UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE CIÊNCIAS JURÍDICAS

FACULDADE DE DIREITO DO RECIFE

OSMAN TORRES XIMENES JUNIOR

LEI GERAL DE PROTEÇÃO DE DADOS: análise de aplicabilidade e adequação na biblioteca da Faculdade de Direito do Recife

Recife

2025

OSMAN TORRES XIMENES JUNIOR

LEI GERAL DE PROTEÇÃO DE DADOS: análise de aplicabilidade e adequação na biblioteca da Faculdade de Direito do Recife

Trabalho de Conclusão de Curso apresentado ao curso de Graduação em Direito da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de bacharel em Direito.

Área de concentração: Direito Civil Administrativo.

Orientador: Geraldo Antonio Simões Galindo

Recife

2025

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Ximenes Júnior, Osman Torres.
Lei Geral de Proteção de Dados: análise de aplicabilidade e adequação na biblioteca da Faculdade de Direito do Recife / Osman Torres Ximenes Júnior. - Recife, 2025.
30 p., tab.

Orientador(a): Geraldo Antonio Simões Galindo
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, Direito - Bacharelado, 2025.

1. Lei Geral de Proteção de Dados. 2. Biblioteca Universitária. 3. Proteção de Dados Pessoais. 4. Governança de Dados. I. Galindo, Geraldo Antonio Simões. (Orientação). II. Título.

340 CDD (22.ed.)

OSMAN TORRES XIMENES JUNIOR

LEI GERAL DE PROTEÇÃO DE DADOS: análise de aplicabilidade e adequação na biblioteca da Faculdade de Direito do Recife

Trabalho de Conclusão de Curso apresentado ao curso de Graduação em Direito da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de bacharel em Direito.

Aprovado em: 24/11/2025.

BANCA EXAMINADORA

_____

Prof. Dr. Geraldo Antonio Simões Galindo (Orientador)

Universidade Federal de Pernambuco - UFPE

_____

Prof. Dr. Leônio José Alves da Silva (1º Examinador)

Universidade Federal de Pernambuco - UFPE

_____

Ma. Karine Gomes Falcão Vilela (2º Examinadora)

Universidade Federal de Pernambuco - UFPE

RESUMO

A proteção de dados pessoais não é apenas um direito individual, mas uma condição para o exercício da cidadania, a preservação da dignidade humana e a manutenção de um ambiente democrático e livre. Atualmente o tratamento de dados pessoais no Brasil é regulado pela Lei Geral de Proteção de Dados, conhecida por LGPD. Este trabalho tem como fundamento o estudo da referida lei, em cotejo com uma análise das procedimentalidades operacionais em bibliotecas universitárias, com especial foco na conceituada e histórica biblioteca da Faculdade de Direito do Recife, dado seu papel crucial no acesso à informação e no armazenamento de grandes volumes de dados. Tendo como parâmetro as premissas operacionais implementadoras das boas práticas bibliotecárias, esta pesquisa busca elencar propostas alternativas de aprimoramentos e/ou correções pragmáticas, buscando contribuir para a adequação efetiva à LGPD. Conclui-se então que a conformidade legal exige a implementação de um programa contínuo de governança de dados e uma profunda mudança de cultura institucional.

Palavras-chave: Lei Geral de Proteção de Dados; Biblioteca Universitária; Proteção de Dados Pessoais; Governança de Dados.

ABSTRACT

Personal data protection is not merely an individual right, but a condition for the exercise of citizenship, the preservation of human dignity, and the maintenance of a free and democratic environment. Currently, personal data processing in Brazil is regulated by the General Data Protection Law, also known as LGPD. This study is based on the analysis of the aforementioned law, in conjunction with an examination of the operational procedures in university libraries, with a special focus on the renowned and historic library of the Faculdade de Direito do Recife, given its crucial role in accessing information and storing large volumes of data. Taking as a parameter the operational premises that implement best practices in libraries, this research seeks to list pragmatic alternative proposals for improvements and/or corrections, aiming to contribute to effective compliance with the LGPD. It is thus concluded that legal conformity requires the implementation of a continuous data governance program and a profound change in institutional culture.

Keywords: General Data Protection Law; University Library; Personal Data Protection; Data Governance.

SUMÁRIO

1 INTRODUÇÃO

Com a vigência da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, novas formas de regulamentação do tratamento de dados pessoais foram incorporadas ao ordenamento jurídico brasileiro, com foco na garantia dos direitos fundamentais à liberdade de expressão e comunicação, privacidade e segurança pública dos cidadãos em um ambiente cada vez mais digitalizado, bem como a livre formação da personalidade de cada indivíduo.

Instituições públicas e privadas que armazenam e processam dados pessoais, como as bibliotecas, devem se adaptar a essa legislação, implementando medidas para garantir a conformidade com os requisitos legais da LGPD e a proteção dos dados de seus usuários.

No contexto da Faculdade de Direito do Recife (FDR) da Universidade Federal de Pernambuco (UFPE), a biblioteca, uma das mais tradicionais e relevantes no âmbito jurídico nacional, desempenha um papel crucial no acesso ao seu acervo de informação e pesquisa jurídica e legislativa, armazenando grandes volumes de dados pessoais, exigindo, portanto, a conformidade de suas práticas de gestão de dados pessoais à LGPD. Assim, o presente trabalho tem como objetivo central realizar um estudo de caso da aplicação da referida norma, oferecendo recomendações e soluções relacionadas ao tratamento de dados pela Biblioteca da FDR - Biblioteca Setorial do Centro de Ciências Jurídicas da UFPE (BIBCCJ).

2 PROTEÇÃO DE DADOS: Direito Fundamental em construção

A consolidação do direito à proteção de dados pessoais como direito fundamental reflete um processo histórico e normativo complexo, que acompanha a evolução das sociedades modernas diante dos avanços tecnológicos e da intensificação das interações no meio digital. “Fazemos parte de uma sociedade que busca ter e deter informações, como forma diferenciadora entre elas e conservar o seu poder” (CARDOZO et al, 2007, p. 327). Não se trata apenas de proteger informações isoladas, mas de garantir a autodeterminação informativa do indivíduo, sua dignidade e sua liberdade de expressão e comunicação em um ambiente cada vez mais marcado pela coleta massiva e automatizada de dados.

No Brasil, a proteção da privacidade e dos dados pessoais ganhou contornos constitucionais ao longo do tempo. A Constituição Federal de 1988 já assegurava, em seu artigo 5º, a inviolabilidade da intimidade, da vida privada, da honra e da imagem, e previa mecanismos como o habeas data para garantir o acesso e a retificação de informações pessoais. Contudo, a positivação expressa do direito à proteção de dados como direito fundamental só se deu com a Emenda Constitucional nº 115, de 2022, em resposta às novas dinâmicas sociais e tecnológicas que atualmente demandam maior segurança jurídica e padronização de regulamentos e práticas para a proteção dos dados pessoais.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> [...]
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022).

Historicamente, os direitos fundamentais evoluíram em dimensões. O direito à privacidade pertence à primeira dimensão, voltada à abstenção do Estado. Já a proteção de dados se insere na terceira dimensão, por ser um direito difuso, essencial à coletividade e à manutenção da democracia. Trata-se de um direito que pressupõe prestações estatais, regula o tratamento da informação em circulação e busca equilibrar interesses públicos, privados e individuais.

O contexto atual é marcado pela chamada “sociedade da informação”, onde

dados pessoais são insumos essenciais para o funcionamento do mercado, da administração pública e até das relações sociais mais triviais. A emergência da internet, da inteligência artificial, do big data e da vigilância digital transformou o valor da informação e expôs vulnerabilidades antes inexistentes. Em resposta, o ordenamento jurídico brasileiro construiu uma arquitetura normativa multifacetada, envolvendo o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei de Acesso à Informação e, mais recentemente, a Lei Geral de Proteção de Dados.

A LGPD, de 14 de agosto de 2018, inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) europeu, representa um marco regulatório robusto para o tratamento de dados pessoais no Brasil. Ela define os direitos dos titulares, as obrigações dos agentes de tratamento e é composta por princípios, tais como da transparência, segurança, finalidade, responsabilização e prestação de contas. Sua aplicação é transversal, abrangendo desde plataformas digitais até serviços interpessoais, em que o tratamento de dados sensíveis demanda ainda maior rigor.

Além disso, a LGPD institui a Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar, regulamentar e educar a sociedade sobre o tema. A proteção de dados, portanto, não se limita ao cumprimento legal, mas implica uma mudança cultural nas práticas empresariais, no poder público e na vida cotidiana dos cidadãos.

A constitucionalização do direito à proteção de dados e o reconhecimento da sua autonomia em relação à privacidade, como declarado pelo Supremo Tribunal Federal, reforçam sua centralidade no Estado Democrático de Direito. A decisão do STF na ADI 6387, por exemplo, ao barrar o compartilhamento de dados pessoais pelas operadoras de telefonia ao IBGE, destacou o princípio da autodeterminação informativa e demonstrou que, na era digital, não há mais dados “insignificantes”, e, portanto, sua manipulação e tratamento devem observar os limites delineados pela proteção constitucional.

> A autodeterminação individual pressupõe – mesmo sob as condições da moderna tecnologia de processamento de informação – que, ao indivíduo está garantida a liberdade de decisão sobre as ações a serem procedidas ou omitidas e, inclusive, a possibilidade de se comportar realmente conforme tal decisão. (STF; Ação Direta de Inconstitucionalidade (ADI) 6387; Relatora: Min. Rosa Weber; Data do julgamento: 24/04/2020).

Entretanto, essa construção ainda está em curso. A efetividade do direito à proteção de dados exige a criação de uma cultura de privacidade, a capacitação de

agentes públicos e privados, a educação digital da população e a constante atualização normativa para acompanhar as inovações tecnológicas. É preciso ir além da mera observância da lei, adotando práticas transparentes e éticas, que respeitem a centralidade do indivíduo no tratamento de seus dados.

Em suma, a proteção de dados pessoais não é apenas um direito individual, mas uma condição para o exercício da cidadania, a preservação da dignidade humana e a manutenção de um ambiente democrático e livre. Sua consolidação como direito fundamental é, portanto, um passo necessário que exige vigilância permanente, engajamento coletivo e compromisso institucional.

3 ÂMBITO DE APLICAÇÃO DA LGPD: as cinco lentes de análise jurídica

A LGPD, ao instituir um novo paradigma jurídico para o tratamento de informações pessoais no Brasil, possui um vasto espectro de aplicabilidade que exige uma análise multifacetada. A compreensão integral da lei demanda a sua dissecação por meio de perspectivas analíticas que revelam o seu alcance. As cinco lentes – subjetiva, material/objetiva, territorial, temporal e quantitativa – permitem um estudo aprofundado sobre os limites e as exigências do novo marco regulatório nacional.

3.1 A PERSPECTIVA SUBJETIVA: a quem se aplica?

A análise subjetiva da LGPD define a quem a lei se aplica, identificando os atores envolvidos na relação de tratamento de dados e suas responsabilidades legais. No centro da legislação está o Titular de Dados, a pessoa natural a quem se referem os dados pessoais e cuja autonomia e privacidade são os bens jurídicos tutelados pela lei. Todos os dispositivos da LGPD convergem para garantir o controle do titular sobre suas informações.

Em contrapartida, a lei estabelece os Agentes de Tratamento. O Controlador é a pessoa jurídica ou natural a quem compete a tomada de decisões relativas ao tratamento dos dados, definindo a finalidade e as bases legais. A responsabilidade do Controlador é primária. O segundo agente é o Operador, que realiza o tratamento em nome e sob as instruções do Controlador. O Art. 23 da lei impõe um regime específico para o Poder Público quando atua como Controlador, exigindo o cumprimento da lei, mas orientando as bases legais majoritariamente para o cumprimento da obrigação legal e a execução de políticas públicas.

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

Por fim, a lei obriga a nomeação de um Encarregado de Dados, que funciona como o canal de comunicação entre os agentes de tratamento, os titulares de dados e a ANPD.

3.2 A PERSPECTIVA MATERIAL/OBJETIVA: sobre o que se aplica?

O âmbito material ou objetivo da LGPD estabelece o objeto de sua regulação, que é o tratamento (toda e qualquer operação realizada com dados) de dados pessoais e dados pessoais sensíveis. A lei é aplicada a um universo de operações que incluem a coleta, a utilização, o acesso, o armazenamento, a classificação e a eliminação das informações.

Crucialmente, a perspectiva material exige que o tratamento esteja sempre justificado por uma das Bases Legais taxativamente previstas na LGPD (Art. 7º e Art. 11), em observância ao Princípio da Finalidade.

A lei dispensa proteção mais rigorosa aos Dados Pessoais Sensíveis – aqueles relacionados a aspectos íntimos e potencialmente discriminatórios do indivíduo (saúde, religião, origem racial, filiação política, dados biométricos). O tratamento desses dados é vedado, exceto sob condições específicas e mais estritas, reforçando o cuidado com informações que podem impactar os direitos e liberdades fundamentais do titular.

3.3 A PERSPECTIVA TERRITORIAL: onde se aplica?

A análise territorial define os limites geográficos e operacionais da aplicação da LGPD. A lei possui um escopo de aplicação amplo e transnacional, aplicando-se a: (1) qualquer operação de tratamento de dados realizada em território nacional; (2) atividades de tratamento que busquem oferecer bens ou serviços a indivíduos localizados no Brasil; (3) ou dados pessoais coletados no Brasil.

Esse caráter de extraterritorialidade mitigada significa que a lei alcança empresas e órgãos, mesmo que o tratamento de dados seja realizado fora do país, desde que a finalidade ou a coleta esteja vinculada ao Brasil. A lei, portanto, estabelece um padrão de proteção de dados que deve ser seguido globalmente por qualquer entidade que interaja com o ecossistema brasileiro.

3.4 A PERSPECTIVA TEMPORAL: quando se aplica?

A perspectiva temporal aborda a vigência da LGPD e sua incidência sobre o acervo de dados. A lei não opera somente pro futuro, regulando as operações de tratamento que se iniciam após sua entrada em vigor. Pelo contrário, ela é plenamente aplicável ao conjunto de dados pessoais já existente na base das organizações, o chamado acervo histórico.

Este ponto exige que as entidades revisem seus cadastros passados para garantir que a retenção e o tratamento contínuo desses dados estejam amparados em uma base legal e em conformidade com o Princípio da Adequação. A proteção de dados, reforçada como direito fundamental na Constituição Federal pela Emenda Constitucional nº 115, de 2022, tem um caráter contínuo e permanente, exigindo uma adequação constante dos procedimentos ao longo do tempo.

3.5 A PERSPECTIVA QUANTITATIVA: quanta aplicação?

A LGPD se aplica a qualquer volume de tratamento de dados pessoais, mas a perspectiva quantitativa é essencial para a gestão de riscos e para a definição das medidas de segurança. O volume de dados manipulados por uma organização é diretamente proporcional ao risco de um incidente de segurança e ao potencial danoso contra o titular.

Organizações que lidam com uma grande massa de dados ou com alto número de dados sensíveis devem implementar medidas técnicas e administrativas mais robustas e complexas. Essa proporcionalidade é um dos pilares do Princípio da Segurança. Além disso, a acumulação de um vasto acervo de dados aumenta a responsabilidade dos agentes de tratamento, exigindo um rigoroso processo de governança e a manutenção de uma cultura de privacidade permanente.

4 OS DADOS NA BIBCCJ E A LGPD

A BIBCCJ, uma das mais tradicionais e importantes do país, coleta e processa uma vasta quantidade de dados pessoais de discentes, docentes, técnicos e pesquisadores. Por lidar diretamente com dados de diversas partes interessadas, a BIBCCJ deve adaptar seus procedimentos, principalmente na coleta, verificação, armazenamento, tratamento e disseminação dessas informações, oportunamente para modernizar a sua gestão de dados pessoais, o que demanda a implementação de políticas e práticas adequadas de governança de dados.

Além disso, a proteção de dados pessoais está cada vez mais associada à reputação institucional, sendo fundamental que a biblioteca adote políticas transparentes e robustas para fortalecer a confiança de seus usuários, garantindo a preservação das informações pessoais e mitigando riscos associados à violação da privacidade. Isso é especialmente relevante para instituições de ensino e pesquisa, sendo as bibliotecas destes órgãos espaços socioculturais que dispõem de produtos e serviços informacionais. Nesse sentido, a American Library Association (ALA) ressalta a importância do direito à privacidade no exercício do serviço público de todas as bibliotecas, como fóruns de informação e de ideias.

> Todas as pessoas, independentemente de origem, idade, formação ou ponto de vista, possuem o direito à privacidade e confidencialidade no uso da biblioteca. As bibliotecas devem advogar, educar e proteger a privacidade das pessoas, salvaguardando todos os dados de uso da biblioteca, incluindo informações de identificação pessoal. (AMERICAN LIBRARY ASSOCIATION, 1996, tradução minha).

Para operações como registro de empréstimos, acesso a bases de dados e comunicação com o usuário, a aplicação da LGPD na BIBCCJ define os seguintes papéis: O Titular de Dados é, primariamente, o aluno, professor ou funcionário que se cadastra na biblioteca. Ele é a ponta da cadeia, a pessoa física a quem os dados, o foco da proteção legal, pertencem; A FDR atua como controlador, pois é quem toma as decisões sobre a finalidade e a forma como esses dados são utilizados no sistema da biblioteca; por fim, os operadores são os profissionais, entre técnicos e bibliotecários, responsáveis por executar as tarefas de coleta, processamento, armazenamento ou descarte de dados pessoais, conforme as determinações estabelecidas pela alta direção da instituição.

A BIBCCJ coleta dados pessoais, como por exemplo: nome completo; matrícula; número de registro no cadastro de pessoa física (CPF); número da

identidade (RG); endereço; telefone fixo e celular; lista de livros retirados; lista de doadores de livros; estatística de empréstimo; biometria utilizada como autenticação de cadastro; e o levantamento do perfil do usuário para a disseminação seletiva da informação, os quais passam a ser abordados a seguir, no sentido de responder a pergunta central que norteia a pesquisa: quais medidas institucionais devem ser adotadas pela Biblioteca da Faculdade de Direito do Recife para garantir a adequação à LGPD e assegurar a proteção dos dados pessoais de seus usuários?

4.1 DADOS PESSOAIS NA BIBCCJ

O ponto de partida para a conformidade é o mapeamento completo dos dados coletados, armazenados e tratados. A BIBCCJ, no desempenho de suas funções informacionais e socioculturais , lida com um grande volume de informações que permitem a identificação de seus usuários, caracterizando-os como dados pessoais, informação relacionada a pessoa natural identificada ou identificável.

Conforme levantamento realizado para a presente pesquisa, a lista de dados pessoais coletados pela biblioteca engloba, mas não se limita a:

1. Dados de Identificação e Contato: Nome completo, CPF, RG, e-mail, telefone (fixo e celular), login adicional e foto.
2. Dados Residenciais: Endereço, rua, número, complemento, bairro, CEP, cidade, UF e nacionalidade.
3. Dados Institucionais/Acadêmicos: Matrícula, categoria de usuário, nível de autorização, tipo de empréstimo, situação/unidade de informação, situação/instituição e unidade de informação.
4. Dados de Registro: Data de cadastro, data de nascimento, validade, senha, via da carteira, nome do arquivo da foto, demais informações, mensagem de aviso e informações restritas.
5. Dados Estatísticos e Histórico: Escolaridade e histórico (lista de livros retirados).

4.2 DADOS SENSÍVEIS NA BIBCCJ

A LGPD estabelece uma categoria de dados que exige maior rigor no tratamento: os dados pessoais sensíveis. Estes são definidos como aqueles

referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Tais informações são consideradas íntimas e potencialmente discriminatórias, exigindo consentimento específico, destacado e explícito para seu tratamento, salvo exceções legais.

No contexto da BIBCCJ, destacam-se como dados sensíveis:

1. Deficiência: A coleta desta informação é um dado sensível referente à saúde, utilizado pela biblioteca, por exemplo, para garantir a adequada acessibilidade e o tratamento no atendimento.
2. Gênero: Embora a LGPD não o liste explicitamente, seu tratamento é frequentemente associado a dados potencialmente discriminatórios. É um dado coletado para adequado tratamento no atendimento.
3. Biometria: A biometria utilizada como autenticação de cadastro também se classifica como dado sensível conforme a lei (dado biométrico).

Para o tratamento destes dados sensíveis, a base legal deve ser rigorosamente observada. Em órgãos públicos como a FDR, a coleta pode se justificar pela implementação e execução de políticas públicas que requerem o mapeamento de informações como raça ou deficiência para fins estatísticos ou de garantia de direitos.

4.3 DADOS ANONIMIZADOS NA BIBCCJ

A anonimização é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Quando os dados são anonimizados, eles deixam de ser regidos pela LGPD, o que pode ser uma estratégia importante para o tratamento de grandes massas de dados.

A LGPD, em seu Art. 5º, III, define o dado anonimizado como "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

A prática da biblioteca deve observar se dados como o histórico de livros retirados e o levantamento do perfil do usuário para a disseminação seletiva da informação são devidamente anonimizados antes de seu uso para finalidades

genéricas, como relatórios institucionais ou estatísticas. Por exemplo, o preenchimento de dados de auto identificação com finalidade exclusivamente estatística não deve identificar o usuário, garantindo assim a anonimização dos dados coletados.

5 DESAFIOS NO TRATAMENTO DE DADOS: análise dos requisitos legais

A conformidade com a LGPD exige que toda operação de tratamento de dados esteja fundamentada em uma das bases legais previstas nos Artigos 7º e 11 da Lei. Para instituições que atuam no serviço público, como é o caso em análise, o tratamento de dados pessoais é viabilizado por um conjunto específico de critérios jurídicos.

5.1 AS BASES LEGAIS PARA O PROCESSAMENTO DE DADOS PESSOAIS

O Artigo 7º da LGPD estabelece as condições sob as quais o tratamento de dados pessoais é lícito, sendo as mais pertinentes para o contexto do serviço público:

1. Consentimento do Titular (Art. 7º, I): O tratamento pode ocorrer mediante o fornecimento de consentimento pelo titular. O consentimento é definido como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018, art. 5º, XII). Sua relevância é destacada pelas políticas de privacidade, que se tornam pressuposto para a autorização do usuário;
2. Execução de Contrato ou Procedimentos Preliminares (Art. 7º, V): O tratamento é permitido quando for essencial para a execução de um contrato ou de procedimentos preliminares a ele relacionados, do qual o titular dos dados seja parte. No serviço público, a coleta de dados é necessária, por exemplo, para a formalização de um contrato de empréstimo de bem público, como o comodato de um material do acervo;
3. Interesse Público e Boa-fé (§ 3º do Art. 7º): Mesmo que o dado pessoal seja de acesso público, seu tratamento deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. A boa-fé é, portanto, um elemento necessário para a prestação do serviço.

Apesar de o consentimento ser uma base legal aplicável, a confiança do usuário na instituição como um ambiente seguro para o armazenamento de seus dados e o interesse legítimo do serviço também se aplicam, conforme a doutrina

(BIONI, 2019). É imperativo, todavia, que o titular seja sempre informado sobre o uso e a finalidade do tratamento, possuindo o direito de acesso, retificação, apagamento e restrição do processamento de seus dados.

5.2 AS BASES LEGAIS PARA O PROCESSAMENTO DE DADOS SENSÍVEIS

Pensando no tratamento de dados sensíveis, existem alguns requisitos para que uma biblioteca possa processá-los que estão elencados no artigo 11 da LGPD. Para além da condição referida acima, que guarda relação com o consentimento do titular, existe a previsão legal nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, como o utilizado pela BIBCCJ, na garantia da prevenção à fraude e à segurança do titular de dados (Art. 11, II, g).

Dessa forma, o tratamento de dados sensíveis é permitido, mesmo sem o consentimento do titular, quando for indispensável para a proteção do próprio titular contra usos indevidos ou fraudulentos, como na verificação de identidade para acesso a serviços ou sistemas.

5.3 OUTROS DESAFIOS: o compartilhamento e a interoperabilidade de dados pelo poder público

O compartilhamento de dados é um tema que exige rigorosa análise, devendo ser pautado pela confiança e pelo princípio da finalidade. Os Artigos 25 e 26 da LGPD tratam especificamente da interoperabilidade e do compartilhamento de dados públicos:

> Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.
> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6o desta Lei.
> § 1o É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
> I - em casos de execução descentralizada de atividade pública que

> exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei no 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
> II - (VETADO);
> III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
> IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou
> V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.
> § 2o Os contratos e convênios de que trata o § 1o deste artigo deverão ser comunicados à autoridade nacional.

A avaliação da legalidade do compartilhamento frequentemente alcança o âmbito judicial, como ilustrado pela suspensão de medida provisória pelo Supremo Tribunal Federal em 2020. Na ocasião, o STF suspendeu o compartilhamento de dados de usuários de telecomunicações com o IBGE, pautando-se na violação da inviolabilidade da intimidade e do sigilo de dados, e exigindo a avaliação da necessidade, relevância, urgência, razoabilidade e proporcionalidade da medida. Esse precedente reforça a necessidade de que os órgãos públicos, que incluem instituições integrantes da administração direta ou indireta , avaliem criteriosamente a necessidade de compartilhamento, evitando usos que possam ter finalidades diversas daquelas para as quais os dados foram originalmente coletados.

6 RESPONSABILIDADE E CONSEQUÊNCIAS DO DESCUMPRIMENTO DA LGPD

O descumprimento da LGPD por instituições públicas implica responsabilidade e pode gerar consequências jurídicas severas. O Art. 23 da Lei impõe ao Poder Público a obrigação de adequação, estabelecendo que o tratamento de dados pessoais deve ser realizado para o atendimento de sua finalidade pública específica.

A atuação do agente de tratamento deve ser balizada pelos princípios da lei, sobretudo o Princípio da Finalidade, que determina que o tratamento deve ocorrer para "propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018, art. 5º, II, art. 6º). O tratamento que não atende a essa finalidade, como aquele realizado com o intuito de melhor atender o usuário por meio de um serviço individualizado, pode incorrer em descumprimento da LGPD.

A proteção diferenciada de dados sensíveis – como dados biométricos, que exigem atenção especial por afetarem a intimidade dos indivíduos – intensifica a responsabilidade dos agentes públicos. A lei de proteção de dados possui implicações econômicas e políticas internas e externas, e todas as instituições que tratam dados pessoais, incluindo as entidades públicas, estão sujeitas à necessidade de adequação. A inobservância dessas regras acarreta responsabilidade e a possível aplicação de sanções administrativas e judiciais.

7 A ADEQUAÇÃO INSTITUCIONAL: BOAS PRÁTICAS E SEGURANÇA JURÍDICA

A adequação à LGPD é um processo contínuo que envolve a adoção de medidas técnicas e administrativas, visando a segurança dos dados e o cumprimento dos princípios legais. A partir de uma análise crítica da práxis da BIBCCJ confrontada com a LGPD, torna-se possível elencar boas práticas a serem implementadas em caráter corretivo, de aprimoração e, até mesmo de inovação, no sentido de oferecer serviços mais adequados ao público usuário, ou mesmo internos e entre outras instituições análogas.

7.1 TRANSPARÊNCIA E INFORMAÇÃO AO TITULAR DE DADOS PESSOAIS

O princípio da transparência é essencial e se materializa por meio de documentos claros de política de privacidade. As plataformas institucionais devem prever espaço para informações detalhadas sobre a coleta e o tratamento dos dados pessoais, como a forma como os dados são coletados; a finalidade clara e específica do tratamento; a legitimação existente para o tratamento; e o local de armazenamento dos dados.

Para além da necessidade do consentimento, a coleta dos dados de uma biblioteca é necessária para execução de um contrato de empréstimo de bem público, nesse caso um livro ou outro material do acervo. O titular dos dados apesar de fornecer o consentimento, possui direitos individuais de ser informado sobre o uso que será dado aos seus dados e a finalidade expressa do consentimento; de acessar esses dados; de retificá-los; de apagá-los; de restringir seu processamento e de não estar sujeito a decisões e perfis automatizados.

Uma cartilha de autoria da BIBCCJ disponibilizada ao público usuário é exemplo de uma boa prática a ser implementada na garantia da transparência e informação ao titular de dados pessoais em conformidade com a LGPD. A Tabela 1 explicita os dados da composição deste documento.

Tabela 1 - Protótipo de Cartilha

Dados coletados.	Dados de identificação (nome, matrícula, endereços residencial, comercial ou eletrônico, números de telefone, etc.); fotografia e biometria.
A forma de coleta dos dados.	Por meio do formulário de consentimento, de mensagens eletrônicas enviadas à biblioteca, etc.
A finalidade da coleta dos dados.	Inscrição na biblioteca para fazer uso do empréstimo domiciliar e entre bibliotecas, serviço de disseminação seletiva da informação, outros.
A forma de armazenamento e tratamento dos dados.	Bases de dados da biblioteca, outros.
A forma de proteção dos dados.	Meios de segurança utilizados para proteger os dados, treinamento para todos os funcionários da biblioteca sobre o conteúdo da LGPD, outras formas.
Os direitos dos usuários em relação aos seus dados pessoais.	Direito ao consentimento; de confirmação da existência do tratamento; de acesso aos dados e de correção de dados incompletos, inexatos ou desatualizados; de eliminação dos dados; de revogação do consentimento.
A forma de contato com a biblioteca.	Fisicamente, correspondência, mensagem eletrônica, outros.
As mudanças na política de privacidade da biblioteca.	Temporalidade, forma de aviso aos usuários, etc.

Fonte: O autor (2025)

7.2 MEDIDAS TÉCNICAS E ANONIMIZAÇÃO

A segurança dos sistemas que abrigam dados pessoais é uma preocupação necessária para garantir a privacidade e o cumprimento do marco regulatório. Dos mecanismos de segurança técnica, destaca-se como fundamental, o processo de anonimização dos dados. A aplicação da anonimização, quando possível, garante que a informação possa ser utilizada para fins estatísticos e de pesquisa sem a total incidência da lei, o que vem a ser crucial estrategicamente para a elaboração de relatórios, como aqueles concernentes a histórico de multas ou de empréstimos de livros.

Portanto a BIBCCJ observaria adequadamente a LGPD, ao garantir que todas as informações coletadas e respostas às perguntas fornecidas para a elaboração do relatório em análise serão anonimizadas. De forma que quaisquer informações pessoais ou potencialmente identificáveis serão removidas ou alteradas antes que os resultados sejam compartilhados em um relatório e tornados públicos.

7.3 O PERÍODO DE RETENÇÃO E CONSERVAÇÃO DOS DADOS

O tempo de tratamento dos dados deve seguir o Art. 15 da LGPD, que estabelece as hipóteses para o término do tratamento, como o alcance da finalidade e o fim do período de retenção necessário.

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
> II - fim do período de tratamento;
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
> IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Pragmaticamente, a BIBCCJ deve promover o descarte dos dados dos alunos que não tem mais vínculo com a instituição como premissa operacional implementadora de boas práticas. Por exemplo, discentes formados não configuram usuários e, portanto, seus dados pessoais podem ser excluídos do repositório da biblioteca sem prejuízo ao princípio da finalidade.

7.4 OS DIREITOS AUTORAIS SOB A PERSPECTIVA DA PROTEÇÃO DAS BASES DE DADOS

A Lei Nº 9.610/98, conhecida por Lei de Direitos Autorais (LDA), protege as criações intelectuais, regulando a relação entre o autor e sua obra, incluindo o controle sobre a circulação por terceiros. Especificamente para bases de dados, o artigo 87 da LDA assegura ao titular o direito exclusivo sobre a forma de expressão e a estrutura dessa base.

Por outro lado, a LGPD permite em seu artigo 13 que órgãos de pesquisa em saúde pública acessem bases de dados pessoais, desde que o uso seja estritamente para estudos, adotando a anonimização sempre que possível. Um exemplo prático disso é o repositório COVID-19 Data Sharing/BR da FAPESP, que compartilha dados de pacientes, como internações e desfechos, com o devido tratamento de pseudonimização.

Diante disso, as bases de dados, armazenadas pela biblioteca e compostas por trabalhos de conclusão de curso de seus usuários, requerem uma dupla proteção legal: a do Direito Autoral, que protege a seleção, organização ou disposição do conteúdo; e a da LGPD, exigindo a anonimização ou pseudonimização dos dados pessoais. Assim, é essencial que a LDA e a LGPD atuem de forma complementar para garantir a circulação segura e correta das informações, respeitando tanto a proteção dos dados pessoais quanto o direito de autor do titular da base organizada.

8 CONSIDERAÇÕES FINAIS

O presente estudo objetivou analisar a aplicação da LGPD e as medidas de adequação necessárias no contexto do serviço público, especificamente em uma instituição de ensino e pesquisa. A análise demonstrou que o tratamento de dados pessoais por essas entidades enquadra-se integralmente no que a LGPD direciona para o Poder Público, exigindo o rigoroso cumprimento das bases legais, sobretudo a execução de políticas públicas e o cumprimento de obrigação legal.

A conformidade com a LGPD não se restringe à mera observância formal das normas, mas demanda uma profunda mudança de cultura institucional, que se apoia na transparência, na segurança dos sistemas e na adesão às boas práticas, como a adoção de protocolos de criptografia e a anonimização de dados quando a finalidade assim o permitir.

As preocupações com a forma como os dados são coletados, a finalidade de seu uso e a segurança dos sistemas de armazenamento são essenciais para garantir a privacidade e o cumprimento legal sobre o tema. Espera-se que as conclusões deste trabalho sirvam de subsídio para a implementação de um programa de governança de dados eficaz, mitigando os riscos de responsabilização e assegurando os direitos fundamentais dos titulares.

REFERÊNCIAS

AMERICAN LIBRARY ASSOCIATION. Library Bill of Rights. Chicago, IL: American Library Association, 1996. Disponível em: https://www.ala.org/advocacy/intfreedom/librarybill. Acesso em: 10 out. 2025.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Ed. Forense. 3ª ed. Rio de Janeiro. 2021.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 23/09/2024.

BRASIL. Decreto-Lei nº 4.657, de 4 de setembro de 1942. Lei de Introdução às normas do Direito Brasileiro. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm. Acesso em: 23/09/2024.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 23/09/2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23/09/2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados (LGPD). Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23/09/2024.

BRASIL. Lei n. 13.853, de 8 de julho de 2019. Brasília, DF. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em:

http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2. Acesso em: 23/09/2024.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade (ADI) 6387. Relatora: Min. Rosa Weber. Data do julgamento: 24/04/2020. Disponível em: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf. Acesso em: 27/05/2025.

CARDOZO, Teodomiro et al. Crimes praticados na Internet: breve visão da necessidade de uma legislação penal para tutelar os bens jurídicos na rede mundial de computadores. In: CARDOZO, Teodomiro et al (Coord.). Ciências Criminais no Século XXI. Recife-PE: Editora Universitária UFPE, 2007. 325-336.