REVISTA DA MICRO E PEQUENA EMPRESA
Vol. 19, No. 1, Jan-Abr 2025, p.01-20
ISSN: 2237-3713

Diretrizes para aplicação da LGPD em sistemas de software de pequeno porte*

Guidelines for applying the LGPD to small-scale software systems

Júlio César Ferreira Pedrini
Universidade de Vassouras
juliocesarfp8@gmail.com

Matheus Almeida de Carvalho
Universidade Federal Fluminense
ac_matheus18@hotmail.com

RESUMO

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) em sistemas utilizados por agentes de tratamento de pequeno porte apresenta desafios decorrentes de restrições financeiras, técnicas e organizacionais. Nesse contexto, o objetivo deste estudo é analisar as implicações da LGPD e da Resolução CD/ANPD nº 2/2022 e propor práticas simplificadas de proteção de dados. Para tanto, realizou-se uma pesquisa qualitativa, de natureza teórico-aplicada, baseada em análise documental da legislação e regulamentação aplicáveis, pesquisa bibliográfica e síntese aplicada, mediante categorização dos requisitos identificados. Os resultados indicam que as flexibilizações aplicáveis aos agentes de pequeno porte não afastam a proteção de dados, mas permitem a adoção de medidas proporcionais aos riscos e à capacidade operacional. A minimização de dados, a privacidade por padrão, o controle de acesso, a transparência e a proteção desde a concepção podem favorecer uma implementação pragmática e tecnicamente viável dos requisitos de proteção de dados em sistemas de menor porte.

Palavras-chave: Agentes de tratamento de pequeno porte. Privacidade. Segurança da informação. Proteção de dados pessoais. Conformidade regulatória.

ABSTRACT

The application of the Brazilian General Data Protection Law (LGPD) to systems used by small-scale data processing agents presents challenges arising from financial, technical, and organizational constraints. In this context, this study aims to analyze the implications of the LGPD and ANPD Resolution CD/ANPD No. 2/2022 and to propose simplified data protection practices. To this end, a qualitative, theoretically applied study was conducted based on documentary analysis of the applicable legislation and regulatory framework, a literature review, and an applied synthesis involving the categorization of the identified requirements. The results indicate that the flexibilities applicable to small-scale data processing agents do not exempt them from data protection requirements but allow for the adoption of measures proportionate to the risks involved and their operational capacity. Data minimization, privacy by default, access control, transparency, and data protection from the design stage can support a pragmatic and technically feasible implementation of data protection requirements in smaller-scale systems.

* Recebido em 29 de novembro de 2024, aprovado em 09 de julho de 2025, publicado em 31 de agosto de 2025.

Keywords: Small-scale data processing agents. Privacy. Information security. Personal data protection. Regulatory compliance.

1. INTRODUÇÃO

A transformação digital modificou a forma como organizações de diferentes portes coletam, armazenam e processam informações. Nas micro e pequenas empresas (MPEs), sistemas informatizados passaram a cumprir funções antes realizadas manualmente, como cadastro de clientes, agendamento, emissão de documentos e gestão financeira. Como consequência, mesmo sistemas relativamente simples podem envolver tratamento de dados pessoais e inserir a organização no campo de aplicação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

A LGPD estabeleceu um marco jurídico para o tratamento de dados pessoais no Brasil, fundamentado na proteção dos direitos de liberdade e privacidade e no livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018). Sua abrangência não está condicionada ao porte econômico da organização: a dimensão reduzida de uma empresa não elimina, por si só, a necessidade de observar os requisitos legais aplicáveis ao tratamento de dados pessoais.

Esse aspecto é particularmente relevante para as MPEs, cuja capacidade de implementar mecanismos de governança e segurança costuma diferir da observada em organizações com equipes jurídicas e departamentos de tecnologia dedicados. Estudos anteriores já apontavam dificuldades técnicas enfrentadas por micro e pequenas empresas na adequação à LGPD, ao mesmo tempo em que destacavam a necessidade de traduzir conceitos jurídicos para uma linguagem acessível a organizações com estrutura operacional reduzida (TRISTÃO et al., 2021; DINIZ et al., 2021).

Essa dificuldade não configura incompatibilidade entre proteção de dados e pequeno porte empresarial. A Autoridade Nacional de Proteção de Dados (ANPD), por meio da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, estabeleceu regras específicas para agentes de tratamento de pequeno porte (ATPPs), contemplando microempresas, empresas de pequeno porte, startups e determinados entes que realizam tratamento de dados pessoais, condicionadas ao porte econômico e ao risco do tratamento. O art. 6º do regulamento deixa expresso que a dispensa ou flexibilização de obrigações não exime os ATPPs do cumprimento das demais disposições da LGPD, incluindo bases legais, princípios e direitos dos titulares (BRASIL,

2022). A simplificação regulatória constitui, portanto, mecanismo de adequação proporcional, e não autorização para tratar dados sem controles de privacidade e segurança.

Essa distinção é central quando a legislação é traduzida para o desenvolvimento de software. Um sistema de pequeno porte não precisa reproduzir a estrutura de governança de uma grande organização para incorporar princípios de proteção de dados, mas sua arquitetura, seus formulários, suas permissões de acesso e seus processos de manutenção devem considerar, desde a concepção, os riscos associados ao tratamento realizado.

Quanto ao alcance concreto dessa flexibilização, o art. 9º da Resolução prevê que os ATPPs podem cumprir de forma simplificada a obrigação de registro das operações de tratamento (art. 37 da LGPD), sem que isso configure dispensa dessa obrigação. De modo semelhante, os arts. 12 e 13 não estabelecem dispensa geral de elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD). A Resolução também dispensa a indicação de encarregado, desde que seja disponibilizado canal de comunicação com o titular, e permite política simplificada de segurança da informação, considerando custos, estrutura, escala e volume das operações (BRASIL, 2022). A norma não isenta o pequeno agente de adotar medidas de segurança: determina a adoção de medidas essenciais e necessárias, proporcionais ao risco e à realidade da organização.

A própria regulamentação estabelece limites a esse tratamento diferenciado. O art. 3º exclui do regime os agentes que realizem tratamento de alto risco ou ultrapassem os limites de receita aplicáveis, e o art. 4º apresenta critérios para caracterização do alto risco, incluindo tratamento em larga escala, uso de tecnologias emergentes, vigilância de áreas públicas, decisões automatizadas e utilização de dados sensíveis ou de crianças, adolescentes e idosos. Consequentemente, "sistema de pequeno porte" não deve ser tratado como sinônimo de "sistema de baixo risco": as diretrizes discutidas neste trabalho destinam-se ao contexto delimitado pela pesquisa e não constituem autorização geral para redução de controles independentemente da natureza do tratamento.

Nesse cenário, o Privacy by Design (PbD), desenvolvido por Ann Cavoukian, oferece uma abordagem útil para conectar os requisitos jurídicos às decisões de engenharia de software, ao propor que a privacidade seja considerada desde a concepção dos sistemas, e não incorporada apenas depois da implementação (CAVOUKIAN, 2009). O art. 6º da LGPD, por sua vez, estabelece princípios que devem orientar o tratamento, entre eles finalidade, adequação,

necessidade, transparência e segurança (BRASIL, 2018); a seção 2 retoma esses fundamentos de maneira articulada com a literatura sobre pequenas empresas.

A partir desse enquadramento, o problema investigado neste artigo pode ser formulado da seguinte maneira: como os princípios da LGPD e as flexibilizações da Resolução CD/ANPD nº 2/2022 podem ser traduzidos em práticas técnicas de Privacy by Design e segurança da informação adequadas à realidade de sistemas de pequeno porte? A pergunta não pretende determinar se uma MPE está juridicamente "em conformidade" em sentido amplo, uma vez que tal conclusão dependeria da análise concreta das atividades de tratamento e de outros elementos que extrapolam a arquitetura do software. Seu propósito é mais delimitado: identificar requisitos e práticas técnicas que possam contribuir para uma proteção de dados proporcional e operacionalmente viável.

O objetivo geral deste trabalho é analisar as implicações da LGPD e da Resolução CD/ANPD nº 2/2022 para o desenvolvimento de sistemas de pequeno porte e propor práticas de Privacy by Design e segurança da informação tecnicamente aplicáveis e compatíveis com restrições de recursos. Como objetivos específicos, busca-se: (i) identificar os requisitos da LGPD com implicações diretas sobre sistemas de software utilizados por ATPPs; (ii) examinar as flexibilizações e obrigações da Resolução CD/ANPD nº 2/2022; (iii) relacionar princípios de Privacy by Design a requisitos técnicos de privacidade e segurança; e (iv) sintetizar diretrizes simplificadas que possam orientar desenvolvedores e pequenos negócios na incorporação desses requisitos ao ciclo de desenvolvimento e operação de sistemas.

A pesquisa é de natureza qualitativa e combina análise documental da legislação e da regulamentação da ANPD, pesquisa bibliográfica sobre proteção de dados, Privacy by Design e realidade organizacional das MPEs, e um procedimento de síntese aplicada, sem presumir que as medidas técnicas resultantes sejam, isoladamente, suficientes para caracterizar conformidade jurídica integral. A relevância do estudo decorre da necessidade de aproximar três dimensões frequentemente tratadas de forma separada: regulação, capacidade organizacional e engenharia de software. É nessa articulação que reside a contribuição pretendida deste trabalho.

As seções seguintes apresentam a revisão de literatura sobre LGPD, tratamento diferenciado dos ATPPs, Privacy by Design e realidade das MPEs; descrevem o percurso metodológico; apresentam a síntese das diretrizes técnicas propostas; e discutem suas implicações e limitações.

2. REVISÃO DE LITERATURA

2.1 LGPD, tratamento diferenciado e Privacy by Design

O art. 6º da LGPD estabelece princípios que devem orientar as atividades de tratamento de dados pessoais, entre eles finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização (BRASIL, 2018). Para sistemas de pequeno porte, alguns desses princípios têm implicações diretas sobre arquitetura e experiência de uso. O princípio da necessidade, por exemplo, fornece base normativa para questionar a coleta indiscriminada de dados: se determinada informação não é necessária à finalidade pretendida, sua inclusão no sistema carece de justificativa técnica e jurídica. A segurança, por sua vez, não deve depender exclusivamente de procedimentos administrativos externos ao software; controles de acesso, autenticação, registros e backups podem integrar a própria arquitetura da solução.

A Resolução CD/ANPD nº 2/2022, examinada na íntegra e em sua redação vigente (atualizada pela Resolução CD/ANPD nº 15/2024, relativa à comunicação de incidentes de segurança), associa segurança e proteção de dados à realidade operacional do agente. A norma não dispensa a organização pequena de adotar medidas de segurança: determina a adoção de medidas essenciais e necessárias, considerando o risco e as características da organização, e permite política simplificada de segurança da informação, levando em conta custos, estrutura, escala e volume das operações (BRASIL, 2022). A proporcionalidade, portanto, não significa ausência de controles, mas adequação dos controles às circunstâncias concretas.

O Privacy by Design (PbD), sistematizado por Cavoukian (2009), propõe que a privacidade seja considerada desde a concepção dos sistemas e processos, e não incorporada apenas após a implementação. O framework é organizado em sete princípios: atuação proativa e preventiva, privacidade como configuração padrão, incorporação da privacidade ao design, proteção durante todo o ciclo de vida da informação, funcionalidade total, visibilidade e transparência, e respeito à privacidade do usuário. A aproximação entre PbD e LGPD não significa que o framework substitua a análise jurídica; neste trabalho, o PbD é tratado como abordagem de engenharia e governança capaz de auxiliar na operacionalização de princípios legais, traduzindo minimização, configuração padrão, controle do ciclo de vida, transparência e segurança em requisitos concretos de software.

2.2 MPEs, capacidade organizacional e adoção tecnológica

A literatura recente sobre pequenas empresas oferece evidência contextual relevante para compreender as condições em que a proteção de dados precisa ser implementada, ainda que nenhum dos estudos a seguir investigue diretamente a LGPD. Batista, Arouca e Lobato (2024), ao analisarem estratégias de digitalização comunicacional em micro e pequenas empresas de Santarém (PA) por meio de pesquisa bibliográfica, documental e pesquisa-ação, identificaram que a disponibilidade de tecnologias não implica seu aproveitamento pleno: barreiras relacionadas à falta de treinamento e de tempo para planejamento estratégico, somadas a pressões mercadológicas e concorrenciais, limitam a digitalização, ainda que exista potencial de ganho competitivo mediante uso planejado de mídias digitais.

Alves e Nodari (2023), em revisão sistemática nas bases Scopus e Web of Science, identificaram quatro dimensões associadas à inovação frugal em pequenas e médias empresas (agregação de valor, otimização de processos, capital humano e modelo de negócios), sugerindo que soluções sustentáveis em organizações com recursos limitados tendem a exigir priorização e definição clara dos elementos de maior valor. Esse achado não permite concluir que minimização de dados equivalha a inovação frugal, mas autoriza uma aproximação conceitual restrita: a identificação de controles essenciais, proporcionais ao risco, é compatível com a lógica de otimização de recursos discutida pelas autoras.

A capacidade de transformar princípios abstratos em procedimentos executáveis também depende de fatores cognitivos e organizacionais. Lima e Silva (2024), em estudo exploratório com entrevistas semiestruturadas junto a pequenos empresários, verificaram que o desconhecimento sobre o escopo e o valor da consultoria jurídico-tributária constituía a principal razão para sua não contratação. Esse achado, transposto por analogia ao campo da proteção de dados, sugere que recomendações técnicas excessivamente abstratas podem ter baixa efetividade quando os responsáveis pelo sistema não compreendem sua operacionalização. Gonçalves et al. (2023), ao analisarem o crescimento de uma pequena empresa ao longo de dezoito anos, observaram alterações nos ciclos decisórios em resposta a pressões internas e externas e associaram a ascensão de gestores intermediários a maior propensão à inovação sem abandono da eficiência, evidenciando que processos organizacionais em pequenas empresas nem sempre seguem modelos formais de planejamento.

Alves, Aires e Salgado (2023), em estudo de caso sobre o Programa Agentes Locais de Inovação em micro e pequenas empresas do Rio Grande do Norte, analisaram doze ações mediante pesquisa documental, entrevistas semiestruturadas e o modelo VRIO, identificando

que seis apresentaram potencial de gerar vantagem competitiva (uma sustentável e cinco temporárias). O estudo demonstra que intervenções dirigidas a pequenos negócios produzem efeitos heterogêneos, o que recomenda cautela ao associar automaticamente uma prática, ainda que tecnicamente adequada, a ganhos competitivos. Por fim, Silva et al. (2024), em estudo quantitativo com 376 consumidores de produtos de segunda mão comercializados por pequenos negócios, verificaram influência positiva da comunicação em mídias sociais e do boca a boca eletrônico (eWOM) sobre a decisão de compra, sem significância estatística para influenciadores digitais. O resultado não permite inferir relação entre privacidade e comportamento de compra, mas evidencia que a digitalização amplia os pontos de interação entre pequenos negócios e titulares de dados, ampliando a relevância de práticas de transparência nesses canais.

Em conjunto, essa literatura caracteriza um contexto organizacional marcado por restrições de conhecimento, planejamento e recursos, no qual soluções de proteção de dados precisam ser tecnicamente acessíveis para serem efetivamente adotadas. Nenhum dos estudos mencionados constitui evidência direta sobre LGPD ou Privacy by Design; sua função nesta pesquisa é contextual, sustentando a premissa metodológica de que recomendações dirigidas a ATPPs devem ser compatíveis com diferentes níveis de maturidade organizacional e tecnológica. É nesse espaço, entre as exigências normativas da LGPD e a realidade operacional das MPEs, que se situa a contribuição pretendida deste trabalho: articular Privacy by Design e requisitos legais em um conjunto de práticas simplificadas e tecnicamente viáveis.

3. METODOLOGIA

3.1 Delineamento

Este estudo adota abordagem qualitativa, de natureza aplicada, fundamentada em pesquisa documental, pesquisa bibliográfica e procedimento de síntese aplicada. A escolha decorre da natureza do problema investigado: compreender como exigências jurídicas de proteção de dados podem ser traduzidas em práticas técnicas e organizacionais factíveis para sistemas utilizados por microempresas e empresas de pequeno porte. O propósito não é mensurar estatisticamente o nível de conformidade de um conjunto de empresas, mas interpretar o marco normativo, confrontá-lo com a literatura pertinente e sistematizar diretrizes técnicas simplificadas a partir dessa articulação.

A investigação foi organizada em quatro etapas: (i) análise documental do marco jurídico e regulatório; (ii) levantamento e análise da literatura; (iii) categorização qualitativa dos requisitos identificados; e (iv) síntese aplicada dos requisitos em diretrizes técnicas para sistemas de pequeno porte. Essa estrutura procura manter separação metodológica entre o que decorre diretamente da legislação e o que corresponde à interpretação técnica proposta pelos autores.

3.2 Pesquisa documental

A pesquisa documental concentrou-se na Lei nº 13.709/2018 (LGPD) e na Resolução CD/ANPD nº 2/2022, consideradas em sua redação vigente. A LGPD foi examinada com atenção aos princípios do tratamento, às bases legais, aos direitos dos titulares e às obrigações de segurança e prevenção (BRASIL, 2018); a Resolução, com o propósito de identificar quais obrigações podem ser flexibilizadas para ATPPs e, sobretudo, quais responsabilidades permanecem aplicáveis mesmo diante dessas flexibilizações, uma vez que o art. 6º do regulamento não isenta o agente de pequeno porte do cumprimento dos demais dispositivos da LGPD (BRASIL, 2022).

A análise documental foi estruturada em três categorias: obrigações gerais, correspondentes aos requisitos da LGPD aplicáveis a qualquer tratamento; obrigações flexibilizadas ou simplificadas, identificadas a partir da Resolução; e requisitos técnicos e organizacionais remanescentes, cuja observância permanece necessária mesmo quando uma obrigação formal é dispensada ou simplificada. Essa classificação evitou uma leitura exclusivamente formal da norma, permitindo identificar quais requisitos jurídicos têm implicações diretas sobre projeto, implementação, operação e manutenção dos sistemas de informação. Também foi considerada a alteração do art. 14 da Resolução, relativo aos prazos diferenciados dos ATPPs, pela Resolução CD/ANPD nº 15/2024, de modo a evitar tratar como permanentes formulações normativas posteriormente modificadas.

3.3 Pesquisa bibliográfica e análise qualitativa

A pesquisa bibliográfica considerou quatro eixos: micro e pequenas empresas; transformação digital e inovação; desafios organizacionais de pequenos negócios; e proteção de dados e privacidade em sistemas de informação, cujo conteúdo é apresentado na seção 2. As referências da Revista da Micro e Pequena Empresa (RMPE) foram empregadas de maneira

complementar e contextual, e não como evidência direta de conformidade à LGPD; a legislação e os atos normativos da ANPD permanecem como fontes primárias das afirmações jurídicas.

A análise qualitativa consistiu na interpretação integrada das informações obtidas nas etapas documental e bibliográfica, buscando correspondências entre requisitos normativos, problemas organizacionais e possíveis respostas técnicas, sem tratar recomendações de engenharia de software como obrigações expressamente previstas em lei. Foram definidas três categorias analíticas: categorias jurídico-regulatórias (princípios da LGPD, bases legais, direitos dos titulares, segurança, transparência e flexibilizações para ATPPs); categorias técnicas (minimização de dados, controle de acesso, proteção de dados em trânsito e em repouso, registros, atendimento ao titular e recuperação); e categorias organizacionais e operacionais (capacidade financeira, conhecimento especializado, maturidade tecnológica e capacidade de implementação). Uma recomendação técnica somente foi considerada adequada ao contexto das MPEs quando havia correspondência entre sua finalidade de proteção e sua viabilidade operacional.

3.4 Procedimento de síntese aplicada

A síntese aplicada seguiu três movimentos. Primeiro, foram identificados os requisitos jurídicos com relação direta ao funcionamento de sistemas de informação, priorizando os princípios da necessidade, segurança, prevenção e transparência e as obrigações específicas dos ATPPs. Segundo, cada requisito foi relacionado a implicações para o ciclo de desenvolvimento e operação de software: o princípio da necessidade foi interpretado em termos de redução da coleta; os requisitos de segurança, em controles técnicos de proteção; e a transparência, em disponibilização de informações compreensíveis e mecanismos de atendimento aos titulares. Terceiro, foram selecionadas medidas tecnicamente acessíveis e potencialmente implementáveis em ambientes de pequena escala, sem afirmar que sua adoção isolada seja suficiente para assegurar conformidade jurídica integral. As diretrizes resultantes não constituem lista universal e suficiente para qualquer sistema, mas um núcleo mínimo de práticas técnicas capaz de orientar a implementação inicial de mecanismos de privacidade e segurança em sistemas de pequeno porte.

3.5 Delimitação

A pesquisa está delimitada à aplicação dos princípios da LGPD e das disposições específicas para ATPPs ao desenvolvimento e à operação de sistemas de software utilizados

por microempresas e empresas de pequeno porte. Não constituem objeto da investigação: sistemas corporativos de médio ou grande porte; organizações fora das condições regulamentares aplicáveis aos ATPPs; tratamentos de alto risco; auditorias de conformidade jurídica; testes técnicos de invasão ou avaliações quantitativas de segurança; mensuração estatística de custos de implementação; e avaliação empírica da efetividade das diretrizes em uma amostra de empresas. A exclusão de tratamentos de alto risco decorre diretamente dos arts. 3º e 4º da Resolução CD/ANPD nº 2/2022, de modo que as recomendações deste estudo não substituem avaliações específicas de risco ou obrigações adicionais eventualmente determinadas pela ANPD (BRASIL, 2022).

3.6 Considerações éticas

A pesquisa não envolveu coleta direta de dados pessoais de participantes, entrevistas, questionários ou experimentos com seres humanos; o corpus é constituído por legislação, atos normativos, literatura científica e documentos públicos. Dada a natureza do objeto, um trabalho sobre conformidade e proteção de dados, buscou-se distinguir metodologicamente três níveis de afirmação: o que está expressamente previsto na legislação ou regulamentação, o que é sustentado pela literatura científica, e o que constitui recomendação técnica derivada da síntese realizada neste estudo. Essa distinção é mantida nas seções seguintes: as soluções apresentadas nos resultados não são tratadas como imposições literais da LGPD quando constituem, na realidade, escolhas de engenharia destinadas a operacionalizar seus princípios. Não houve validação experimental das diretrizes propostas em empresas, o que impõe reserva quanto a qualquer afirmação de que sua implementação, isoladamente, garanta conformidade integral com a LGPD.

4. RESULTADOS E DISCUSSÃO

A análise documental e bibliográfica permitiu identificar que a aplicação da LGPD em sistemas destinados a microempresas e empresas de pequeno porte não deve ser compreendida como redução das obrigações legais em razão do tamanho da organização. O tratamento diferenciado previsto para ATPPs adequa determinadas exigências à capacidade operacional desses agentes, mas não elimina a necessidade de observância dos princípios, das bases legais, dos direitos dos titulares e das medidas de segurança estabelecidas pela LGPD. Os resultados apontam, nesse sentido, para uma abordagem técnica seletiva: em vez de reproduzir estruturas de governança concebidas para organizações de maior porte, os pequenos sistemas podem

priorizar controles diretamente relacionados aos riscos e às características dos tratamentos efetivamente realizados. A síntese aplicada organizou esses resultados em quatro dimensões: minimização e proteção de dados, segurança por padrão, transparência e exercício dos direitos dos titulares, e organização operacional proporcional ao porte e ao risco. Essas dimensões são apresentadas na Quadro 1 e detalhadas nas subseções seguintes.

Quadro 1: Diretrizes simplificadas para aplicação da LGPD em sistemas de pequeno porte

Aspecto regulatório ou princípio	**Implicação para o sistema**	**Diretriz técnica simplificada**
Dispensa de indicação obrigatória de Encarregado, nas condições previstas na Resolução	A organização continua necessitando de um meio de comunicação com os titulares	Disponibilizar canal de contato claramente identificado, preferencialmente integrado à aplicação ou ao sítio eletrônico
Flexibilização de determinadas obrigações documentais, nas condições regulamentares	Redução da carga documental não significa eliminação da necessidade de compreender os tratamentos realizados	Manter documentação mínima sobre dados coletados, finalidades, responsáveis e controles essenciais
Tratamento sujeito à avaliação de risco	Quanto maior o risco, menor deve ser a dependência de controles simplificados	Identificar tratamentos de maior risco e aplicar controles proporcionais
Princípio da necessidade	Dados sem relação com a finalidade aumentam a exposição e a complexidade do sistema	Coletar somente os dados necessários para a finalidade informada
Princípio da segurança	Dados pessoais precisam ser protegidos contra acessos e situações inadequadas	Utilizar autenticação, controle de acesso, proteção das comunicações, registros e backups
Transparência	O titular precisa compreender o tratamento realizado	Disponibilizar política de privacidade clara e informações acessíveis
Direitos dos titulares	O sistema deve possibilitar o atendimento das solicitações previstas na legislação	Criar mecanismo de solicitação e fluxo interno para tratamento das demandas
Segurança ao longo do ciclo de vida	A proteção não deve existir apenas no momento da coleta	Incorporar requisitos de privacidade às fases de desenvolvimento, manutenção e descarte
Restrições de recursos	Controles complexos podem ser inviáveis para organizações pequenas	Priorizar medidas de alto impacto e baixo custo operacional

A matriz evidencia que a conformidade técnica não depende necessariamente de ferramentas sofisticadas. Em muitos casos, decisões arquiteturais simples reduzem a quantidade de dados expostos e, consequentemente, a superfície de risco do sistema. A minimização é o exemplo mais direto dessa relação, ao atuar simultaneamente como requisito jurídico e como estratégia de engenharia.

A matriz evidencia que a conformidade técnica não depende necessariamente de ferramentas sofisticadas. Em muitos casos, decisões arquiteturais simples reduzem a quantidade de dados expostos e, consequentemente, a superfície de risco do sistema. A minimização é o exemplo mais direto dessa relação, ao atuar simultaneamente como requisito jurídico e como estratégia de engenharia.

4.1 Minimização e proteção de dados

O princípio da necessidade, previsto no art. 6º, III, da LGPD, estabelece que o tratamento deve ser limitado ao mínimo necessário à realização de suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos (BRASIL, 2018). Do ponto de vista da engenharia de software, esse princípio converte-se em uma pergunta a ser feita antes da definição dos campos do banco de dados e dos formulários, e não depois de o sistema já implantado: este dado é necessário para que a funcionalidade seja executada? Em um sistema de agendamento, por exemplo, determinadas funcionalidades exigem informações de identificação e contato, mas isso não torna necessários todos os dados disponíveis sobre o usuário; campos adicionais devem ser justificados pela finalidade correspondente, sob pena de ampliar desnecessariamente o volume de informações a proteger, atualizar e eventualmente eliminar. Um efeito associado é a redução da quantidade de dados potencialmente expostos em um incidente, ainda que a minimização não elimine o risco de ocorrência.

O mesmo raciocínio aplica-se a relatórios internos que não exijam identificação direta dos indivíduos, nos quais a anonimização ou a pseudonimização podem ser avaliadas quando tecnicamente e juridicamente adequadas. É necessário, contudo, distinguir os dois conceitos: a pseudonimização substitui identificadores sem necessariamente eliminar a possibilidade de reidentificação, de modo que a simples substituição de um nome por um código não deve ser apresentada como anonimização automática. A escolha entre manter o dado identificável, pseudonimizá-lo ou anonimizá-lo depende da finalidade concreta, da possibilidade de reidentificação e dos requisitos da operação; a anonimização não deve ser utilizada como solução genérica para qualquer problema de proteção de dados.

Essa abordagem preventiva é coerente com o Privacy by Design, segundo o qual a privacidade deve ser considerada desde a concepção do sistema (CAVOUKIAN, 2009). Em pequenas empresas, essa antecipação assume importância adicional: uma decisão tomada na etapa inicial de modelagem pode evitar alterações posteriores no banco de dados, nos formulários, nas integrações e nos procedimentos de segurança, reduzindo retrabalho. A

literatura sobre inovação frugal em PMEs reforça, de maneira contextual, a pertinência dessa lógica de priorização e otimização de recursos (ALVES; NODARI, 2023), sem que se possa afirmar que minimização de dados equivalha a inovação frugal: trata-se de uma aproximação conceitual, não de evidência empírica direta sobre proteção de dados.

4.2 Segurança por padrão e proteção do ciclo de vida

O art. 46 da LGPD determina que os agentes de tratamento adotem medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (BRASIL, 2018). Para sistemas de pequeno porte, o desafio não é reproduzir integralmente arquiteturas de segurança de grandes organizações, mas selecionar controles fundamentais e compatíveis com os riscos existentes: proteção das comunicações e dos dados armazenados, controle de acesso e mecanismos de backup e recuperação.

A utilização de protocolos seguros de comunicação, como TLS/HTTPS, constitui medida básica para evitar exposição inadequada de informações transmitidas entre usuários e sistemas; a proteção de dados armazenados deve ser avaliada de acordo com a sensibilidade das informações e os riscos identificados, sem que a presença isolada de uma tecnologia de criptografia caracterize, por si só, conformidade com a LGPD. O controle de acesso, baseado em perfis e permissões (RBAC), permite restringir o acesso às informações necessárias a cada função, reduzindo a exposição decorrente da concessão indiscriminada de privilégios. Registros de auditoria também auxiliam na identificação de eventos relevantes, mas devem observar o próprio princípio da minimização: logs que reproduzem dados pessoais ou sensíveis de forma indiscriminada geram novos riscos em vez de mitigá-los.

O backup constitui outro controle fundamental, sobretudo porque a perda de dados pode comprometer a continuidade operacional de pequenos negócios. O resultado relevante dessa recomendação não está apenas na existência de cópias de segurança, mas na possibilidade de recuperação efetiva: backups nunca testados podem gerar falsa percepção de segurança, de modo que o procedimento deve contemplar periodicidade, proteção das cópias e testes compatíveis com a capacidade operacional da empresa. Essa ênfase em processos, e não apenas em ferramentas, converge com o achado de Batista, Arouca e Lobato (2024) de que a disponibilidade de tecnologia não garante seu aproveitamento adequado: adquirir um serviço de armazenamento seguro não substitui a configuração correta de permissões, autenticação, backups e rotinas operacionais. A noção de segurança ao longo do ciclo de vida, central ao

Privacy by Design, reforça essa leitura: a proteção deve ser considerada durante especificação, desenvolvimento, implantação, manutenção e descarte (CAVOUKIAN, 2009).

4.3 Transparência e exercício dos direitos dos titulares

A dispensa de indicação de encarregado para determinados ATPPs não elimina a necessidade de comunicação com os titulares; a própria Resolução CD/ANPD nº 2/2022 determina a disponibilização de um canal de comunicação para o agente que optar por não indicá-lo, sem afastar os direitos assegurados pela LGPD (BRASIL, 2018; BRASIL, 2022). No nível do sistema, essa exigência pode ser operacionalizada por meio de uma política de privacidade acessível, que explique, de forma compatível com o público-alvo, quais informações são coletadas, para quais finalidades e como o titular pode entrar em contato com a organização. A transparência não deve ser tratada apenas como documento jurídico pouco acessível: constitui também requisito de interface, podendo ser disponibilizada em pontos relevantes do fluxo de utilização, especialmente quando uma funcionalidade solicitar informações adicionais.

A criação de um canal específico para requisições pode ser considerada medida de baixo custo: um formulário estruturado permite registrar solicitações, identificar o titular, encaminhar a demanda ao responsável e acompanhar seu atendimento, sem exigir uma plataforma sofisticada de gestão de direitos. Essa dimensão é especialmente relevante diante da crescente digitalização das MPEs: Silva et al. (2024) verificaram influência positiva da comunicação em mídias sociais e do boca a boca eletrônico sobre a decisão de compra de consumidores de pequenos negócios. O resultado não demonstra que políticas de privacidade aumentam vendas ou confiança, inferência que este estudo não sustenta, mas evidencia que pequenos negócios estão inseridos em ambientes digitais nos quais a comunicação com consumidores assume relevância crescente, o que reforça a pertinência de tratar a transparência sobre dados pessoais como parte da própria experiência digital oferecida pela empresa, e não apenas como exigência documental.

4.4 Flexibilização regulatória e responsabilidade proporcional

Um dos principais resultados interpretativos deste estudo é que a flexibilização prevista pela ANPD deve ser compreendida como mecanismo de proporcionalidade regulatória, e não como autorização para negligenciar a proteção de dados. A Resolução CD/ANPD nº 2/2022 estabelece tratamento diferenciado para ATPPs, mas também prevê condições para sua

aplicação e distingue situações de maior risco (BRASIL, 2022). O porte da empresa não determina, isoladamente, o risco de uma operação de tratamento: uma empresa pequena pode operar com informações cuja exposição apresente consequências relevantes para os titulares, de modo que uma abordagem baseada exclusivamente no número de empregados ou no volume financeiro seria insuficiente para definir a intensidade dos controles técnicos necessários. A simplificação defendida neste trabalho deve ser entendida, portanto, como simplificação operacional, isto é, redução de complexidade documental e priorização de controles essenciais, e não como simplificação indiscriminada dos requisitos materiais de proteção.

Essa compreensão também permite relacionar conformidade e capacidade de inovação com a devida cautela. Alves, Aires e Salgado (2023), ao analisarem doze ações do Programa Agentes Locais de Inovação em MPEs do Rio Grande do Norte, identificaram potencial de vantagem competitiva em seis delas, com efeitos heterogêneos conforme as características de cada ação. O achado não permite afirmar que práticas de privacidade gerem automaticamente vantagem competitiva, mas sustenta que intervenções voltadas a MPEs devem ser avaliadas quanto à sua capacidade efetiva de produzir valor e à adequação aos recursos disponíveis. Esse raciocínio, aplicado à LGPD, favorece a priorização de controles que reduzam riscos relevantes sem impor estruturas desproporcionais ao contexto organizacional.

4.5 Privacy by Design como estratégia preventiva

Os resultados permitem interpretar o *Privacy by Design* não como metodologia independente da LGPD, mas como abordagem capaz de aproximar requisitos jurídicos de decisões concretas de engenharia. Seu valor para pequenos sistemas está, principalmente, na possibilidade de antecipar decisões relacionadas à coleta, ao armazenamento, ao acesso, à exposição e ao descarte das informações: se a necessidade de determinado dado for questionada antes da criação do banco de dados, evita-se a implementação de campos e rotinas que posteriormente precisariam ser removidos; se os perfis de acesso forem definidos durante a arquitetura do sistema, reduz-se a necessidade de reconstruir a lógica de autorização após a implantação.

Os sete princípios de Cavoukian (2009), apresentados na seção 2.1, podem ser operacionalizados de forma gradual em ATPPs, priorizando os aspectos diretamente relacionados ao tratamento realizado. A privacidade como configuração padrão pode significar que campos não essenciais não sejam obrigatórios; a incorporação da privacidade ao design pode significar que fluxos de acesso e exclusão sejam definidos junto às demais

funcionalidades; a proteção de ponta a ponta orienta a segurança durante transmissão, armazenamento, utilização e descarte; e a transparência orienta a construção das interfaces e da política de privacidade. A ideia de funcionalidade total é particularmente relevante porque privacidade não deve ser tratada como oposição à funcionalidade: em muitos casos, a solução está em redesenhar o fluxo para manter a funcionalidade com menor exposição de dados, e não em suprimir funcionalidades do sistema. A adoção do conceito, contudo, não se resume à presença isolada de criptografia ou de uma política de privacidade; envolve uma orientação preventiva e sistemática das decisões de projeto, de modo que as medidas apresentadas neste trabalho devem ser entendidas como exemplos de operacionalização dos princípios, e não como lista exaustiva ou certificação de conformidade.

4.6 Capacidade organizacional, conhecimento e competitividade

A dificuldade de conformidade não é exclusivamente tecnológica: a adoção de mecanismos de proteção depende de conhecimento organizacional sobre o tratamento de dados e sobre o propósito dos controles implementados. Lima e Silva (2024) identificaram, em pequenos negócios, que o desconhecimento sobre o escopo e o valor de serviços especializados constitui a principal razão para sua não contratação; embora o estudo trate de consultoria jurídico-tributária, e não de proteção de dados, o achado é pertinente por demonstrar que, em pequenos negócios, a existência de uma necessidade técnica ou jurídica não implica sua percepção como prioridade administrativa. Esse aspecto reforça a necessidade de diretrizes compreensíveis por profissionais não especializados: uma política de privacidade, um fluxo de atendimento ao titular ou um procedimento de backup só são efetivos se os responsáveis pela organização souberem utilizá-los, de modo que a simplicidade defendida neste artigo possui também dimensão cognitiva.

Gonçalves et al. (2023) demonstraram, por meio do caso de uma pequena empresa com trajetória de crescimento sem planejamento estratégico formal, que processos decisórios podem se modificar em resposta a pressões internas e externas e que a ascensão de gestores intermediários esteve associada a maior propensão à inovação sem abandono da eficiência. O estudo não investiga proteção de dados, mas reforça que mudanças organizacionais em pequenas empresas podem ocorrer de maneira adaptativa e distribuída, e não apenas mediante planejamento formal centralizado. Esse achado é relevante para a implementação das diretrizes propostas, já que a responsabilidade por práticas de privacidade em uma MPE pode recair sobre

o proprietário, o administrador, o desenvolvedor ou o prestador de serviço, e não necessariamente sobre um encarregado formal.

A literatura sobre inovação e digitalização das MPEs também situa a proposta deste trabalho em uma discussão mais ampla sobre competitividade. Simplicidade não é proposta aqui como sinônimo de redução dos padrões de proteção: um sistema pequeno pode ter arquitetura simples e, simultaneamente, adotar controles adequados de autenticação, autorização, criptografia, minimização, registro de eventos, backup e transparência. O que deve ser evitado é associar conformidade a complexidade tecnológica, como se sistemas mais sofisticados fossem necessariamente mais protegidos. Da mesma forma, não se afirma que a adoção das diretrizes propostas produza vantagem competitiva mensurável; os benefícios da conformidade devem ser tratados com prudência, e segurança, privacidade e transparência são apresentadas neste artigo prioritariamente como requisitos de proteção e adequação, não como mecanismos comprovados de desempenho econômico.

4.7 Síntese das diretrizes propostas

A partir da integração entre legislação, Privacy by Design e literatura sobre o contexto das MPEs, as diretrizes deste estudo constituem um núcleo mínimo de práticas técnicas e organizacionais, organizado em cinco prioridades. A primeira é reduzir a quantidade de dados pessoais tratados, mediante avaliação da necessidade de cada campo e funcionalidade. A segunda é estabelecer configurações de segurança compatíveis com os riscos, incluindo proteção das comunicações, controle de acesso e rotinas de backup testadas. A terceira é assegurar transparência por meio de informações claras e de um canal funcional para os titulares. A quarta é considerar, desde o desenvolvimento, os requisitos relacionados ao ciclo de vida dos dados, incluindo armazenamento, acesso, alteração e descarte. A quinta é manter procedimentos mínimos para incidentes e solicitações de titulares, mesmo quando obrigações formais tenham sido flexibilizadas pela ANPD. Essa síntese evita que a flexibilização regulatória seja interpretada como justificativa para ausência de controles: a Resolução nº 2/2022 cria condições diferenciadas para ATPPs, mas não transforma a proteção de dados em preocupação opcional.

4.8 Limitações dos resultados

Os resultados devem ser interpretados considerando as limitações metodológicas do estudo. A pesquisa é documental, bibliográfica, qualitativa e de síntese aplicada; não houve

implementação das diretrizes em uma amostra de sistemas reais de MPEs, tampouco avaliação experimental de sua eficácia, custo ou impacto sobre indicadores de segurança. Consequentemente, a caracterização das medidas propostas como de "baixo custo" deve ser entendida como proposição de viabilidade técnica relativa, e não como resultado de análise quantitativa: o estudo não calculou custos de desenvolvimento, manutenção, licenciamento ou treinamento, tampouco comparou o custo total de propriedade de diferentes arquiteturas. A pesquisa também não avaliou quantitativamente o nível de maturidade em proteção de dados das MPEs brasileiras; as diretrizes não devem, portanto, ser interpretadas como protocolo universal de conformidade, uma vez que diferentes setores, tipos de dados, volumes de tratamento e níveis de risco podem demandar controles adicionais. Por fim, a classificação como ATPP depende do atendimento às condições da regulamentação aplicável, e situações de alto risco exigem atenção específica que não se enquadra nas flexibilizações aqui discutidas.

A literatura sobre MPEs utilizada neste estudo (digitalização, inovação frugal, consultoria, crescimento organizacional, programas de inovação e transformação digital no varejo) não investiga diretamente a implementação da LGPD em sistemas de pequeno porte; sua utilização é contextual e comparativa, o que delimita, e não enfraquece, a integridade da discussão, ao distinguir claramente o que foi observado na literatura correlata daquilo que constitui a síntese aplicada desenvolvida neste artigo. Apesar dessas limitações, o estudo apresenta contribuição prática ao organizar princípios jurídicos e de *Privacy by Design* em decisões técnicas passíveis de consideração durante o desenvolvimento de sistemas pequenos, aproximando o conteúdo normativo da realidade de implementação das MPEs sem tratar a limitação de recursos como impedimento absoluto à adoção de práticas de privacidade.

5. CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo analisar as implicações da LGPD e da Resolução CD/ANPD nº 2/2022 para o desenvolvimento de sistemas de pequeno porte e propor práticas de Privacy by Design e segurança da informação compatíveis com as restrições de recursos das MPEs. A análise documental e bibliográfica indica que o tratamento diferenciado concedido aos ATPPs não constitui dispensa geral de conformidade: a Resolução flexibiliza obrigações específicas (registro simplificado das operações, dispensa condicionada de encarregado, política simplificada de segurança), mas seu art. 6º preserva a exigência de observância dos princípios, das bases legais e dos direitos dos titulares previstos na LGPD. O principal achado da síntese aplicada é que essa flexibilização deve se traduzir, no plano da engenharia de

software, em simplificação da forma de implementação dos controles, e não em redução dos padrões materiais de proteção, organizada em torno de três dimensões técnicas prioritárias: minimização de dados, segurança por padrão e transparência no relacionamento com os titulares.

A contribuição deste trabalho é de natureza aplicada e integrativa: não propõe uma nova teoria sobre proteção de dados nem apresenta evidência experimental sobre a eficácia das medidas recomendadas, mas aproxima o conteúdo normativo da LGPD e da regulamentação da ANPD dos princípios de *Privacy by Design*, organizando um conjunto de práticas capaz de orientar decisões de desenvolvimento em sistemas de pequeno porte. Para desenvolvedores e gestores de MPEs, a implicação prática central é que a privacidade pode ser tratada como decisão de projeto: identificação da finalidade, seleção de campos de cadastro, definição de permissões, estruturação de mecanismos de armazenamento e construção de interfaces de transparência, e não apenas como documento jurídico produzido após a implantação do sistema.

O estudo possui limitações que devem orientar a interpretação de seus resultados. Sua natureza documental, bibliográfica e qualitativa implica que as diretrizes propostas resultam de interpretação e síntese das fontes analisadas, e não de validação empírica: não houve implementação das diretrizes em empresas reais, tampouco mensuração de custos, tempo de desenvolvimento ou redução de incidentes decorrentes de sua adoção. Consequentemente, não se pode afirmar que a adoção das práticas propostas garanta, isoladamente, conformidade integral com a LGPD, uma vez que essa adequação depende do contexto específico de tratamento, das bases legais utilizadas e do enquadramento regulatório efetivo da organização, inclusive quanto a eventuais situações de alto risco.

Como possibilidades de continuidade, sugere-se a implementação e o teste das diretrizes propostas em sistemas reais utilizados por MPEs, a avaliação quantitativa dos custos de desenvolvimento e manutenção dos controles recomendados, estudos de usabilidade sobre os mecanismos de transparência e atendimento aos titulares, e a investigação empírica de como a maturidade digital e o conhecimento organizacional influenciam a adoção de práticas de Privacy by Design em diferentes contextos de pequenas empresas. Nesse sentido, os resultados aqui apresentados sustentam uma estratégia de proporcionalidade técnica: coletar menos, proteger adequadamente, informar com clareza e incorporar a privacidade desde o projeto. Essa estratégia não elimina as responsabilidades legais das MPEs, mas pode contribuir para torná-las operacionalmente mais compreensíveis e viáveis.

6. REFERÊNCIAS

ALVES, Ítalo Bruno Gomes; AIRES, Renan Felinto de Farias; SALGADO, Camila Cristina Rodrigues. O potencial de gerar vantagem competitiva de ações do programa agentes locais de inovação (ALI): um estudo de caso em micro e pequenas empresas do Rio Grande do Norte. **Revista da Micro e Pequena Empresa**, v. 17, n. 1, p. 5-20, 2023. DOI: https://doi.org/10.6034/rmpe.v17i1.1507.

ALVES, Karen Thais; NODARI, Cristine Hermann. Evidências da inovação frugal em pequenas e médias empresas: uma revisão sistemática da literatura. **Revista da Micro e Pequena Empresa**, v. 17, n. 2, p. 75-90, 2023. DOI: https://doi.org/10.6034/rmpe.v17i2.1820.

BATISTA, Alessandra Giselle Silva; AROUCA, Marcia Waimer Spinola; LOBATO, Fábio Manoel França. Estratégias de digitalização comunicacional para micro e pequenas empresas como promotoras da inovação e competitividade. **Revista da Micro e Pequena Empresa**, v. 18, n. 3, p. 60-79, 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm. Acesso em: 21 nov. 2024.

BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. **Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte**. Brasília, DF: 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 nov. 2024. Texto vigente com alterações da Resolução CD/ANPD nº 15/2024.

CAVOUKIAN, Ann. **Privacy by Design:** the 7 foundational principles. Toronto: Information and Privacy Commissioner of Ontario, 2009.

DINIZ, Rafael Henriques Nogueira; DINIZ, Luciana Mara Freitas; VILAÇA, Daniele; OLIVEIRA, Enderson; LEITE, Pedro; SOARES, Tiago; SILVA, William. Modelo de cartilha de conscientização sobre LGPD para micro e pequenas empresas. **Revista Projetos Extensionistas**, v. 1, n. 1, p. 285-288, 2021.

GONÇALVES, Rodrigo Tardin Rosa Ferraz; BERNARDES, Maria Elisa Brandão; SOUSA, Paulo Renato de; VERSIANI, Ângela França. O processo de crescimento de uma pequena empresa sem planejamento estratégico: o papel dos gestores intermediários. **Revista da Micro e Pequena Empresa**, v. 17, n. 2, p. 54-74, 2023.

LIMA, Jorranes Jacomini Nicolau de; SILVA, Fabio Pereira da. A percepção dos pequenos empreendedores sobre a consultoria jurídico-tributária. **Revista da Micro e Pequena Empresa**, v. 18, n. 1, p. 130-149, 2024.

SILVA, Patrícia Leite da; CASSOL, Alessandra; BONA, Claudia Regina Franceschetto de; MARIETTO, Márcio Luiz. A transformação digital no varejo dos pequenos negócios: o papel das mídias sociais, dos influenciadores e do boca-a-boca eletrônico (eWOM) nas decisões de compra das mulheres. **Revista da Micro e Pequena Empresa**, v. 18, n. 1, p. 5-21, 2024.

TRISTÃO, G. R.; FIRMINO, M. C. Lei Geral de Proteção de Dados: desafios técnicos enfrentados por microempresas e empresas de pequeno porte. **Revista Fatec Seg**, v. 1, n. 1, 2021.