

LGPD, SIGILO PROFISSIONAL E PROTEÇÃO DE DADOS NA ADVOCACIA

João Batista Soares da Costa Junior¹.

¹Universidade Salgado de Oliveira – UNIVERSO, Rio de Janeiro, RJ.

<https://lattes.cnpq.br/3514185117159229>

RESUMO: O artigo examina a convergência normativa entre o dever de confidencialidade estabelecido pelo Estatuto da Ordem dos Advogados do Brasil e as novas obrigações legais impostas pela Lei Geral de Proteção de Dados Pessoais no cotidiano dos escritórios jurídicos. O objetivo central consiste em analisar os mecanismos práticos e operacionais que permitem implementar a conformidade regulatória sem promover a erosão das prerrogativas tradicionais da classe, delimitando o perímetro de responsabilidade civil das bancas. Utilizando metodologia baseada na revisão bibliográfica narrativa combinada com análise documental, a pesquisa investiga o arco argumentativo que qualifica a segurança da informação como obrigação legal de controladoria e imperativo de sustentabilidade mercadológica. Os resultados demonstram que a harmonização prática ocorre por meio de uma governança corporativa estruturada, que integra políticas de integridade a salvaguardas técnicas, como criptografia e autenticação multifator. O estudo conclui que a adequação procedimental e o mapeamento de processos convertem o segredo em um direito protegido por ferramentas tecnológicas rigorosas. Esse modelo inovador mitiga os riscos de incidentes cibernéticos e de sanções disciplinares, consolidando a relação fiduciária com o constituinte e reconhecendo o cidadão como titular de garantias fundamentais na atual sociedade conectada.

PALAVRAS-CHAVE: Confidencialidade. Responsabilidade Civil. Compliance Digital.

LGPD, PROFESSIONAL SECRECY, AND DATA PROTECTION IN THE LEGAL PROFESSION

ABSTRACT: The article examines the normative convergence between the duty of confidentiality established by the Statute of the Brazilian Bar Association (OAB) and the new legal obligations imposed by the General Data Protection Law (LGPD) in the daily operations of law firms. The central objective is to analyze the practical and operational mechanisms that allow for the implementation of regulatory compliance without eroding the traditional prerogatives of the legal profession, while defining the scope of civil liability for firms. Using a methodology based on a narrative literature review combined with documentary analysis,

the research investigates the argumentative framework that qualifies information security as both a legal obligation of data controllership and a market sustainability imperative. The results demonstrate that practical harmonization occurs through structured corporate governance, which integrates integrity policies with technical safeguards such as encryption and multi-factor authentication. The study concludes that procedural adaptation and process mapping convert professional secrecy into a right protected by rigorous technological tools. This innovative model mitigates the risks of cyber incidents and disciplinary sanctions, consolidating the fiduciary relationship with the client and recognizing the citizen as a holder of fundamental guarantees in today's connected society.

KEY-WORDS: Confidentiality. Civil Liability. Digital Compliance.

INTRODUÇÃO

A emergência da sociedade da informação e a consolidação de uma economia intensiva em dados transformaram profundamente a dinâmica operacional das instituições públicas e das corporações privadas, estabelecendo novos desafios para a preservação dos direitos da personalidade no cenário contemporâneo. Nesse ecossistema digital complexo, o trânsito massivo de informações pessoais e o desenvolvimento de ferramentas de inteligência artificial alteraram as estruturas tradicionais de comunicação, demandando do ordenamento jurídico respostas regulatórias céleres para conter abusos e mitigar riscos cibernéticos. Os escritórios de advocacia, enquanto depósitos históricos de volumes expressivos de dados sensíveis e segredos de negócio, encontram-se inseridos de forma irrestrita nessa realidade mercadológica, uma vez que a execução regular de suas atividades-fim depende da contínua manipulação de registros de seus constituintes. Essa nova conjuntura tecnológica exige a superação de modelos abstratos de gestão e impõe às sociedades de advogados a necessidade urgente de compreender os dados não apenas como insumos processuais ordinários, mas como ativos revestidos de relevância jurídica e merecedores de salvaguardas estruturais permanentes.

Antes mesmo do advento de legislações abrangentes dedicadas exclusivamente à privacidade digital, o ordenamento jurídico nacional já dispunha de balizas deontológicas consolidadas para assegurar a confidencialidade na relação entre o advogado e seu constituinte como pressuposto para a administração da justiça. O Estatuto da Advocacia e da Ordem dos Advogados do Brasil estabelece a inviolabilidade dos arquivos, registros e correspondências do defensor como uma garantia de ordem pública voltada a viabilizar o livre exercício da ampla defesa e o pleno funcionamento do princípio do contraditório. Contudo, a entrada em vigor da Lei Geral de Proteção de Dados introduziu um microssistema regulatório inédito que impõe obrigações procedimentais e documentais complexas a todos os agentes econômicos que realizam operações de tratamento, sem prever exceções ou imunidades para o setor de serviços jurídicos. Esse cenário cria uma aparente tensão normativa no cotidiano das bancas de advocacia, uma vez que o mesmo agente profissional

encontra-se simultaneamente submetido a deveres tradicionais de segredo profissional e a novas exigências federais de transparência, livre acesso e compartilhamento seguro de informações sensíveis.

OBJETIVO

O objetivo central deste estudo consiste em analisar os mecanismos práticos e operacionais que permitem implementar a conformidade regulatória à LGPD no cotidiano das sociedades de advogados. Busca-se harmonizar essas novas obrigações legais com a manutenção do dever fundamental de sigilo profissional e das prerrogativas da classe. Sob essa perspectiva, complementarmente estabeleceu-se como objetivo secundário a delimitação do perímetro de responsabilidade civil envolvendo tal problematização, com isso, a investigação demonstra que o tratamento irregular de dados atrai a responsabilidade civil objetiva pautada no risco inerente à atividade de tratamento.

Paralelamente, delineou-se como segundo objetivo específico o exame do mapa de sanções concorrentes decorrentes do descumprimento das normativas de privacidade. A pesquisa detalha o cenário punitivo que submete o profissional simultaneamente às penalidades administrativas da ANPD e às sanções disciplinares do Tribunal de Ética da OAB. Por fim, a intenção do presente trabalho é demonstrar, de forma proativa que a governança e a adequação procedimental mitigam os riscos corporativos, salvaguardando a integridade institucional e consolidando a relação fiduciária com o constituinte na sociedade conectada.

METODOLOGIA

Para a concretização dos objetivos propostos neste estudo e com o fito de responder satisfatoriamente à problemática delineada, a investigação adota a metodologia jurídico-dogmática associada a uma abordagem qualitativa de natureza descritiva. O método de abordagem eleito é o hipotético-dedutivo, o qual se inicia com a formulação de um problema central voltado à compatibilização entre a LGPD e o Estatuto da Advocacia, propondo-se uma hipótese positiva a ser validada ao longo do percurso argumentativo. Esse delineamento metodológico afasta o exame isolado das regras, concentrando-se na compreensão das intersecções normativas que definem a controladoria jurídica e na identificação de soluções práticas de governança. Assim, o desenho da pesquisa estrutura-se para permitir a investigação do estado da arte doutrinário, garantindo a segurança jurídica necessária à análise da responsabilidade do profissional. No que concerne às técnicas de investigação, a pesquisa operacionaliza-se por meio de um amplo levantamento bibliográfico e de uma detalhada análise normativa e documental, coletando subsídios doutrinários em livros, artigos científicos e dissertações especializadas. O corpus foi selecionado de forma criteriosa mediante buscas em plataformas acadêmicas como o Portal de Periódicos

CAPES e o Google Scholar, priorizando a revisão da literatura jurídica atualizada sobre a governança de dados pessoais. A análise concentrou-se no exame crítico da legislação aplicável (notadamente a Lei nº 13.709 de 2018 e a Lei nº 8.906 de 1994), bem como na apreensão da jurisprudência incipiente dos tribunais superiores e em guias orientativos oficiais. Essa triangulação fornece a robustez teórica indispensável para estruturar as propostas de compliance aplicadas à realidade fática das sociedades de advogados.

O ESTATUTO DA ADVOCACIA E O DEVER FUNDAMENTAL DE SIGILO PROFISSIONAL

O ordenamento jurídico brasileiro confere ao profissional da advocacia uma posição de extrema centralidade na administração da justiça, estabelecendo a confidencialidade como um pilar intransponível para o regular exercício do devido processo legal e para a consolidação do Estado Democrático de Direito (Legale Educacional, 2026). Sob essa perspectiva constitucional, o Estatuto da Advocacia e da Ordem dos Advogados do Brasil, por meio da Lei nº 8.906 de 1994, consagra em seu artigo sétimo, inciso segundo a garantia de inviolabilidade de seu local de trabalho, abrangendo de forma absoluta todos os seus arquivos, dados cadastrais e registros confiados pelo constituinte no decurso do mandato (Brasil, 1994). Essa prerrogativa legal, longe de se constituir como um privilégio de natureza classista, qualifica-se substancialmente como uma proteção de ordem pública que visa resguardar a própria incolumidade dos direitos do cidadão, uma vez que a preservação do segredo profissional funciona como o alicerce fundamental sobre o qual se sustentam a ampla defesa e o princípio do contraditório (Olivari, 2021; Legale Educacional, 2026). Desse modo, o dever ético-deontológico de guardar sigilo sobre os fatos conhecidos no exercício da profissão, amplamente amparado pelo Código de Ética e Disciplina da OAB, projeta-se para além da esfera privada da relação contratual entre cliente e patrono, configurando uma salvaguarda institucional indispensável para impedir arbítrios e garantir que o direito de defesa não perca sua substância prática no tecido social.

No cenário de extrema complexidade que caracteriza a advocacia corporativa e empresarial, a manutenção dessa barreira de confidencialidade enfrenta desafios práticos severos quando autoridades estatais ou investigativas tentam compelir o causídico a fornecer dados cadastrais, endereços ou informações financeiras dos sócios e da pessoa jurídica. Essa modalidade de coerção governamental representa uma violação direta às prerrogativas profissionais estabelecidas pela legislação federal, visto que os documentos e diálogos recebidos sob o manto do sigilo destinam-se unicamente ao aconselhamento jurídico e ao pleno exercício da defesa técnica (Brasil, 1994). A submissão indevida a ordens de quebra de confidencialidade fora das estritas e raras exceções legais (como o risco iminente à vida ou à dignidade humana) desnatura completamente o sistema acusatório, sujeitando o profissional a severas penalidades administrativas e disciplinares aplicadas pelos Tribunais de Ética da Ordem, que podem culminar na exclusão dos quadros

institucionais, sem prejuízo da responsabilidade civil e criminal pelo delito de violação de segredo.

O advento da Lei Geral de Proteção de Dados (LGPD), por meio da Lei nº 13.709 de 2018, adicionou uma complexa camada regulatória que redimensionou o sigilo profissional, elevando-o de uma dimensão puramente deontológica para uma obrigação legal de segurança da informação com consequências civis e administrativas perfeitamente mensuráveis (Nicodemos, 2022). A cessão leviana ou o compartilhamento não judicializado de informações pessoais custodiadas pela banca rompe simultaneamente com os pilares éticos tradicionais da advocacia e com os princípios basilares de finalidade, adequação e necessidade previstos na nova legislação. Quando o escritório de advocacia ou seus sócios atuam na condição de controladores primários dos dados fornecidos para o ajuizamento de ações ou consultorias, passam a se submeter ao rigor do regime de responsabilidade civil objetiva, respondendo independentemente de culpa por incidentes de segurança, vazamentos ou acessos não autorizados que causem danos patrimoniais ou morais aos titulares. Constata-se, por conseguinte, que o tratamento irregular decorrente da inobservância de medidas técnicas e administrativas aptas a proteger a base de dados (como a falta de criptografia, de controle de acessos ou o armazenamento inadequado) enseja uma ruptura concomitante das normativas corporativas e legais, sujeitando a sociedade de advogados a pesadas indenizações cíveis e a severas sanções administrativas impostas pela autoridade nacional, as quais fragilizam de forma severa a reputação profissional do escritório no mercado.

MECANISMOS PRÁTICOS DE ADEQUAÇÃO E GOVERNANÇA

A categorização jurídica dos escritórios de advocacia perante a LGPD pressupõe o reconhecimento de sua posição como controladores de dados pessoais, uma vez que as bancas e seus sócios gestores detêm o poder de decisão sobre as finalidades e os meios de tratamento das informações que transitam em suas estruturas operacionais. Essa qualificação técnica, estabelecida na legislação federal, estende-se à coleta e ao processamento de dados biográficos e contratuais pertencentes a uma multiplicidade de sujeitos, englobando não apenas os clientes da banca, mas também o corpo de colaboradores internos, advogados associados, estagiários e parceiros comerciais externos. Consequentemente, ao assumir as diretrizes estratégicas das operações de tratamento, o profissional do direito afasta qualquer alegação de imunidade setorial, incorporando à sua rotina jurídica um rol de obrigações institucionais cujo cumprimento é pressuposto direto para salvaguardar os direitos fundamentais de liberdade e privacidade dos indivíduos. Toda atividade que configure operação com dados, desde o atendimento de consultas preliminares até o ajuizamento de demandas complexas, deve ser parametrizada por essa condição jurídica de controladoria, o que impõe a vinculação das noções de controle e de zelo técnico à atividade advocatícia regular (Pimentel, 2023).

Sob o prisma da responsabilidade proativa, a conformidade das sociedades de advogados às exigências regulatórias nacionais demanda a implementação sistemática de um programa de *compliance* operacional estruturado, o qual seja capaz de materializar o princípio da prestação de contas (*accountability*) por meio de evidências de regularidade (CEPPD, 2021). Essa necessidade de adequação procedimental ultrapassa a simples modificação de minutas contratuais ou a inserção de cláusulas genéricas, exigindo a evolução contínua de uma cultura interna de integridade que interligue o planejamento estratégico da organização às operações mais rotineiras realizadas pelas equipes. Considerando que o monitoramento deve ser constante em virtude da modificação de processos e do ingresso de novos colaboradores, as iniciativas de *compliance* precisam ser encaradas como fluxos permanentes na vida institucional da banca, os quais funcionam como um anteparo técnico apto a reduzir a exposição a riscos (OAB Alagoas, 2022). Desse modo, a criação de processos organizacionais rigorosos confere respaldo jurídico ao escritório em eventual escrutínio pela autoridade fiscalizadora, transformando a governança em privacidade em um requisito de sobrevivência mercadológica e de preservação da própria reputação institucional.

SEGURANÇA DA INFORMAÇÃO E O REFORÇO ESTRUTURAL AO ESTATUTO

A implementação de medidas técnicas de proteção, em estrita observância ao artigo quarenta e seis da legislação federal, impõe aos escritórios a adoção de barreiras tecnológicas idôneas e atualizadas para resguardar as informações pessoais virtuais contra acessos não autorizados ou incidentes de segurança cibernética (Alencar, 2023). A segurança lógica do ambiente corporativo requer a inserção de controles como sistemas de criptografia em repouso e em trânsito, mecanismos de autenticação multifator para acesso a sistemas internos e defesas de rede robustas por meio de *firewalls* (OAB Alagoas, 2022). Esses mecanismos técnicos minimizam a vulnerabilidade da infraestrutura digital da banca e funcionam como um reforço estrutural ao dever tradicional de confidencialidade, reduzindo os riscos de vazamentos de dados de clientes (Lima, 2021).

A governança interna voltada à comunicação segura exige que as bancas controlem o fluxo de transmissão de mensagens eletrônicas, e-mails e plataformas de gestão jurídica, evitando a utilização de canais públicos ou desprovidos de ferramentas de segurança adequadas. O uso consciente de ferramentas cotidianas, incluindo o uso responsável das opções de cópia oculta no encaminhamento de e-mails corporativos e o emprego de tecnologias de rede virtual privada para comunicações externas, mitiga riscos de interceptação indevida de segredos de negócio (CEPPD, 2021). Adicionalmente, o manuseio de aplicativos de mensagens instantâneas para a troca de documentos e dados sensíveis de clientes deve ser objeto de diretrizes internas severas, uma vez que o encaminhamento equivocado de arquivos a terceiros estranhos à relação profissional caracteriza incidente de segurança grave.

Paralelamente, a adoção de uma Política de Mesa Limpa, que veda a colagem de anotações com logins e senhas em monitores e restringe a exposição física de pastas de clientes, atua de forma preventiva na redução de vulnerabilidades visuais no ambiente de trabalho (Nicodemos, 2022).

O desfecho do ciclo de vida dos dados pessoais em posse da sociedade de advogados deve ser amparado por rotinas de retenção temporária e de descarte seguro, as quais determinam a trituração física ou a eliminação digital definitiva das informações obsoletas (OAB Alagoas, 2022). Os procedimentos de descarte digital demandam o uso de ferramentas de segurança da informação capazes de atestar que os dados eliminados por decurso de finalidade não remanesçam acessíveis em servidores locais ou em cópias de segurança na nuvem (CEPPD, 2021). Desse modo, o estabelecimento de critérios temporais rígidos para o armazenamento evita o acúmulo de volumes informacionais desnecessários, reduzindo o perímetro de exposição do escritório no mercado e garantindo o atendimento ao princípio da necessidade.

INFRAÇÕES DISCIPLINARES E RESPONSABILIDADE CIVIL DO ADVOGADO

A caracterização jurídica da responsabilidade civil dos escritórios de advocacia encontra fundamento no risco inerente ao manuseio, armazenamento e tratamento de dados pessoais. Sob a égide do artigo 42 da Lei Geral de Proteção de Dados, a obrigação de reparar danos patrimoniais, morais, individuais ou coletivos emerge a partir do momento em que a atividade de processamento de informações viola a legislação protetiva ou deixa de fornecer a segurança que o titular legitimamente poderia esperar do prestador de serviços. Esse modelo de responsabilização proativa inverte o ônus probatório processual e prescinde da verificação de dolo ou negligência, exigindo do julgador apenas a constatação do dano efetivo, do nexo causal e da desconformidade procedimental da controladoria jurídica. Desse modo, o ordenamento vincula a reparação civil ao risco sistêmico da atividade econômica exercida pelas bancas de advocacia, estabelecendo que a manutenção de bancos de dados contendo informações sensíveis de clientes atrai um severo dever de indenizar sempre que a quebra da expectativa de segurança comprometer de forma injustificada os direitos da personalidade dos indivíduos.

Para além da esfera estritamente reparatória cível, o descumprimento dos deveres de segurança da informação e a cessão indevida ou não judicializada de informações de clientes repercutem severamente na esfera administrativa e profissional, configurando infração disciplinar gravíssima tipificada de forma expressa no Estatuto da Advocacia e da Ordem dos Advogados do Brasil. O artigo trinta e quatro, inciso sétimo, da Lei nº 8.906 de 1994, estabelece que a violação injustificada do segredo profissional rompe o vínculo fiduciário essencial da profissão, sujeitando o infrator a um cenário de concorrência de penalidades celeremente fiscalizado por órgãos distintos. Enquanto a Autoridade Nacional de Proteção de Dados atua na esfera administrativa impondo sanções severas (que variam

de advertências com prazos para adoção de medidas corretivas e publicização obrigatória da infração até multas que podem atingir o patamar de cinquenta milhões de reais ou o bloqueio definitivo das bases de dados), o Tribunal de Ética e Disciplina da OAB processa o causídico de forma autônoma. Desse modo, o profissional submete-se paralelamente às penas éticas de censura, suspensão temporária do exercício da profissão ou exclusão definitiva dos quadros da Ordem, evidenciando que a adequação procedimental e técnica deixou de ser uma mera opção administrativa para se converter em um imperativo jurídico absoluto voltado à sustentabilidade da própria atividade advocatícia no mercado.

CONCLUSÃO

A convergência normativa entre o dever de confidencialidade estabelecido pela deontologia da classe e as modernas obrigações de privacidade impostas pela legislação federal revela que a conformidade não se estabelece por meio da exclusão de um ordenamento em detrimento do outro. Pelo contrário, a harmonia prática entre o Estatuto da Advocacia e as diretrizes de proteção de dados demonstra que ambos os sistemas normativos visam resguardar direitos fundamentais de matriz comum, voltados à tutela da dignidade da pessoa humana e ao livre desenvolvimento da personalidade no ambiente tecnológico. Compreende-se que as exigências de conformidade funcionam como um reforço de legalidade que reposiciona a tradicional confiança fiduciária da advocacia dentro de uma “infoesfera” marcada pela circulação massiva e opaca de informações sensíveis. Desse modo, o diálogo das fontes normativas confere à advocacia contemporânea o substrato jurídico necessário para que o cumprimento das regras de privacidade atue em perfeita sincronia com as prerrogativas profissionais há muito consagradas, consolidando a legalidade dos processos e a segurança das relações jurídicas estabelecidas entre o patrono e seu constituinte no tecido da sociedade conectada.

A solução prática para os impasses diários vivenciados pelos escritórios de advocacia reside na construção de uma arquitetura de proteção de dados que transforme o sigilo abstrato em uma obrigação técnica e procedimental de segurança da informação permanentemente auditável. Essa transição corporativa viabiliza-se por meio da implementação de ferramentas de gestão integradas (como o registro de operações de tratamento e a confecção minuciosa de relatórios de impacto à privacidade) que mapeiam o ciclo de vida completo dos dados coletados dentro da organização jurídica. Ao adotar salvaguardas tecnológicas robustas (incluindo a criptografia de fluxos documentais, a autenticação multifator e políticas rigorosas de descarte de arquivos obsoletos), as bancas delimitam com precisão o perímetro de acesso às informações. Essa governança de dados estruturada afasta as vulnerabilidades sistêmicas e assegura que os direitos fundamentais do cliente sejam respeitados em cada fase do mandato, convertendo as boas práticas de segurança em um mecanismo indissociável do exercício regular do direito de defesa e da preservação do segredo profissional diante das novas demandas tecnológicas.

O enquadramento da atividade advocatícia sob o rigoroso regime de responsabilidade civil objetiva consolida a premissa de que a segurança dos dados pessoais deixou de ser uma recomendação puramente gerencial para se tornar um imperativo jurídico absoluto relacionado à própria sustentabilidade da banca. A constatada vulnerabilidade cibernética que possibilita incidentes decorrentes de falhas internas de prepostos ou ataques externos configura fortuitos internos que atraem o dever imediato de indenizar, expondo os escritórios a prejuízos patrimoniais e extrapatrimoniais severos causados à personalidade dos titulares. Adicionalmente, a concorrência entre as severas sanções administrativas impostas pela autoridade nacional e as penalidades ético-disciplinares aplicadas pelos Tribunais de Ética da Ordem dos Advogados do Brasil reforça a gravidade do descumprimento das normativas de privacidade. Diante desse mapa de riscos complexos, o investimento em programas de conformidade digital e o treinamento exaustivo das equipes tornam-se mecanismos vitais para evitar a ruína financeira da corporação e impedir que transgressões procedimentais resultem na cassação do próprio direito de exercício profissional por quebra indevida de sigilo.

Em última análise, a consolidação da conformidade com as regras de proteção de dados no cenário da advocacia nacional redesenha a relação de confiança entre o cidadão e seu defensor, estabelecendo o advogado na posição de fiduciário legítimo desses novos direitos constitucionais. O reconhecimento de que o cliente é o titular exclusivo de suas próprias informações orienta a conduta das bancas contemporâneas para uma atuação pautada pela transparência máxima e pelo respeito à autodeterminação informativa. Essa transformação cultural da gestão legal mitiga os perigos da litigância excessiva e dos danos reputacionais, qualificando as sociedades de advogados adequadas como referências de integridade e cuidado ético perante um mercado altamente concorrencial e exigente. Portanto, ao edificar estruturas internas que harmonizam as obrigações deontológicas clássicas com a vanguarda regulatória cibernética, a advocacia reafirma sua indispensabilidade institucional para a administração da justiça, garantindo que a evolução tecnológica não aniquile as franquias tradicionais da privacidade, mas coopere para o fortalecimento da dignidade humana.

REFERÊNCIAS

ALENCAR, Larissa Camargo Pinho de. Lei Geral de Proteção de Dados - LGPD e segurança na internet. **ReJuB - Revista Judiciária Brasileira**, Brasília, v. 5, ed. esp. Direito Digital, p. 429-447, jul./dez. 2023. Disponível em: https://www.rejub.jus.br/index.php/rejub/article/view/lei_geral_protecao_alencar. Acesso em: 14 jan. 2026.

ALMEIDA, Mario Henrique Silveira de. **Lei Geral de Proteção de Dados-LGPD: solidariedade na responsabilidade civil pela violação aos dados pessoais**. 2023. 150 f. Dissertação (Mestrado em Direito) - Centro Universitário de Brasília, Brasília, 2023. Disponível em: https://repositorio.uniceub.br/jspui/handle/123456789/dissertacao_mario_henrique_silveira.

Acesso em: 02 fev. 2026.

BRASIL. **Lei nº 8.906, de 4 de julho de 1994**. Dispõe sobre o Estatuto da Advocacia e a Ordem dos Advogados do Brasil (OAB). Brasília: Presidência da República, 1994. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: 02 abr. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 abr. 2026.

CAMPOS, Carlos Alberto Casanova. Considerações finais. In: OAB CAMPINAS. COMISSÃO ESPECIAL DE PRIVACIDADE E PROTEÇÃO DE DADOS. **Guia da LGPD aplicada aos escritórios de advocacia**. Campinas: OAB Campinas, 2021. p. 69. Disponível em: https://oabcampinas.org.br/wp-content/uploads/2021/12/Guia-LGPD_Advocacia.pdf. Acesso em: 18 fev. 2026.

FERNANDES, Marcelo Eloy; NUZZI, Ana Paula Eloy. Fundamentos da Lei Geral de Proteção de Dados (LGPD): uma revisão narrativa. **Research, Society and Development**, v. 11, n. 12, e310111234247, p. 1-15, set. 2022. Disponível em: <https://rsdjournal.org/rsd/article/download/34247/29094/385272>. Acesso em: 15 mar. 2026.

LEGALE EDUCATIONAL. **Responsabilidade Civil LGPD**: como advogados atuam na proteção de dados. São Paulo: Legale, 06 set. 2025. Disponível em: <https://legale.edu.br/blog/responsabilidade-civil-lgpd-como-advogados-atuam-protecao-dados>. Acesso em: 03 mar. 2026.

MACIEL, Roberta Araújo de Carvalho. Considerações sobre a Lei Geral de Proteção de Dados Pessoais - LGPD, sua aplicação ao Poder Público e o compartilhamento de dados pessoais pelos órgãos públicos. **ReJuB - Revista Judiciária Brasileira**, Brasília, v. 5, ed. esp. Direito Digital, p. 257-284, jul./dez. 2023. Disponível em: https://www.rejub.jus.br/index.php/rejub/article/view/consideracoes_lei_geral_maciel. Acesso em: 14 jan. 2026.

MAIOLINO, Eurico Zecchin. LGPD e o Poder Judiciário: desafios de adequação e perspectivas. **ReJuB - Revista Judiciária Brasileira**, Brasília, v. 5, ed. esp. Direito Digital, p. 449-468, jul./dez. 2023. Disponível em: https://www.rejub.jus.br/index.php/rejub/article/view/lgpd_poder_judiciario_maiolino. Acesso em: 03 mar. 2026.

OAB ALAGOAS. COMISSÃO DE INOVAÇÃO, TECNOLOGIA E PROTEÇÃO DE DADOS. **Cartilha LGPD para escritórios de advocacia**. Maceió: OAB Alagoas, 2023. Disponível em: https://www.oab-al.org.br/app/uploads/2023/09/pdf_20220923_195050_0000.pdf. Acesso em: 14 jan. 2026.

PIMENTEL, Alexandre Freire. Responsabilidade objetiva do controlador de dados e função do encarregado na LGPD. **Revista Consultor Jurídico**, São Paulo, 11 mai. 2023. Disponível em: <https://www.conjur.com.br/2023-mai-11/pimentel-responsabilidade-objetiva-controlador-dados-encarregado-lgpd>. Acesso em: 14 jan. 2026.

STIVELBERG, Daniel T. O direito procedural da Lei Geral de Proteção de Dados (“LGPD”). In: **LGPD 2022**: debates e temas relevantes. São Paulo: PwC Brasil, 2022. p. 109-116. Disponível em: <https://www.pwc.com.br/pt/publicacoes/livro-lgpd-2022-debates-temas-relevantes.pdf>. Acesso em: 08 fev. 2026.