PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

DESAFIOS PARA EFETIVA IMPLANTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS EM MICROEMPRESAS

ORIENTANDO: BRUNO SILVEIRA VILANOVA

ORIENTADOR: Prof. Dr. JOSÉ ANTÔNIO TIETZMANN E SILVA

GOIÂNIA-GO
2025

BRUNO SILVEIRA VILANOVA

DESAFIOS PARA EFETIVA IMPLANTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS EM MICROEMPRESAS

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás. Professor Orientador: Dr. José Antônio Tietzmann e Silva.

GOIÂNIA-GO

2025

BRUNO SILVEIRA VILANOVA

DESAFIOS PARA EFETIVA IMPLANTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS EM MICROEMPRESAS

Data da Defesa: 19 de novembro de 2025

BANCA EXAMINADORA

Orientador: Prof.: Dr. José Antônio Tietzmann e Silva Nota

Examinadora Convidada: Prof.(a): Dra. Helena Beatriz De Moura Belle Nota

Aos meus pais, pelo amor, pela dedicação e pelo exemplo de perseverança que inspiraram e sustentaram cada etapa da minha formação.

À minha irmã Beatriz e ao meu irmão Leonardo, pelo carinho e incentivo constantes, que sempre me motivaram a seguir em frente.

A todos vocês, dedico com gratidão esta conquista.

DESAFIOS PARA EFETIVA IMPLANTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS EM MICROEMPRESAS

Bruno Silveira Vilanova[1]

O principal objeto de estudo deste artigo foi a análise dos desafios para a efetiva implantação da Lei Geral de Proteção de Dados (LGPD) em microempresas, abordando tanto os benefícios quanto os obstáculos enfrentados por esses negócios. Nesse sentido, foram examinados os aspectos históricos e conceituais da proteção de dados no Brasil, o contexto legislativo da LGPD, bem como os desafios específicos dessas empresas na adequação às exigências legais, como recursos financeiros e capacitação técnica. A metodologia utilizada foi o método dedutivo, baseada na legislação, documentos oficiais, doutrina, jurisprudência e relatórios que analisam o impacto da LGPD em pequenas organizações. Ao final, pretendeu-se demonstrar que, embora a adequação à LGPD possa trazer benefícios como maior segurança jurídica e fortalecimento da confiança dos consumidores, os custos e a complexidade do processo representam barreiras significativas para micro empresários. Assim, conclui-se que são necessárias políticas públicas e mecanismos simplificados para assegurar que a conformidade com a LGPD seja alcançável e proporcional às capacidades desses negócios.

Palavras-chave: LGPD. Microempresas. Proteção de dados. Desafios. Conformidade.

[1] Acadêmico de Direito da Pontifícia Universidade Católica de Goiás.

SUMÁRIO

INTRODUÇÃO

Neste artigo, trataremos da necessidade de analisar os desafios encontrados pelas microempresas para se adequarem à Lei Geral de Proteção de Dados, refletindo sobre a história e surgimento da LGPD e possíveis medidas a serem tomadas para facilitar a adesão à lei. O presente estudo nasceu da observação da dificuldade prática e financeira encontrada por microempresários em adequar suas empresas à Lei Geral de Proteção de dados.

O objetivo geral dessa pesquisa é analisar os principais desafios que microempresas enfrentam para estar em conformidade com a LGPD e propor soluções práticas para facilitar a implementação dessa lei.

Para realização do trabalho, utilizou-se do método dedutivo, partindo do marco normativo e da literatura especializada, por meio da compilação de referenciais bibliográficos, com auxílio de autores especializados no assunto, além do estudo legislativo, doutrinário e jurisprudencial.

Deste modo, o presente artigo foi estruturado em três seções. A primeira seção tem como objetivo proporcionar uma visão e panorama histórico do surgimento da Lei Geral de Proteção de Dados e a sua importância. Em seguida, na segunda seção aborda-se os desafios para efetiva implantação da Lei Geral de Proteção de Dados em microempresas. Por fim, na terceira seção, discutem-se o papel da Agência Nacional da Proteção de Dados e as possíveis medidas facilitadoras e perspectivas para a adequação das microempresas à LGPD.

A relevância do tema se justifica pela crescente digitalização das atividades empresariais e pela vulnerabilidade estrutural das microempresas diante das exigências técnicas impostas pela legislação. Em um cenário em que os dados pessoais se tornaram ativos valiosos e estratégicos, compreender como pequenos empreendimentos podem alcançar conformidade sem comprometer sua sustentabilidade financeira é essencial para garantir não apenas o cumprimento legal, mas também a consolidação de uma cultura de privacidade e segurança da informação.

1. A LEI GERAL DE PROTEÇÃO DE DADOS NA ERA DIGITAL

1.1 HISTÓRICO DE SURGIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

O surgimento da proteção de dados pessoais no contexto global está intimamente ligado às transformações tecnológicas e sociais que ocorreram ao longo do século XX. A crescente digitalização e a automação no processamento de dados impulsionaram a necessidade de regulamentação para garantir os direitos de privacidade dos indivíduos (DONEDA, 2010). A primeira grande iniciativa regulatória no campo da proteção de dados foi a Lei Estadual de Hesse (Alemanha) de 1970, considerada a primeira lei de proteção de dados do mundo, sendo um marco na história da legislação sobre o tema (BRASIL, 2021).

Nos anos 1980, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) publicou os Princípios sobre a Privacidade e Fluxos Transnacionais de Dados Pessoais, reforçando a necessidade de proteção contra o uso indevido de dados (OCDE, 1980). A OCDE recomendou que os países implementassem legislações específicas que limitassem a coleta e o tratamento de dados pessoais a fins específicos e legítimos. Conforme Abrusio (2020), os princípios internacionais estruturaram uma abordagem que assegura a privacidade e, simultaneamente, viabiliza a livre circulação de dados entre países.

Outro marco da evolução das normas de proteção de dados foi a Diretiva 95/46/CE da União Europeia, que, em 1995, estabeleceu regras abrangentes para o tratamento de dados pessoais, conferindo aos cidadãos europeus maior controle sobre suas informações e servindo de influência para as legislações posteriores a respeito do tema, ao passo que estabeleceu princípios como o da finalidade, transparência, necessidade e responsabilidade, que abriram caminho para o posterior reconhecimento da proteção de dados como um direito fundamental (UNIÃO EUROPEIA, 1995).

A grande revolução no campo da proteção de dados ocorreu com a criação do Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, conhecido internacionalmente pela sigla em inglês GDPR (*General Data Protection Regulation*), que entrou em vigor em 2018, estabelecendo que a proteção aos dados pessoais é um direito fundamental. Segundo Paul Lambert:

> o Regulamento Geral de Proteção de Dados (RGPD) é uma das legislações mais importantes para a União Europeia e para o mundo. (Lambert, 2017, p. 24).[2]

Nesse contexto, a LGPD surgiu como uma necessidade para alinhar o Brasil aos padrões internacionais de proteção de dados, estabelecendo regras claras sancionadoras para o tratamento de dados pessoais no país. A LGPD é, portanto, um reflexo das transformações globais na regulação da privacidade.

No cenário brasileiro, o trâmite para o surgimento e aprovação da Lei Geral de Proteção de Dados (LGPD) foi marcado por intensos debates legislativos e pela influência de normativas internacionais, como o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia. O processo legislativo teve início em 2010, com a abertura de consultas públicas pelo Ministério da Justiça para discutir uma possível regulamentação sobre proteção de dados. Após anos de debates, o Projeto de Lei nº 5.276/2016, de autoria do Poder Executivo, foi enviado à Câmara dos Deputados, onde passou por análise e modificações (BRASIL, 2018).

A urgência de o Brasil adotar uma legislação foi reforçada com a entrada em vigor da RGPD, em 2018, criando a necessidade do Brasil alinhar-se aos padrões internacionais a fim de viabilizar a participação de empresas brasileiras no mercado global. Em julho de 2018 o Senado Federal aprovou a LGPD e o então presidente Michel Temer sancionou-a em 14 de agosto de 2018, passando a entrar em vigor somente em setembro de 2020 (BRASIL, 2018). A criação da Autoridade Nacional de Proteção de Dados (ANPD), responsável por zelar, implementar e fiscalizar a aplicação da LGPD, prevista inicialmente no texto da lei, só foi formalizada posteriormente, por meio da medida provisória n° 869/2018, convertida na lei n° 13.853/2019, conferindo maior força ao marco regulatório (BRASIL, 2019).

Um dos principais doutrinadores da área, Danilo Doneda, diz o seguinte à respeito da proteção de dados e sua relevância:

> A proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental. (Doneda, 2011, p. 92).

Em meio a esse cenário internacional de proteção de dados pessoais, o surgimento da Lei Geral de Proteção de Dados no Brasil também é resultado de uma série de incidentes e vazamentos de dados, como os ocorridos nas eleições presidenciais dos Estados Unidos de 2016, em que houve um escândalo envolvendo a empresa Cambridge Analytica.

---

[2] *"The GDPR is one of the most important pieces of legislation for the European Union and for the world."* (LAMBERT, 2017, p. 24)

Episódio esse, em que a empresa teria comprado acesso a informações pessoais de usuários do *Facebook* e usado esses dados para criar um sistema que permitiu predizer e influenciar as escolhas dos eleitores nas urnas (G1, 2018). Esse cenário gerou um alerta global sobre a importância de proteger a privacidade e os direitos dos cidadãos, tornando a regulamentação da proteção de dados uma prioridade para muitos países, incluindo o Brasil.

A LGPD, portanto, é uma medida estratégica para fomentar a confiança do consumidor nas empresas brasileiras e promover um ambiente digital mais seguro e ético. Assim, é visível que além de colaborar para regulação de dados, a Lei Geral de Proteção de Dados também serve como instrumento garantidor de direitos fundamentais que estavam sem proteção legal após o surgimento da era digital, sendo esse principal direito fundamental o direito à privacidade, previsto no artigo 5°, inciso X, da Constituição Federal de 1988.

1.2 IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS

A proteção de dados vai além da esfera de privacidade. Os dados pessoais sustentam a economia digital, servindo para personalizar produtos e serviços, criar novos modelos de negócio e orientar decisões empresariais. Essa vantagem competitiva, porém, precisa vir acompanhada de responsabilidades legais e éticas, tais como: base legal, finalidade clara, minimização, transparência e segurança. Nesse sentido, alerta Bernard Marr:

> a mineração de dados não regulamentada acarreta um conjunto totalmente diferente de problemas — problemas de privacidade e também o desequilíbrio de poder causado pelo fato de a informação estar nas mãos de poucos, e não de muitos. (Marr, 2021, s.p.).[3]

Esse ponto reforça o que consumidores e autoridades esperam: tratamento responsável das informações, com clareza nas práticas, proteção contra abusos e prestação de contas pelas empresas.

[3] -"*Unregulated data-mining causes a whole different set of problems – privacy issues as well as the imbalance of power which is caused by information being in the hands of the few, rather than the many*." (MARR, 2021, s.p.).

No julgamento da Ação Direta de Inconstitucionalidade 6.387, Rel. Min. Rosa Weber, o Supremo Tribunal Federal reconheceu a existência de um direito fundamental autônomo à proteção de dados pessoais e à autodeterminação informacional. Vejamos a seguir:

> A proteção de dados pessoais se encontra no âmbito de tutela da cláusula constitucional da privacidade. Cuida-se de direito fundamental autônomo, que também se conecta, em rede, com a proteção à liberdade e ao livre desenvolvimento da personalidade. (BRASIL, STF, ADI 6387/DF, Rel. Min. Rosa Weber, Plenário, j. 07 maio 2020).

Assim, o Supremo Tribunal Federal já tinha declarado a proteção dos dados pessoais como um direito fundamental implícito na Constituição Federal, inserido na cláusula geral de privacidade, nos artigos 5º, incisos X e XII da Constituição Federal de 1988 (CRFB/88).

Posteriormente, a Emenda Constitucional nº 115, de 10 de fevereiro de 2022, positivou expressamente esse direito fundamental no art. 5º, inciso LXXIX, da Constituição Federal, ao dispor que: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” (BRASIL, 2022). Essa inserção representou um avanço notável, pois deslocou a proteção de dados para o nível constitucional mais elevado, reconhecendo-a como verdadeiro direito fundamental e, portanto, dotado de eficácia imediata e proteção reforçada.

Ao integrar o art. 5º da Constituição, a proteção de dados pessoais passa a ser considerada cláusula pétrea, nos termos do art. 60, §4º, IV, da Constituição, que impede sua supressão ou diminuição pelo poder constituinte derivado. Isso significa que, assim como outros direitos e garantias fundamentais, a tutela dos dados pessoais assume caráter permanente e imutável, compondo o núcleo essencial da ordem constitucional brasileira.

Assim, a constitucionalização explícita da proteção de dados consolida sua posição como condição para o exercício da liberdade, da autonomia e do livre desenvolvimento da personalidade, valores que já estavam na base da decisão do STF. Esse patamar reforçado projeta-se sobre a aplicação da Lei Geral de Proteção de Dados (LGPD), que concretiza o comando constitucional por meio de princípios e direitos específicos, destinados a garantir que o tratamento de informações pessoais ocorra de forma legítima, transparente, proporcional e segura.

Esses princípios, previstos no art. 6º da LGPD, constituem a espinha dorsal do regime protetivo, pois estabelecem parâmetros de legitimidade e responsabilidade no tratamento das informações pessoais. A finalidade, a adequação e a necessidade asseguram que o tratamento seja limitado a objetivos claros, legítimos e proporcionais; o livre acesso e a transparência garantem ao titular controle e clareza sobre o uso de seus dados; a qualidade e a segurança reforçam a confiabilidade das informações e a adoção de medidas contra acessos indevidos; a prevenção e a não discriminação impedem riscos e usos abusivos que possam gerar danos sociais; e, por fim, a responsabilização e prestação de contas consolidam a lógica da boa-fé e da governança de dados. Tais princípios são essenciais porque vinculam o tratamento de dados à proteção da dignidade, da privacidade e da liberdade, conferindo segurança jurídica às relações digitais e fortalecendo a confiança social no uso da informação.

2. DESAFIOS À ADEQUAÇÃO DA LGPD EM MICROEMPRESAS

2.1 LIMITAÇÕES ESTRUTURAIS E OPERACIONAIS DAS MICROEMPRESAS

A implementação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) nas microempresas encontra entraves estruturais significativos. As limitações de ordem material, como restrições orçamentárias, ausência de equipe técnica e escassez de tempo constituem os principais fatores que comprometem a efetiva aplicação da norma. Soma-se a isso a carência de conhecimento jurídico e tecnológico, que impede a correta interpretação das obrigações legais e a adoção de práticas de conformidade minimamente adequadas.

A Autoridade Nacional de Proteção de Dados (ANPD), ao editar a Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, reconheceu formalmente essa realidade, ao estabelecer regras específicas para os agentes de tratamento de pequeno porte. Entretanto, a redução de obrigações procedimentais não afasta a responsabilidade jurídica: mesmo com estrutura limitada, a microempresa deve ser capaz de demonstrar diligência e prestação de contas, conforme o princípio da *accountability* previsto no artigo 6º, inciso X, da LGPD (BRASIL, 2018).

Essa exigência evidencia o primeiro grande desafio: a lei pressupõe um nível mínimo de governança e formalização que, em geral, está distante da realidade operacional das microempresas. Os mesmos indivíduos que exercem atividades comerciais, administrativas e financeiras são também responsáveis por definir finalidades de tratamento, escolher a base jurídica, controlar registros e responder a solicitações de titulares. Essa sobrecarga funcional gera a impossibilidade prática de cumprir integralmente todas as obrigações legais.

A LGPD, todavia, impõe deveres objetivos e documentais. O artigo 37 determina o registro das operações de tratamento de dados pessoais, enquanto o artigo 46 obriga a adoção de medidas técnicas e administrativas aptas a proteger os dados desde a coleta até a eliminação (BRASIL, 2018). Tais dispositivos exigem organização mínima, independentemente do porte econômico. Ocorre que, nas microempresas, a ausência de estrutura tecnológica e de pessoal qualificado torna inviável o atendimento integral dessas disposições, o que compromete a efetividade normativa e revela um descompasso entre a intenção protetiva do legislador e a capacidade de execução do pequeno empreendedor.

A regulamentação buscou mitigar essas barreiras por meio de medidas de simplificação. A Resolução nº 2/2022 prevê um modelo oficial de registro simplificado (art. 9º) e dispensa da nomeação do encarregado, desde que exista canal de comunicação com o titular (art. 11, §§ 1º e 2º). Também orienta que as medidas adotadas sejam proporcionais e compatíveis com a realidade do agente de tratamento (art. 12). Embora tais soluções representem avanço, sua eficácia prática depende de um nível mínimo de consciência organizacional. Sem reflexão sobre necessidade, adequação e transparência, corre-se o risco de uma adequação meramente formal, o chamado *"cumprimento de formulário"*, incapaz de garantir proteção efetiva ou de sustentar defesa em caso de fiscalização ou litígio.

Nesse cenário, constata-se que as microempresas enfrentam desafios estruturais, econômicos e cognitivos que comprometem a aplicação uniforme da LGPD. A flexibilização normativa foi um passo necessário, mas não suficiente.

Em síntese, o desafio da adequação das microempresas à LGPD reside em conciliar a proporcionalidade com a efetividade. Não se trata de replicar modelos corporativos, mas de estabelecer um núcleo mínimo de governança que permita comprovar diligência. Assim, é possível preservar o princípio da responsabilidade, reduzir a improvisação e garantir que a proteção de dados pessoais não se torne um privilégio das grandes organizações.

2.2 ACCOUNTABILITY E REGISTROS DE CONFORMIDADE

Entre os maiores desafios para a efetiva implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas microempresas está a materialização do princípio da *accountability*, ou responsabilização e prestação de contas. Trata-se de um dever que transcende a mera obediência formal à lei, exigindo a capacidade de comprovar, de forma documentada e transparente, que as práticas adotadas são compatíveis com os princípios e as bases legais do tratamento de dados.

O artigo 6º, inciso X, da LGPD consagra expressamente o princípio da responsabilização e prestação de contas, determinando que o agente de tratamento deve "demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais" (BRASIL, 2018). Essa disposição, inspirada no Regulamento Geral de Proteção de Dados da

União Europeia (GDPR), representa a transição de um modelo reativo, baseado em punições, para um modelo proativo de governança, em que a conformidade é comprovada continuamente. Contudo, nas microempresas, a ausência de estrutura administrativa impede que esse ideal se concretize de modo efetivo.

A Resolução CD/ANPD nº 2/2022, ao reconhecer a dificuldade dos agentes de pequeno porte, buscou adaptar as exigências do artigo 37 da LGPD, que prevê o registro das operações de tratamento de dados pessoais. Assim, a norma criou um registro simplificado, que dispensa planilhas complexas e ferramentas de gestão automatizadas, permitindo a utilização de formulários básicos. Apesar dessa flexibilização, o desafio persiste, já que é comum que as microempresas sequer tenham clareza sobre o ciclo de vida dos dados que coletam, não distinguindo adequadamente fases de coleta, armazenamento, compartilhamento e descarte. Essa lacuna compromete a rastreabilidade das decisões e, consequentemente, a prova de conformidade.

Do ponto de vista jurídico, a *accountability* não se limita à documentação de atos administrativos, mas envolve a justificativa das decisões tomadas no tratamento de dados. Cada escolha, desde a definição da base legal até o prazo de retenção das informações deve ser racionalmente explicável à luz dos princípios da finalidade, necessidade e adequação (BRASIL, 2018, art. 6º, I a III). Nas microempresas, essa racionalidade muitas vezes é substituída pela informalidade típica da gestão cotidiana. O pequeno empresário, movido pela urgência operacional, tende a priorizar a continuidade da atividade econômica, deixando a proteção de dados a um segundo plano. Essa postura, ainda que compreensível, fragiliza o cumprimento da lei e expõe a empresa a riscos de responsabilização.

É importante destacar que a prestação de contas possui dimensão dupla: interna e externa. Internamente, implica a criação de rotinas mínimas de controle e verificação das práticas de tratamento, como planilhas simplificadas, relatórios periódicos e políticas resumidas. Externamente, refere-se à capacidade de responder adequadamente às autoridades e aos titulares, fornecendo informações claras sobre o uso dos dados. Para as microempresas, ambas as dimensões são desafiadoras. Internamente, por falta de tempo e capacitação e externamente, por ausência de procedimentos padronizados e de linguagem acessível para comunicar políticas de privacidade.

Nesse sentido, Danilo Doneda diz:

> A dificuldade em registrar as operações e manter a coerência entre o discurso e a prática produz o fenômeno da responsabilidade aparente (Doneda, 2010, p. 37).

Dessa forma, o agente demonstra formalmente cumprimento, mas sem efetividade material. Na prática, isso se traduz em políticas genéricas copiadas da internet, sem vínculo com os reais fluxos de tratamento da organização. Esse modelo de “conformidade de fachada” é incompatível com o espírito da LGPD, que exige compromisso substancial com a proteção da pessoa humana e não mera formalidade burocrática.

Do ponto de vista teórico, a *accountability* representa um instrumento de concretização da boa administração pública e privada, vinculada ao princípio da transparência e ao dever de confiança nas relações econômicas. Ao exigir que o agente prove que cumpre a lei, a LGPD inverte a lógica da presunção de inocência administrativa e impõe uma nova cultura de responsabilidade.

Em conclusão, essa inversão, embora coerente com a finalidade da norma, é particularmente onerosa para as microempresas, que operam em ambientes informais e com baixa capacidade de registro. O desafio, portanto, não é apenas técnico, mas cultural: instaurar uma mentalidade de governança onde antes prevalecia a informalidade.

2.3 SEGURANÇA DA INFORMAÇÃO E GESTÃO DE TERCEIROS

A segurança da informação constitui um dos eixos estruturantes da proteção de dados pessoais e representa, para as microempresas, um dos pontos mais críticos da adequação à Lei nº 13.709/2018. O artigo 46 da LGPD estabelece que os agentes de tratamento devem adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado (BRASIL, 2018). Essa obrigação, embora genérica, traduz o princípio da prevenção e o dever de cuidado contínuo na manipulação de informações.

Entretanto, no universo das microempresas, a implementação de práticas seguras enfrenta barreiras práticas e econômicas. Tais organizações geralmente não

dispõem de infraestrutura tecnológica robusta, nem de equipe qualificada para avaliar riscos cibernéticos ou configurar políticas de segurança da informação. As operações são realizadas em sistemas simples e muitas vezes sem criptografia, controle de acesso ou backup regular, o que aumenta a exposição a incidentes. Assim, a aplicação do artigo 46 deve ser lida sob o prisma da proporcionalidade e da capacidade operacional do agente, sem descaracterizar o dever jurídico de proteção.

A Resolução CD/ANPD nº 2/2022, ao regular os agentes de pequeno porte, reforça esse entendimento. O artigo 12 determina que as medidas de segurança adotadas devem ser “essenciais e necessárias”, consideradas as peculiaridades do agente. Essa diretriz não significa redução da responsabilidade, mas adequação da exigência ao contexto. O pequeno empreendedor não está obrigado a adotar soluções tecnológicas avançadas, mas deve demonstrar boas práticas proporcionais: controle de senhas, atualização de softwares, limitação de acessos, cópias de segurança e treinamento básico da equipe. São condutas simples, porém eficazes, que materializam o dever de diligência e minimizam riscos de vazamentos.

O problema central, contudo, não reside apenas na limitação de recursos, mas na ausência de cultura organizacional voltada à segurança da informação. Em microempresas, a tecnologia é tratada como ferramenta operacional, e não como ativo estratégico. A proteção de dados é vista como um custo e não como parte da reputação empresarial. Essa percepção reduz a prioridade das medidas preventivas e agrava a vulnerabilidade a ataques cibernéticos e fraudes. Assim, mais do que tecnologia, o desafio está na mudança de mentalidade, com a incorporação da segurança como valor institucional.

O risco de incidentes é amplificado pela forma como as microempresas se relacionam com terceiros e fornecedores. Frequentemente, essas organizações dependem de prestadores externos para o tratamento de dados, como serviços de contabilidade, marketing digital, hospedagem de sites, plataformas de pagamento e armazenamento em nuvem. Nesses casos, o artigo 39 da LGPD (BRASIL, 2018) impõe que o operador trate os dados “conforme as instruções do controlador”, o que exige que os contratos estabeleçam cláusulas específicas de confidencialidade, finalidades e responsabilidades. Todavia, a realidade mostra que a maioria das microempresas não dispõe de assessoria jurídica para revisar contratos ou exigir garantias de segurança de seus parceiros.

Essa carência gera uma zona de incerteza jurídica: quando ocorre um vazamento, torna-se difícil delimitar a responsabilidade entre o controlador (a microempresa) e o operador (o prestador de serviço).

A gestão da cadeia de terceiros, portanto, é componente essencial da segurança da informação. Mesmo em estruturas reduzidas, é possível adotar medidas básicas de controle contratual, como cláusulas de confidencialidade, proibição de compartilhamento não autorizado, obrigação de notificação imediata em caso de incidente e previsão de sanções. A ANPD, em seus guias orientativos, recomenda que os agentes de pequeno porte priorizem fornecedores que já possuam políticas de privacidade e segurança estabelecidas, reduzindo o risco de corresponsabilidade. Assim, a adoção de critérios mínimos de seleção e o acompanhamento contínuo das práticas desses terceiros configuram uma forma de mitigação de risco compatível com o porte da organização.

2.4 ATENDIMENTO AOS TITULARES E RISCOS JURÍDICOS REPUTACIONAIS

O atendimento aos direitos dos titulares constitui dimensão essencial da efetividade da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e representa, para as microempresas, um dos maiores desafios práticos de adequação. O artigo 18 da LGPD garante ao titular o direito de obter do controlador, a qualquer momento e mediante requisição, informações sobre o tratamento de seus dados pessoais, incluindo confirmação de existência, acesso, correção, anonimização, portabilidade e eliminação (BRASIL, 2018). A norma impõe, portanto, um dever de transparência ativa e responsiva, cuja observância depende de organização documental, tempo e conhecimento jurídico.

Na prática, o exercício dos direitos dos titulares revela o conflito entre a amplitude protetiva da lei e a capacidade operacional do pequeno agente econômico. A Resolução CD/ANPD nº 2/2022, ao tratar do tema, reconhece a necessidade de simplificação e permite prazos e procedimentos diferenciados, desde que se mantenha a efetividade do direito de resposta (art. 14). Contudo, essa flexibilização não resolve o problema estrutural: a falta de procedimentos padronizados faz com que cada solicitação seja tratada de forma improvisada, gerando respostas incompletas,

atrasadas ou incoerentes. Tal cenário não apenas frustra a finalidade protetiva da norma, mas também expõe o agente a riscos jurídicos e reputacionais relevantes.

O impacto jurídico dessa inviabilidade é expressivo. O não atendimento, ou o atendimento inadequado ao titular, configura violação de dever legal, podendo ensejar sanções administrativas previstas no artigo 52 da LGPD, além de eventual responsabilização civil nos termos do artigo 42. O referido artigo 52 prevê, entre as penalidades, advertência, multa simples, multa diária, bloqueio ou eliminação dos dados pessoais, e até mesmo publicização da infração (BRASIL, 2018).

Em se tratando de agentes de pequeno porte, a Resolução CD/ANPD nº 4/2023 estabeleceu critérios específicos para o cálculo e a gradação das penalidades, em conformidade com o princípio da proporcionalidade. Nos termos do artigo 52, inciso II, da Lei nº 13.709/2018, a multa simples pode alcançar até 2% do faturamento da pessoa jurídica, grupo ou conglomerado no Brasil, limitada a R$ 50 milhões por infração. A resolução mencionada detalha os parâmetros para fixação da sanção, permitindo que a Autoridade Nacional de Proteção de Dados (ANPD) reduza percentuais e valores em função da receita bruta anual e da gravidade da conduta. Na prática, as penalidades aplicáveis às microempresas tendem a ser significativamente inferiores, de modo a compatibilizar a responsabilização com a capacidade econômica e o impacto social do agente.

Mesmo em percentuais aparentemente baixos, o impacto financeiro sobre microempresas é expressivo. Uma multa equivalente a 1% do faturamento pode comprometer a continuidade de atividades e inviabilizar investimentos. Ademais, o bloqueio temporário ou a eliminação de dados pessoais, medidas também previstas na LGPD, podem afetar diretamente a operação do negócio, especialmente quando os dados constituem o núcleo de suas atividades, como em *e-commerces*, clínicas ou prestadores de serviço digital.

Deve-se considerar, ainda, que o atendimento deficiente aos titulares constitui fator de ampliação do risco reputacional, uma vez que o cidadão tende a associar o descumprimento da LGPD à falta de ética ou transparência empresarial. Em tempos de comunicação instantânea e exposição digital, a imagem de uma organização pode ser comprometida por um único incidente mal gerido. Nesse contexto, a proteção de dados pessoais deixa de ser mera obrigação legal e passa a integrar o patrimônio reputacional da empresa, funcionando como critério de confiança e diferencial

competitivo, não devendo, portanto, ser vista como um obstáculo burocrático, mas como um instrumento de proteção jurídica e fortalecimento da confiança.

3. MEDIDAS FACILITADORAS E PERSPECTIVAS DE ADEQUAÇÃO DAS MICROEMPRESAS À LGPD

3.1 PAPEL INSTITUCIONAL DA ANPD E INCENTIVOS À CONFORMIDADE

A efetiva implementação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) depende, em grande medida, do desempenho institucional da Autoridade Nacional de Proteção de Dados (ANPD), criada pela Lei nº 13.853/2019. Como órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, a ANPD exerce função não apenas sancionadora, mas também pedagógica, essencial à consolidação de uma cultura de proteção de dados em um país marcado por desigualdades estruturais. Para viabilizar a adequação das microempresas, a autoridade editou a Resolução CD/ANPD nº 2/2022, que instituiu tratamento jurídico diferenciado para agentes de pequeno porte, contemplando medidas como registro simplificado, dispensa do encarregado e procedimentos proporcionais de atendimento aos titulares, incorporando o princípio da proporcionalidade e da boa-fé regulatória.

No mesmo sentido, a Resolução CD/ANPD nº 4/2023, que regulamenta o processo administrativo sancionador e a dosimetria das penalidades, reforçou o caráter educativo da atuação institucional ao prever a possibilidade de redução das multas conforme o porte econômico, a gravidade da infração e o grau de colaboração. Essas diretrizes demonstram que a função da ANPD vai além da repressão, buscando equilibrar a efetividade da LGPD com a viabilidade econômica dos pequenos negócios. A autoridade também desempenha papel orientador por meio da publicação de guias técnicos e materiais explicativos, como o Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte (2022), que traduzem a linguagem normativa em orientações práticas e acessíveis.

Portanto, para as microempresas, a ANPD deve representar não apenas um agente sancionador, mas um vetor de apoio técnico e educativo, capaz de traduzir obrigações legais em práticas exequíveis.

3.2 ESTRATÉGIAS DE ADEQUAÇÃO SIMPLES E PROPORCIONAIS

A adequação das microempresas à LGPD pode ser alcançada por meio de medidas simples, proporcionais e de baixo custo. A primeira medida que pode ser adotada, consiste na elaboração de uma política de privacidade clara e objetiva, que

descreva quais dados são coletados, a finalidade do tratamento e os direitos dos titulares. Em seguida, é recomendável manter um registro simplificado das operações de tratamento, conforme autoriza a Resolução CD/ANPD nº 2/2022, o que pode ser feito por meio de planilhas ou formulários digitais. Esse registro deve conter informações básicas como a base legal utilizada, o período de retenção dos dados e o responsável pelo tratamento. A criação de um canal de comunicação acessível ao titular e o uso de formulários padrão para responder solicitações também demonstram transparência e boa-fé e são boas medidas de adequação a serem adotadas.

No campo técnico, as microempresas devem adotar medidas operacionais essenciais, como controle de acesso a arquivos, utilização de senhas fortes, atualização de softwares, realização de cópias de segurança e orientação dos colaboradores sobre sigilo e descarte seguro de informações. A inserção de cláusulas de confidencialidade e de notificação de incidentes nos contratos com terceiros é igualmente importante para reduzir riscos e delimitar responsabilidades. A adoção dessas práticas, ainda que simples, cumpre o disposto nos artigos 46 e 49 da LGPD (BRASIL, 2018), reforça a cultura de prevenção e evidencia diligência perante a Autoridade Nacional de Proteção de Dados (ANPD). Dessa forma, a conformidade torna-se possível sem comprometer a sustentabilidade econômica, equilibrando segurança jurídica e viabilidade empresarial.

CONCLUSÃO

A análise desenvolvida ao longo deste trabalho permitiu constatar que a implementação efetiva da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) enfrenta obstáculos significativos no contexto das microempresas brasileiras. Embora a LGPD represente um marco normativo essencial para a consolidação do direito fundamental à privacidade e para o fortalecimento da confiança nas relações digitais, sua aplicação uniforme, sem considerar as desigualdades estruturais entre os agentes econômicos, compromete a efetividade do sistema de proteção de dados.

O estudo demonstrou que as limitações estruturais, financeiras e cognitivas são os principais entraves à conformidade. A escassez de recursos, a falta de pessoal especializado e o déficit de conhecimento técnico-jurídico tornam inviável a implementação integral das exigências legais. Ainda que a Resolução CD/ANPD nº 2/2022 tenha instituído um tratamento jurídico diferenciado para agentes de pequeno porte, incluindo as microempresas, persistem desafios relacionados à ausência de cultura organizacional voltada à segurança da informação e à dificuldade de manutenção de registros e políticas internas.

Conclui-se que a efetividade da LGPD nas microempresas depende diretamente da atuação pedagógica e proporcional da Autoridade Nacional de Proteção de Dados (ANPD). O papel da autoridade deve ir além da fiscalização e da aplicação de sanções: é indispensável que atue como agente de apoio técnico, promotor da educação digital e indutor de boas práticas de governança. A política regulatória voltada a esse segmento deve priorizar a orientação, a simplificação e a capacitação, reconhecendo as limitações econômicas que caracterizam as microempresas.

As estratégias de adequação simples e proporcionais, como registros básicos das operações, políticas de privacidade acessíveis, controle mínimo de acesso a dados e procedimentos padronizados de atendimento aos titulares, revelaram-se juridicamente suficientes para atender ao princípio da *accountability*, desde que executadas com boa-fé e coerência. O modelo de conformidade deve, portanto, privilegiar a prova de diligência e não a complexidade formal.

Por fim, verifica-se que a consolidação da proteção de dados pessoais no ambiente das microempresas requer equilíbrio entre a proteção dos direitos

fundamentais e a viabilidade econômica dos pequenos negócios. A aplicação da LGPD não pode se tornar um fator de exclusão produtiva, mas sim um instrumento de fortalecimento institucional e de credibilidade social. Assim, a adequação das microempresas à LGPD deve ser compreendida como um processo gradual, baseado em educação, proporcionalidade e apoio institucional, capaz de assegurar que a proteção de dados pessoais seja um valor democrático acessível a todos os agentes econômicos.

REFERÊNCIAS:

ALMEIDA, S. C. D.; SOARES, T. A. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. *Perspectivas em Ciência da Informação*, v. 27, n. 3, p. 26 – 45, jul./set. 2022. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/. Acesso em: 2 out. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo de segurança da informação para agentes de tratamento de pequeno porte*. Brasília: ANPD, 2022.

BLUM, Renato Opice; NÓBREGA, Viviane. *LGPD comentada: Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018.* Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*, Brasília, DF, 15 ago. 2018.

BRASIL. *Lei nº 13.853, de 8 de julho de 2019.* Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a Autoridade Nacional de Proteção de Dados e dá outras providências. *Diário Oficial da União*, Brasília, DF, 9 jul. 2019.

BRASIL. *Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.* Dispõe sobre a aplicação da Lei nº 13.709, de 14 de agosto de 2018, para agentes de tratamento de pequeno porte. *Diário Oficial da União*, Brasília, DF, 28 jan. 2022.

BRASIL. *Resolução CD/ANPD nº 4, de 24 de maio de 2023.* Dispõe sobre o processo administrativo sancionador e o cálculo do valor-base das sanções de multa. *Diário Oficial da União*, Brasília, DF, 25 maio 2023.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade 6387/DF.* Rel. Min. Rosa Weber. Plenário, julgado em 07 maio 2020. Disponível em: https://jurisprudencia.stf.jus.br/. Acesso em: 2 out. 2025.

KOHLS, Cleize. *LGPD: Lei Geral de Proteção de Dados Pessoais – teoria e prática.* São Paulo: Saraiva Educação, 2021.

DONEDA, Danilo. *A proteção de dados pessoais nas relações de consumo: para além da informação creditícia.* Brasília: Ministério da Justiça, Secretaria de Direito Econômico, Departamento de Proteção e Defesa do Consumidor, 2010.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Revista Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91–108, jul./dez. 2011.

IDEc – INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. *Manual LGPD para micro e pequenas empresas.* São Paulo: IDEC, 2021. Disponível em: https://idec.org.br/. Acesso em: 2 out. 2025.

LAMBERT, Paul. *Understanding the GDPR: a practical guide to the General Data Protection Regulation.* London: Routledge, 2018.

LAMBERT, Paul. *Understanding the new European data protection rules.* Boca Raton: CRC Press, 2017.

MARR, Bernard. Here's why data is not the new oil. *Bernard Marr*, 2 jul. 2021. Disponível em: https://bernardmarr.com/heres-why-data-is-not-the-new-oil/. Acesso em: 2 out. 2025.

MARTINS, Renato Leite; MONTEIRO, Bruna; GOMES, Matheus. *Privacidade e proteção de dados pessoais: comentários à Lei nº 13.709/2018 (LGPD).* São Paulo: Método, 2019.

MEDEIROS, Júlia Ribeiro; REZENDE, Pedro Henrique. *Manual de proteção de dados pessoais: fundamentos e aplicações práticas da LGPD.* Rio de Janeiro: Forense, 2020.

OPICE BLUM, Renato; NÓBREGA, Viviane; BLUM, Renato. *Proteção de dados e privacidade: a nova Lei Brasileira de Proteção de Dados Pessoais.* São Paulo: Revista dos Tribunais, 2019.

SOUZA, Adriano Mendes de. *LGPD na prática para micro e pequenas empresas.* São Paulo: Literare Books International, 2021.