ainda, o artigo 14, que concedeu prazos mais amplos para a comunicação de incidentes de segurança, tornando a adequação mais viável para negócios de menor porte.

Já a cartilha “Simplificando a LGPD nos Negócios” (SEBRAE, 2022) possui o Sebraetec que se trata de uma consultoria voltada justamente para auxiliar os empresários a se adaptarem à LGPD, por um valor mais acessível. Além disso, também reforça a importância de instrumentos de autoavaliação, como checklists de conformidade, e o passo a passo para adequação.



Uma característica interessante para o empresário sobre a ANPD, segundo o art. 58-A, da LGPD, é que o Conselho Nacional de Proteção de Dados deve contar com representantes do setor empresarial. Dessa forma, o diálogo contínuo com a ANPD, aliado a uma postura proativa e preventiva das empresas, representa uma oportunidade de transformação positiva, capaz de conciliar proteção de dados e crescimento sustentável.

Dessa forma, a soma de esforços entre políticas públicas, práticas de gestão e mudanças culturais representa uma oportunidade de transformação positiva, capaz de conciliar a proteção de dados e o crescimento sustentável das micro e pequenas empresas.

5 CONSIDERAÇÕES FINAIS

Diante das dificuldades identificadas para a implementação da Lei Geral de Proteção de Dados, torna-se necessário apontar estratégias que auxiliem os empresários, especialmente os de pequeno e médio porte, no processo de conformidade legal. Essas estratégias envolvem a capacitação de equipes, um planejamento funcional e o papel orientador da Autoridade Nacional de Proteção de Dados (ANPD).

A Lei Geral de Proteção de Dados Pessoais (LGPD) representa uma mudança paradigmática no cenário jurídico-empresarial brasileiro, exigindo uma reestruturação significativa das práticas de tratamento de dados no setor privado. Como foi demonstrado ao longo deste trabalho, a empresa que não implementar adequadamente a legislação sofrerá uma série de consequências - como na sua reputação e a multa mencionada - em razão da relevância dos direitos violados, especialmente no que tange às micro e pequenas empresas.

Diante dos desafios evidenciados, entende-se que o enfrentamento das barreiras impostas pela LGPD não pode recair exclusivamente sobre o pequeno empresário. É necessária a criação de políticas públicas específicas de incentivo, que auxiliem as micro e pequenas empresas no processo de adequação, seja por meio de linhas de crédito subsidiadas para investimento em segurança da informação, seja por programas de capacitação técnica gratuitos em parceria com universidades, Sebrae e órgãos de classe. Além disso, mecanismos de incentivo fiscal poderiam ser



instituídos para premiar empresas que comprovem conformidade efetiva com a legislação, estimulando uma cultura de proteção de dados que vá além do mero cumprimento formal.

Nesse sentido, discute-se também a pertinência de uma regulamentação diferenciada, que reconheça as limitações estruturais das empresas de menor porte, mas sem esvaziar a essência da proteção de dados pessoais. Flexibilizações, como prazos mais amplos para comunicação de incidentes ou dispensa de determinadas obrigações burocráticas, podem se justificar, desde que acompanhadas de salvaguardas mínimas e mecanismos de supervisão da ANPD. Em outras palavras, é possível reduzir o peso regulatório sem comprometer a essência da proteção conferida aos titulares, conciliando o direito fundamental à privacidade com a liberdade de iniciativa e a função social das empresas no fortalecimento da economia nacional.

Sendo assim, o estudo revela que tais barreiras podem ser superadas por meio de estratégias bem-definidas como o fortalecimento da cultura organizacional de proteção de dados, a adoção de tecnologias apropriadas e o uso de programas de compliance. A capacitação contínua de colaboradores e gestores e o apoio de consultorias especializadas também se destacam como caminhos viáveis para mitigar riscos e promover a conformidade.

Assim, conclui-se que, embora a LGPD represente um desafio significativo, ela também oferece uma oportunidade para o fortalecimento da governança corporativa, o aprimoramento da relação entre empresas e consumidores e a inserção mais ética e segura das organizações na economia digital. O empresariado brasileiro, portanto, não deve apenas temer a LGPD, mas utilizá-la como instrumento estratégico para inovação, confiança e crescimento sustentável.

REFERÊNCIAS

AMARAL, Francisco. **Direito civil : introdução**. 10. ed. Rio de Janeiro: Saraiva Jur, 2018. E-book. ISBN 9788553602100. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788553602100/>. Acesso em: 21 ago. 2025.

BATISTA, Daniela Oliveira. A aplicação da Lei Geral de Proteção de Dados nas microempresas brasileiras: desafios e perspectivas. **Revista Jurídica da FMP**, v.

15, n. 1, p. 212–230, 2022. Disponível em: <https://www.fmp.edu.br/revista-juridica/article/view/3424>. Acesso em: 5 maio 2025.

BITTAR, Carlos A. **Os Direitos da Personalidade**, 8ª edição.. Rio de Janeiro: Saraiva Jur, 2015. E-book. ISBN 9788502208292. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788502208292/>. Acesso em: 20 ago. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 de maio de 2025.

BRASIL. **Guia Orientativo para Agentes de Tratamento de Pequeno Porte**. Brasília: ANPD, 2021. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-vf.pdf>. Acesso em: 21 ago. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157-A, p. 1–10, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 maio 2025.

BRASIL. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022**. Brasília: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 21 ago. 2025.

COSTA JUNIOR, Jose Cassio da. **Os desafios da Lei Geral de Proteção de Dados para pequenas empresas: um estudo de caso em uma distribuidora em Natal/RN**. Universidade Federal do Rio Grande do Norte Centro de Ciências Sociais Aplicadas Curso de Graduação em Administração. Natal, 2023. Disponível em: <https://repositorio.ufrn.br/server/api/core/bitstreams/da63035a-ad57-4151-810e-57614745c088/content>. Acesso em 21 de ago. de 2025.

EDI BASICS. **What is EDI (Electronic Data Interchange)?** Disponível em: <https://www.edibasics.com/what-is-edi/>. Acesso em: 26 ago. 2025.

GUEDES, Gisela Sampaio da Cruz; MEIRELES Rose Melo Vencelau. A importância do compliance para o término do tratamento de dados. In: Ana Frazão e Ricardo Villas Bôas Cueva (coord.). Compliance e políticas de proteção de dados. São Paulo: **Revista dos Tribunais**, 2021, pp. 245-269. Disponível em: <https://giselasampaio.com.br/2022/03/22/a-importancia-do-compliance-para-o-termino-do-tratamento-de-dados/>. Acesso em: 20 maio 2025.

JESUS, Hémilly Machado de; ARAÚJO FILHO, Gilson Dias de. A Proteção de Dados Pessoais na Era Digital: Uma Reflexão Acerca da Responsabilidade das Redes Sociais Sobre a Captação e o Uso de Dados Pessoais dos Seus Usuários (Protecting Users Data in the Digital Age: A Reflection on the Responsibility of Social



Networks in the Use and Analysis of User Data). **Revista FACISA Online**, vol. 11, no. 2, pp. 54-70, ago.-dez. de 2022, Barra do Garças - MT. ISSN 2238-8524.

LISBOA, Letícia Lobato Anicet. **Proteção de dados na sociedade da informação e aplicação aos contratos empresariais (business to business) no Brasil**. Tese (Doutorado). Universidade do Estado do Rio de Janeiro, Faculdade de Direito, 2019. Disponível em: <https://www.bdt.d.uerj.br:8443/handle/1/9204>. Acesso em: 20 de maio de 2025.

RIBEIRO, Juliane Gonçalves; MOREIRA, Andresa de Cássia. A percepção dos profissionais da área contábil e dos gestores sobre os impactos da implementação da LGPD. **Revista Científica Multidisciplinar Núcleo do Conhecimento**, v. 2, n. 10, 2021. Disponível em: <https://revistas.fucamp.edu.br/index.php/ragc/article/view/2431>. Acesso em: 27 de maio de 2025.

SANTOS, Osni Ribeiro dos; EVANGELISTA, Leonardo Costa; OLIVEIRA, André Luiz. LGPD nas microempresas: impactos em decorrência da nova lei. **RECIMA21 - Revista Científica Multidisciplinar**, v.4, n.6, 2023. Disponível em: <https://doi.org/10.47820/recima21.v4i6.3424>. Acesso em: 20 de maio de 2025.

SEBRAE. **Simplificando a LGPD nos Negócios**. Brasília: Sebrae, 2022. Disponível em: https://sebrae.com.br/Sebrae/Portal%20Sebrae/UFs/AM/Anexos/10_Cartilha%20para%20MPE_Sebrae%20AM.pdf. Acesso em 21 de ago. de 2025.

SILVA, Ana Cristina Mendes da; MARTINS, Letícia Braga. A LGPD e a sua aplicação às microempresas: uma análise crítica dos desafios e limitações enfrentados. **Revista de Direito, Desenvolvimento e Novas Tecnologias**, v. 10, n. 23, p. 89–104, 2023. Disponível em: <https://sdn.ufv.br/2215-910X-sdn-10-23-89>. Acesso em: 5 maio 2025.