Centro de Documentação e Pesquisa

OABRJ

# PROTEÇÃO DE DANOS E PRIVACIDADE (LGPD): A CONSOLIDAÇÃO DO COMPLIANCE COMO INSTRUMENTO DE GOVERNANÇA E RESPONSABILIDADE

*Dayse Kubis Baumeier*[1]

[1] Advogada. Sócia fundadora do escritório Kubis Advogados Associados. Diretora Executiva de Patrocínio do IAB Nacional. Membro da Comissão de Inovação e IA do IAB. Membro da Comissão de Direitos Humanos do IAB. Especialista em Responsabilidade Civil. Direito de Empresa. Direitos Humanos. Direito Sucessório e Planejamento Patrimonial e Sucessório. Compliance e Proteção de Dados.

Resumo

A utilização de dados pessoais na economia digital teve um crescimento exponencial nos últimos anos e transformou a privacidade de dados em um dos principais direitos fundamentais da atualidade. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), vem para suprir um marco normativo no Brasil, voltado à proteção da dignidade da pessoa humana, da liberdade e da autodeterminação informativa, trazendo ao Brasil às tendências internacionais de regulação. A partir disso, a EC 115/2022, inseriu a proteção de dados na Constituição da República Federativa do Brasil, como direito fundamental.

O presente artigo a LGPD sob a ótica do *compliance,* destaca a implementação de estruturas organizacionais voltadas à governança de dados, com base nos princípios da transparência, finalidade e segurança. Infere que a adoção de programas de compliance em proteção de dados é essencial não apenas para a mitigação de riscos jurídicos e reputacionais, mas também como estratégia de competitividade das empresas.

Procura demonstrar, ainda, através de pesquisa bibliográfica, que o cumprimento da LGPD exige mudanças estruturais e culturais nas organizações, envolvendo desde o mapeamento de dados até a implementação de mecanismos de controle e responsabilização. Além disso, evidencia-se que a responsabilização civil e administrativa dos agentes de tratamento reforça o caráter preventivo da lei. Examina, também, a evolução doutrinária do direito à privacidade, os fundamentos normativos da legislação e a crescente consolidação jurisprudencial do Superior Tribunal de Justiça.

Por fim, conclui que a proteção de dados deve ser compreendida como um eixo transversal do Direito contemporâneo, especialmente diante dos desafios impostos por tecnologias emergentes, como a inteligência artificial, o *big data*. e o *data center*. Propõe, por fim, uma crítica à adoção de modelos meramente formais de compliance, defendendo uma abordagem orientada à responsabilidade e à prevenção de danos.

Palavras-chave: dados pessoais; privacidade; LGPD; *compliance*; governança.

## 1. Introdução.

O mundo passou por grande transformação depois do advento da Segunda Guerra Mundial, pois diante da violação à dignidade humana pelos governos totalitários, verificou-se a importância dos direitos da personalidade para o mundo jurídico, a sua proteção foi efetivada na Assembleia Geral da ONU de 1948,

Assim, com o advento da Declaração Universal dos Direitos Humanos os direitos da personalidade tiveram destaque. É consenso que a proteção à personalidade está ligada à dignidade da pessoa humana, a qual trata-se de atributo do ser humano e não apenas um direito, pois é inerente à própria condição de pessoa, merecendo proteção integral do Estado de Direito.[2]

Importante entender os conceitos de privacidade e intimidade, personalidade jurídica e de dados sensíveis. Relevante, também, o desenvolvimento das questões que envolvem o Direito à Privacidade como direito fundamental e sua correlação com o Princípio Constitucional da Dignidade da Pessoa Humana.

É preciso enfatizar o regime legal e jurisprudencial sobre privacidade e a segurança do tratamento e armazenamento dos dados sensíveis, diante da enormidade de dados tratados pelos usuários, como também, da Inteligência Artificial, das *Big Data* e do *Data Center.*

A economia atual está estruturada a partir da circulação de dados pessoais de forma massiva, que se tornaram ativos estratégicos para organizações públicas e privadas. Nesse cenário, a proteção da privacidade assume papel central na tutela da dignidade da pessoa humana, especialmente diante dos riscos inerentes ao tratamento indevido de informações e o risco de sua circulação pública indiscriminada.

A promulgação da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados representa um marco normativo no ordenamento jurídico brasileiro, estabelecendo diretrizes para o

---

[2] BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento*.** Rio de Janeiro: Forense, 2019. p. 55

tratamento de dados pessoais e impondo deveres de governança e responsabilidade aos agentes de tratamento.

Essa transformação baseia-se em alguns pilares essenciais, como a 1) autodeterminação informativa e dignidade**,** que garante à pessoa o direito de controlar suas próprias informações, portanto, a privacidade não se limita mais apenas ao sigilo, mas envolve o controle sobre suas informações; 2) consolidação constitucional, através da Emenda Constitucional 115/2022, que incluiu a proteção de dados de forma explícita no rol de direitos fundamentais do art. 5º da Constituição Federal; 3) Jurisprudência, diversas decisões do STJ - Superior Tribunal de Justiça, consolidando a proteção de dados, e firmando entendimento de que o vazamento indevido de dados pessoais gera dano moral *in re ipsa,* dispensando a comprovação do dano, aplicando à proteção de dados uma lógica protetiva semelhante à de outros direitos da personalidade.

A aplicação prática da autodeterminação informativa fica prejudicada, quando as decisões sobre dados se concentram nas mães dos agentes econômicos, que os utilizam, e o titular somente tem o condão de consentir, por termos de adesão de difícil entendimento, não havendo paridade de armas, criando-se uma assimetria estrutural de poder[3]. Com essa assimetria criada, fica evidente que a verdadeira proteção de dados exige uma redistribuição real de poder sobre a informação, não só o mero consentimento formal, como também, um avanço na proteção legal.

Portanto, a LGPD representou um avanço significativo na proteção dos direitos fundamentais ao alinhar o Brasil às melhores práticas internacionais e exigir que a conformidade com a proteção de dados seja compreendida como um compromisso substancial com a dignidade da pessoa humana, indo além da mera formalidade.

"A Lei traz uma série de princípios e deveres legais que devem ser respeitados pelos agentes de tratamento, ou seja, pessoas jurídicas ou naturais que tratam dados pessoais."[4] Conforme previsto no art. 50 da LGPD:

> "Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações

---

[3] DONEDA, Danilo. ***Da privacidade à proteção de dados pessoais***. 2ª ed. Revista dos Tribunais: 2020.

[4] TAMER, Maurício Antonio. ***Proteção de Dados: desafios e soluções na adequação à lei***. Rio de Janeiro; Forense, 2020, p. 213.

> específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais"[5].

A adequação à LGPD demanda a implementação de programas estruturados de compliance, capazes de promover uma cultura organizacional orientada à proteção de dados.

## 2. A proteção de dados como direito fundamental.

A proteção de dados pessoais evoluiu de um direito patrimonial para se consolidar como direito fundamental, protegido pela Constituição Federal. Tal entendimento foi reforçado no Brasil, seguindo tradição de alguns países Europeus[6], com a inclusão da proteção de dados no rol do art. 5º da Constituição Federal, por meio da Emenda Constitucional nº 115/2022.

No Brasil, a Constituição Federal em seu art. 5º, X, prevê a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, instituindo ainda a indenização por danos morais e patrimoniais decorrentes dessa violação.

A doutrina defendia que de tal inciso derivou o reconhecimento da proteção de dados como um direito fundamental, em razão de seu direto relacionamento com a inviolabilidade da intimidade[7].

Outro dispositivo apto a albergar o status de direito fundamental para a proteção de dados é o art. 5º, XII, que dispõe ser

> "inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal"[8].

---

[5] BRASIL, Lei 13.709/2018 Lei Geral de Proteção de Dados LGPD.

[6] PFEIFFER, Roberto Augusto Castellanos. **Proteção de Dados Pessoais como um Direito Fundamental: Consequências Amparo ao Diálogo de Fontes entre a LGPD e o CDC.** Revista de Direito do Consumidor | vol. 152/2024 | p. 59- 73

[7] DONEDA, Danilo. ***Da privacidade à proteção de dados pessoais***. 2ª ed. Revista dos Tribunais: 2020.

[8] PFEIFFER, Roberto Augusto Castellanos. **Proteção de Dados Pessoais como um Direito Fundamental: Consequências Amparo ao Diálogo de Fontes entre a LGPD e o CDC.** Revista de Direito do Consumidor | vol. 152/2024 | p. 59- 73

Sobre a referência a dados no dispositivo, inicialmente prevaleceu a interpretação de que seria limitado apenas à "comunicação dos dados" ou aos dados em si mesmos[9]. Após esse primeiro momento, a proteção de dados foi erigida a direito fundamental.

De acordo com a doutrina de Danilo Doneda, esse conceito é a expressão da proteção de dados que decorre diretamente do princípio da dignidade da pessoa humana[10]. A dignidade da pessoa humana é a base de tudo. Significa que a cada pessoa deve ser atribuído direitos, que assegurem a sua dignidade na vida social.

Na atual sociedade da informação, como destaca a autora Laura Schertel Mendes, a compreensão de privacidade evoluiu: ela não se limita mais apenas ao sigilo, mas envolve fundamentalmente o controle ativo sobre o fluxo informacional[11].

Essas considerações nos remetem ao princípio da dignidade humana, que para Francisco do Amaral "a pessoa humana é um valor em si mesmo, um valor intrínseco, absoluto, não um meio de realização de interesses alheios, devendo merecer respeito e consideração social".[12]

Oliveira Ascensão afirma que "a dignidade humana implica que a cada homem sejam atribuídos direitos, por ela justificados e impostos, que assegurem esta dignidade na vida social. Esses direitos devem representar um mínimo, que crie o espaço no qual cada homem poderá desenvolver a sua personalidade. Mas devem representar também um máximo, pela intensidade da tutela que recebem".[13]

"Rosa Maria de Andrade Nery confirma ser o princípio da dignidade da pessoa humana o mais importante regramento do direito. A estudiosa acentua que "É por ele que se faz prevalecer, no contexto das relações humanas, o valor da vida e da liberdade humana".[14]

A Constituição Federal brasileira encerra diversos direitos da personalidade erigidos a direitos fundamentais, como o direito à vida, à saúde, à liberdade, à segurança e à propriedade, e a proteção de dados pessoais.

---

9 PFEIFFER, Roberto Augusto Castellanos. **Proteção de Dados Pessoais como um Direito Fundamental: Consequências Amparo ao Diálogo de Fontes entre a LGPD e o CDC.** Revista de Direito do Consumidor | vol. 152/2024 | p. 59- 73

10 DONEDA, Danilo. ***Da privacidade à proteção de dados pessoais***. 2ª ed. Revista dos Tribunais: 2020

11 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

12 Francisco Amaral apud MIRANDA, Adriana Augusta Telles. **Adoção de Embriões Excedentários à Luz do Direito Brasileiro**. p. 57.

13 ASCENSÃO, José de Oliveira – **Teoria Geral, vol. 1: Introdução. As Pessoas. Os Bens.** p. 59.

14 MIRANDA, Adriana Augusta Telles. **Adoção de Embriões Excedentários à Luz do Direito Brasileiro**. p. 59.

Através da Emenda Constitucional 115 de 2022, foi incluído o inciso LXXIX ao art. 5º, alçando a proteção de dados pessoais entre os direitos e garantias fundamentais. Alterou, ainda, o art. 22, XXX, para incluir entre as matérias privativas de legislação federal a proteção e tratamento de dados pessoais. Passou, também, a ser atribuição exclusiva da União Federal organizar e fiscalizar a proteção, bem como, do tratamento de dados pessoais, nos termos da lei, conforme art. 21, XXVI, da Constituição Federal. *Data Centers*, fez surgir nova legislação aplicada ao setor, incluindo a proteção de dados. A Resolução Anatel nº 780/2025 estabelece diretrizes técnicas, incluindo segurança física e cibernética. A Lei nº 11.196/2005 (alterada pela MP 1318/2025, incluiu o regime especial de incentivo à instalação e expansão de *data centers*. O PL 3018/2024 visa a regulamentar especificamente os *data centers* voltados à inteligência artificial. Surgiu, ainda, Normas Técnicas (ANSI/TIA-942 e NBR ISO/IEC 22237), que são padrões internacionais e nacionais (NBR) amplamente adotados para requisitos de infraestrutura física, elétrica, segurança e monitoramento de dados.

Em relação ao uso de Inteligência Artificial, o PL 2338/2023, que visa instituir o Marco Legal da IA no Brasil, exige relatórios de impacto, transparência no uso de dados e proíbe sistemas de alto risco que violem direitos fundamentais. A transparência prevista, visa permitir que os usuários saibam quando estão interagindo com um sistema de Inteligência Artificial, e possam ter acesso aos seus dados pessoais.

## 3. Estrutura normativa da LGPD - Lei Geral de Proteção de Dados (Lei nº 13.709/2018) - Tratamento de Dados.

A LGPD estabelece um regime jurídico abrangente para o tratamento de dados pessoais, aplicável a pessoas naturais e jurídicas, de direito público e privado. Seus dispositivos estabelecem que os agentes de tratamento de dados pessoais devem observar questões relacionadas à segurança e governança de suas atividades[15]. Para tanto:

---

[15] "A seguir, a Legal Ethics Compliance (LEC) define os principais passos para a efetivação de um Programa de Compliance:
•Análise de riscos: essa etapa consiste na avaliação de todos os problemas de conduta que a empresa pode estar sujeita de acordo com a sua área de atuação. Plano de ação: trata-se de planejar uma estratégia para a implementação de um Programa de Compliance. Nele deve ser descrita cada etapa, como será realizada, além de pontos como a divulgação, a capacitação dos colaboradores e o monitoramento.
•Código de conduta: documento precisa ser claro, objetivo e pertinente à realidade da empresa. Por mais bonito que o texto possa parecer, ele precisa ter um significado alinhado aos valores e às necessidades da organização.
• Canais de comunicação: não basta criar um código, ele tem que ser colocado em prática. Para isso, devem ser criados e divulgados canais de denúncias e análise de situações. Esses canais precisam ser abertos tanto para o público interno (colaboradores) quanto para o externo (clientes e fornecedores). Essencial que todos tomem conhecimento sobre as diretrizes e ter o apoio da alta administração.

> "a empresa alvo de adequação à Lei Geral de Proteção de Dados deve: (i) reforçar as medidas de segurança sobre as suas atividades que envolvem tratamento de dados pessoais; (ii) criar regras de boas práticas e governança para redução dos riscos envolvidos nas atividades relacionadas ao tratamento de dados pessoais, além de ações educativas, o que seria o seu Programa de Privacidade."[16]

Sempre que houver o registro das atividades de tratamento de dados, deve ser apontada a base legal de cada atividade, art. 7 da LGPD. Em seu art. 37 da LGPD, é previsto que o controlador e o operador devem registrar as operações de tratamento que fizerem, ainda mais quando a base legal for o interesse legítimo.

"Dando sequência, o art. 39 da LGPD determina que o operador realizará o tratamento segundo as instruções do controlador, a quem compete verificar a observância das normas acerca de proteção de dados."[17]

As empresas para atingirem seu fim, acabam por tratar dados pessoais de seus clientes, parceiros e colaboradores. Desse modo, para atenderem a conformidade da lei, e a expectativa de segurança de todos os envolvidos na cadeia produtiva, deve-se estabelecer o escopo do programa de privacidade, a fim de reduzir o risco de vazamento ou exposição de dados pessoais, preservando sua marca, reputação e confiabilidade. Os princípios de Compliance devem estar no escopo do programa de privacidade, incluindo os conceitos de p*rivacy by design* e *privacy by default*.

Para atender ao art. 37 da LGPD, é necessário a identificação dos dados pessoais coletados e que serão tratados, e o registro do tratamento de dados pessoais que a empresa realiza. Após, fazer o mapeamento das bases legais a serem aplicadas, como o consentimento do titular e o legítimo interesse do controlador, levando-se em conta a legislação estrangeira,

---

•Capacitação de colaboradores: todos os funcionários devem estar conscientes das responsabilidades de seus atos. Mas acima de tudo, eles devem de fato aderir ao Programa de Compliance. Para isso, podem ser feitos treinamentos periódicos, campanhas de conscientização e de comunicação interna.
• Monitoramento do funcionamento do Programa: monitorar o funcionamento de cada um dos pilares do Programa de Compliance . Não basta colocá-los em pé, é preciso acompanhar a operação e testar cada um dos componentes do programa, constantemente, para ter certeza sobre sua efetividade.
•Avaliação e correção de problemas: as soluções não devem considerar apenas os casos isolados, mas sim o contexto que possibilitou tais ocorrências. Ou seja, um Programa de Compliance não se trata de um simples paliativo. Tem como principal objetivo propor mudanças permanentes na conduta dos membros da empresa (LEC, 2021). MACHADO, Ronny Max et al. ***A proteção de dados pessoais com o advento da lei geral de proteção de dados (LGPD): Boas práticas no tratamento e na proteção de dados pessoais em empresas nacionais.*** : Revista Direito em Debate: 2023, v.32 n.59.

[16] BRUNO, Marcos Gomes da Silva. ***Proteção de Dados: desafios e soluções na adequação à lei***. Rio de Janeiro; Forense, 2020, p. 213.
[17] LIMA, Caio Cesar Carvalho. ***Proteção de Dados: desafios e soluções na adequação à lei***. Rio de Janeiro; Forense, 2020, p. 26.

como também os regulamentos a serem aplicados. No caso do tratamento de dados no Brasil é necessário, portanto, a observância da LGPD e as orientações da Autoridade Nacional de Proteção de Dados.

A partir disso, cria-se o programa de privacidade, para a proteção dos dados pessoais, condicionando o tratamento desses dados a princípios norteadores como finalidade, necessidade e transparência. Permitindo, portanto, o desenvolvimento de atividades econômicas de forma justificada e responsável.

A LGPD, no seu §2º do art. 46, incluiu, conforme entendimento da maior parte da doutrina, os conceitos de p*rivacy by design* e *privacy by default*:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.
> (...)
> §2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução[18].

Nos termos do art. 50, §2º, I, "g" da LGPD, o plano de resposta a incidentes e remediação é parte obrigatória do programa de privacidade, e é fundamental para o sucesso do programa.

> **§ 2º** Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
> **I** - implementar programa de governança em privacidade que, no mínimo:
> (...)
> **g)** conte com planos de resposta a incidentes e remediação;

Ainda, o art. 50, §2º, I, "h" da LGPD, orienta que o programa de privacidade "seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas"[19].

O programa de proteção de dados em conformidade com a LGPD, não deve ser visto como obstáculo ou empecilho à finalidade das empresas, mas como um valor estratégico capaz de fortalecer a confiança, a reputação e a sustentabilidade das relações jurídicas das empresas no mercado.

Importante observar que no tratamento de dados pessoais deverão ser observados a boa-fé, e seus principais pilares, destacando-se os princípios da finalidade, adequação,

---

[18] BRASIL, Lei 13.709/2018 Lei Geral de Proteção de Dados LGPD.
[19] BRASIL, Lei 13.709/2018 Lei Geral de Proteção de Dados LGPD.

necessidade, transparência, não discriminação, segurança e responsabilização, que orientam toda a atividade de tratamento de dados, conforme art. 6º da LGPD.

A LGPD, em seu art. 11, e incisos, confere proteção reforçada aos dados sensíveis, reconhecendo seu potencial discriminatório e os riscos associados ao seu uso indevido.

Perante as condições das novas tecnologias da informação, observamos o conflito entre a liberdade de expressão e de informação presente na rede de computadores e a privacidade e intimidade. "Um aspecto fundamental está, porém, na posição particular atribuída aos dados sensíveis, de que já falamos. Estes abrangem, nos termos do art. 7/1, os dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada, origem racial ou étnica, saúde, vida sexual, incluindo os dados genéticos"[20].

Diogo Leite de Campos enfatiza que "tem-se a consciência de que a omnissapiência dos meios informáticos, sobretudo quando se cruzam as informações, coloca a pessoa numa situação de grande vulnerabilidade"[21]

Não podemos deixar de nos preocupar com a vulnerabilidade do tratamento de dados pessoais, e principalmente em relação à intimidade da vida privada. "A vida privada aparece assim como um dos vários domínios em que os dados são sensíveis. Há assim uma considerável diferença de grau, entre dados pessoais e o círculo mais restrito representado pelos dados referentes à vida privada"[22].

Na medida que a proteção de dados pessoais é um instrumento de contenção às práticas discriminatórias, é por esse motivo que as leis de proteção de dados pessoais, incluindo a brasileira, dedicam um regime jurídico mais protetivo em relação a dados sensíveis com o intuito de frear práticas discriminatórias.[23]

Assim, diferente dos dados pessoais comuns, o tratamento de dados sensíveis não pode ser fundamentado em "legítimo interesse", sendo permitido se o titular consentir de forma específica. Excetuando-se o consentimento, em caso de cumprimento de obrigação legal ou regulatória pelo controlador, tratamento compartilhado de dados necessários à execução de políticas públicas, realização de estudos por órgão de pesquisa; exercício regular de direitos, proteção da vida ou da incolumidade física; em relação a tutela da saúde, somente

---

[20] ASCENSÃO, José de Oliveira – **Teoria Geral, vol. 1: Introdução. As Pessoas. Os Bens.** p. 105

[21] Diogo Leite de Campos apud ASCENSÃO, José de Oliveira – **Teoria Geral, vol. 1: Introdução. As Pessoas. Os Bens.** p. 103

[22] ASCENSÃO, José de Oliveira – **Teoria Geral, vol. 1: Introdução. As Pessoas. Os Bens.** P. 105

[23] BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento*.** Rio de Janeiro: Forense, 2019. p.86.

em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

## 4. Compliance em proteção de dados: da formalidade à cultura organizacional

A implementação da LGPD nas organizações exige muito mais do que a elaboração de documentos formais. Trata-se de um verdadeiro processo de transformação cultural.

O compliance em proteção de dados envolve a adoção de políticas internas, treinamento de colaboradores, mapeamento de fluxos de dados e implementação de medidas técnicas e administrativas de segurança.

Bruno Bioni ressalta que a proteção de dados não pode ser reduzida a um modelo baseado exclusivamente no consentimento, devendo ser compreendida como um sistema de governança que distribui responsabilidades entre os agentes envolvidos.

O modelo baseado exclusivamente no consentimento "tem se mostrado falho (...) seja porque ele reforça a aventada assimetria do mercado informacional, seja porque se trata de uma ferramenta que não capacita, efetivamente, o cidadão para exercer controle sobre as suas informações pessoais"[24].

O art. 49 da LGPD estabelece que os sistemas informáticos e programas utilizados para o tratamento e armazenamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança.

Nesse contexto, destacam-se conceitos como a*ccountability,* o qual remete ao dever de demonstrar conformidade; *privacy by design,* que significa a incorporação da proteção de dados desde a concepção de produtos e serviços e, *privacy by default:* adoção de configurações padrão mais protetivas ao titular. Os conceitos de *Privacy by Design* e *Privacy by Default* funcionam como pilares fundamentais para a implementação de um sistema de governança e compliance efetivo em proteção de dados, indo muito além da mera formalidade burocrática.

Os 7 princípios fundamentais do *Privacy by Design*, desenvolvidos originalmente pela especialista Ann Cavoukian, são:

1. Proativo, não reativo; Preventivo, não corretivo: os sistemas devem ser concebidos de modo a antecipar ameaças;

---

[24] BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento*.** Rio de Janeiro: Forense, 2019. p.170

2. Privacidade como configuração padrão (*Privacy by Default*): O sistema devem ser entregues por padrão, com as configurações em pleno atendimento à legislação;
3. Privacidade incorporada ao *design*: a intenção é garantir que a privacidade efetivamente fará parte de toda a prática empresarial, sendo incorporado integralmente em todos os produtos e serviços.
4. Funcionalidades integrais (Soma positiva, não soma zero): deve-se passar a entender aos ditames de privacidade;
5. Segurança de "fim a fim" (Proteção completa ao ciclo de vida dos dados): as questões de segurança sejam pensadas desde o início e englobam a integralidade do ciclo de vida dos dados, desde a coleta até o descar, estando-se constantemente monitorando esses aspectos, a fim de sanar gaps tão logo apareçam.
6. Visibilidade e transparência: não só devem ser garantidas a todos (titulares de dados, fornecedores, autoridades em geral) como também devem ser criados mecanismos para possibilitar a fiscalização acerca do seu atendimento, sendo passível de auditoria.
7. Respeito pela privacidade do usuário (Foco no usuário): o titular dos dados deve ser, desde o início, considerado como o foco de todo desenvolvimento de produtos e serviços, de tal forma que possa ter papel ativo e relevante no exercício dos seus direitos, bem como controle acerca do tratamento dos seus dados pessoais.[25]

Deve-se evitar o fenômeno de compliance de fachada, adotando programas de adequação à LGPD meramente formais, somente para blindagem reputacional do que como efetivo mecanismo de proteção de dados. Nesse cenário, a aparência de conformidade substitui a efetividade da proteção, com políticas de privacidade padronizadas, termos de consentimento extensos, e um simulacro de estruturas organizacionais, sem uma governança ativa na proteção de dados.

---

[25] LIMA, Caio Cesar Carvalho. ***Proteção de Dados: desafios e soluções na adequação à lei***. Rio de Janeiro; Forense, 2020, p. 60-62.

O art. 50 da LGPD estabelece a possibilidade de controladores e operadores, sozinhos ou coletivamente, criarem boas práticas corporativas, para o tratamento de dados pessoais.[26]

A adoção de boas práticas é um dos itens que são considerados no momento da imposição de sanções administrativas, que podem variar de advertência à multa de 50 milhões de reais, publicização da infração, e diversas outras sanções conforme previsto no art. 52 da LGPD.[27]

É necessário para um compliance efetivo a revisão periódica da forma de coleta de dados; a limitação da finalidade e tempo da retenção dos dados coletados; transparência e treinamento periódico para prevenção de danos.

A disposição do art. 50 da LGPD está em consonância às atuais políticas empresariais de governança e compliance, que visam realizar uma gestão de riscos, por meio de boas práticas, com a criação de controles internos[28].

## 5. Responsabilidade civil e sanções administrativas.

O art. 42 da LGPD dispõe que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a reparar o dano.

A LGPD estabelece um regime de responsabilização dos agentes de tratamento, baseado na obrigação de reparar danos causados em decorrência do tratamento irregular de dados pessoais.

A responsabilidade pode ser solidária entre controlador e operador, especialmente quando houver falha na adoção de medidas de segurança.

Conforme ressalta Gustavo Tepedino, a responsabilização no âmbito da proteção de dados deve ser interpretada à luz da teoria do risco, considerando a natureza da atividade desenvolvida.[29]

---

[26] COTS, Marcio, OLIVEIRA, Ricardo. ***Lei geral de proteção de dados pessoais comentada***. 3ª ed. rev., atual e ampl. - São Paulo: Thomson Reuters Brasil, 2019. p. 201.

[27] COTS, Marcio, OLIVEIRA, Ricardo. ***Lei geral de proteção de dados pessoais comentada***. 3ª ed. rev., atual e ampl. - São Paulo: Thomson Reuters Brasil, 2019. p. 201.

[28] COTS, Marcio, OLIVEIRA, Ricardo. ***Lei geral de proteção de dados pessoais comentada***. 3ª ed. rev., atual e ampl. - São Paulo: Thomson Reuters Brasil, 2019. p. 203.

[29] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. ***Fundamentos do Direito Civil***. Rio de Janeiro: Forense, 2020.

De fato, a responsabilidade civil dos agentes de tratamento de dados, atribuída pelo artigo 42, segue a regra geral do Código Civil, em seu artigo 927.

O Superior Tribunal de Justiça (STJ) tem construído uma jurisprudência que busca aplicar a LGPD de forma equilibrada entre a proteção efetiva do titular das informações e a segurança jurídica das atividades econômicas.

No caso de disponibilização para terceiros de informações pessoais armazenadas em banco de dados, sem a comunicação prévia ao titular e sem seu consentimento, a Terceira Turma do STJ, em voto prevalente da Ministra Nancy Andrighi no REsp nº 2201694 / SP, decidiu por maioria que há violação dos direitos de personalidade, passível de indenização por danos morais.[30]

Ainda, de acordo com a jurisprudência do STJ, o vazamento de dados sensíveis se baseiam no dano moral presumido (*in re ipsa*), entendendo que os dados sensíveis têm características de intimidade do titular dos dados, gerando indenização por danos morais independente da prova do dano.

Diferentemente, em se tratando de vazamento de dados pessoais, o STJ estabeleceu entendimento de que é necessária a demonstração do prejuízo concreto sofrido pelo titular, para que haja condenação por danos morais.

Em relação à responsabilidade pelo risco e ataques de hackers, o STJ consolidou a visão de que a responsabilidade civil na LGPD se orienta por uma lógica de risco da atividade, na forma do art. 927 do CC. Assim, é dever do controlador demonstrar que adotou as medidas adequadas de segurança para tentar afastar a sua responsabilidade de indenizar. Além disso, a Corte já sinalizou que, mesmo quando o vazamento ocorre por um ataque hacker, o agente de tratamento pode permanecer sujeito às obrigações legais, não havendo a exclusão automática de sua responsabilidade sob a justificativa de "fato de terceiro".

Chegamos a um entendimento de que é inequívoco que as organizações que controlam dados assumem os riscos dessa atividade, e responderão por eles caso não implementem uma governança real e responsável.

A Autoridade Nacional de Proteção de Dados (ANPD) possui competência legal para aplicar sanções administrativas aos agentes em caso de tratamento irregular de dados pessoais. As sanções que podem ser aplicadas incluem advertências, multas e até a suspensão das atividades de tratamento.

---

[30] REsp nº 2201694 / SP (2025/0081134-2)

Além do caráter punitivo, a atuação da ANPD na aplicação dessas sanções e na edição de normas tem o objetivo de reforçar a dimensão preventiva da LGPD. Com isso, a autoridade busca incentivar as organizações a adotarem práticas reais de governança e dever de demonstrar conformidade, indo além da mera adequação formal.

A expansão da inteligência artificial, em conjunto com o *big data* e a economia digital, amplia exponencialmente a capacidade de coleta, processamento e análise de dados, o que traz riscos significativos à privacidade. "Coletam-se, cada vez mais, informações sobre um indivíduo, a fim de compor um perfil detalhado para alimentar análises preditivas a seu respeito. Isso equivale a classificá-lo e, até mesmo, segregá-lo."[31][32]

Nesse contexto, a utilização de algoritmos e sistemas automatizados levanta preocupações e riscos diretamente relacionados à transparência, à discriminação e ao controle social. Para conseguir enfrentar esses desafios gerados por essa acelerada transformação tecnológica, é exigida uma atuação regulatória cada vez mais sofisticada por parte das autoridades.

Ao exigir que o funcionamento e os critérios das inteligências artificiais sejam transparentes e explicáveis, garante-se uma verdadeira redistribuição de poder sobre a informação. Aliada à revisão crítica da coleta massiva de dados e à limitação efetiva da finalidade, a transparência e a explicabilidade promovem uma postura ativa de prevenção de danos, impedindo que os riscos inerentes à IA se concretizem e afetem a personalidade jurídica dos titulares de dados.

## 6. Conclusão.

---

[31] BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento.*** Rio de Janeiro: Forense, 2019. p.229.

[32] Ilustrando a questão da discriminação por dados sensíveis coletados, trazemos mais uma vez ensinamento de Bruno Bioni, "Há, primeiro, um protocolo adicional à Convenção de Oviedo para tratar, especificamente, de dados genéticos. Nele, retoma-se a limitação de que o tratamento de dados genéticos para fins preditivos deve-se limitar unicamente à proteção da saúde e para fins de pesquisa, a fim de que os indivíduos não sejam "discriminados e estigmatizados de acordo, respectivamente, com o art. 12 da Convenção e o art. 4 (1) (2) do seu Protocolo Adicional. Uma dessas possíveis estigmatizações e discriminações se daria na área dos contratos securitários. Na medida em que é a ciência atuarial e estatística que - por meio de cálculos que identificam a probabilidade de um acontecimento - decide se o isco é assegurável ou não (cobertura) e, em caso afirmativo, o prêmio a ser pago pelo segurado, testes genéticos teriam um grande impacto nesse arranjo contratual, segregando-se a sociedade entre aqueles com características genéticas mais ou menos propensas a desenvolver certos tipos de doenças. Da recusa em contratar à fixação de prêmios fixados em patamares mais elevados, uma seleção eugênica poderia prosperar." BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento.*** Rio de Janeiro: Forense, 2019. p.231. Podemos, também, ilustrar com possíveis discriminação na contratação de colaboradores que apresentem alguma probabilidade de acontecimento de doença, o que na prática já acontece com mulheres em idade fértil, e idosos, ou até mesmo pessoas acima de 40 anos.

Percebemos que a LGPD representou um avanço significativo dos direitos fundamentais no Brasil, alinhando o país às melhores práticas de governança de dados internacionais.

Todavia, sua efetividade não se esgota na conformidade formal, nem na simples adoção de estruturas de compliance. De fato, depende da internalização de seus princípios pelas instituições públicas e privadas, por meio da implementação de programas de compliance em proteção de dados.

Entendemos que mais do que evitar sanções, a proteção de dados deve ser compreendida como um valor estratégico, capaz de fortalecer a confiança, a reputação e a sustentabilidade das relações jurídicas.

Portanto, é necessário superar a lógica burocrática de somente reproduzir programas de proteção de dados no papel, e reconhecer que a proteção de dados envolve questões de poder, controle e responsabilidade.

Não é somente para evitar sanções administrativas ou jurídicas, o compliance em proteção de dados deve ser compreendido como um compromisso substancial com a dignidade da pessoa humana, exigindo transformação cultural, transparência e responsabilidade ativa.

Se o tratamento de dados pode representar poder e ganhos econômicos, a omissão na proteção dos dados pessoais também deve ser compreendida como forma de violação, é passível de reparação civil.

Restou demonstrado pela evolução jurisprudencial do STJ, que a efetividade da LGPD não depende do cumprimento literal da norma, mas depende muito mais de sua interpretação concreta à luz dos princípios da dignidade humana, da confiança, do consentimento e da responsabilidade.

Nesse contexto, torna-se ainda mais evidente que o compliance em proteção de dados não pode ser meramente formal. Ele deve ser estruturado como instrumento real de prevenção de riscos, capaz de resistir ao escrutínio judicial.

No cenário atual, em que dados representam poder, a governança responsável dessas informações torna-se imperativa para a preservação da dignidade humana e da própria legitimidade do sistema jurídico. Resta claro que quem controla dados, assume riscos e responderá por eles.

**FONTES**

**FONTES DOCUMENTAIS**


BRASIL, *CONSTITUIÇÃO da República Federativa do Brasil*, Diário oficial da União, N.º 192-A (05-10-1988).

BRASIL*, CÓDIGO CIVIL: lei n.º 10.406/02, de 10 de Janeiro. São Paulo: Revista dos Tribunais, 2014.*

BRASIL, *LEI 12.965/2014, 23/04/2014.* Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso 27/03/2026.

BRASIL *Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso 27/03/2026.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 27/03/2026.

REsp nº 2201694 / SP (2025/0081134-2) Disponível em: <https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=329011149&registro_numero=202500811342&peticao_numero=&publicacao_data=20250815&formato=PDF>. Acesso em: 27/03/2026


**BIBLIOGRAFIA**


ALMEIDA, Daniel Freire e – **Um tribunal internacional para a internet**. São Paulo: Almedina, 2015. ISBN 978-858-49-3007-4.

ARTESE, Gustavo (coord.) – **Marco Civil da Internet: Análise Jurídica sob uma Perspectiva Empresarial**. São Paulo: Quartier Latin, 2015. ISBN 85-7674-762-6.

ASCENÇÃO, José de Oliveira – **Estudos sobre direito da internet e da sociedade da informação.** Coimbra: Almedina, 2001.

ASCENSÃO, José de Oliveira – **Teoria Geral, vol. 1: Introdução. As Pessoas. Os Bens.** 3.ª ed. São Paulo: Saraiva, 2010. ISBN 978-85-02-10296-5.

ASCENSÃO, José de Oliveira – **Teoria Geral, vol. 2: Introdução. As Pessoas. Os Bens.** 3.ª ed. São Paulo: Saraiva, 2010. ISBN 978-85-02-10296-5.

ASCENSÃO, José de Oliveira – **Teoria Geral, vol. 3: Introdução. As Pessoas. Os Bens.** 3.ª ed. São Paulo: Saraiva, 2010. ISBN 978-85-02-10296-5.

BIONI, Bruno Ricardo. ***Proteção de dados pessoais: a função e os limites do consentimento*.** Rio de Janeiro: Forense, 2019. ISBN 978-85-309-8168-6.

BITTAR, Carlos Alberto – **Os direitos da personalidade.** 7ª ed. / atualizada por Eduardo Carlos Bianca Bittar. Rio de Janeiro: Forense Universitária. 2004.

BRUNO, Marcos Gomes da Silva. ***Proteção de Dados: desafios e soluções na adequação à lei***. Rio de Janeiro; Forense, 2020, p. 213.

CAMPOS, Diogo Leite de. **Lições de direitos da personalidade**. Boletim da Faculdade de Direito de Coimbra, v. 67, p. 129-223, 1991.

CAMPOS, Diogo Leite de. **Nós Estudos sobre os direitos das pessoas**. Coimbra: Livraria Almedina. 2004.

CANOTILHO, José Joaquim Gomes **–** ***Direito constitucional e teoria da constituição.*** *7.*ª ed. Coimbra: Edições Almedina, 2003. ISBN 978-972-4021-06-5.

COELHO, Fernando da Cruz; CARVALHO, Adriane M. A. ***A Lei Geral de Proteção De Dados (Lgpd) sob a Ótica da Complexidade***. Código 31: revista de informação, comunicação e interfaces , v. 1, p. 7-15, 2023.

COTS, Marcio, OLIVEIRA, Ricardo. ***Lei geral de proteção de dados pessoais comentada***. 3ª ed. rev., atual e ampl. - São Paulo: Thomson Reuters Brasil, 2019.

DESCARTES, René – ***Discurso do Método*** / tradução de Paulo Neves. Porto Alegre: L&PM, 2013.

DONEDA, Danilo. ***Da privacidade à proteção de dados pessoais***. 2ª ed. Revista dos Tribunais: 2020. ISBN 978-85-5321-957-5.

FACHANA, João – **A responsabilidade civil pelos conteúdos ilícitos colocados e difundidos na internet em especial da responsabilidade pelos conteúdos gerados por utilizadores.** Coimbra: Almedina, 2012. ISBN 978-972-40-4851-2.

FRADA, Manuel A. Carneiro da - **Direito Civil, responsabilidade civil: o método do caso.** Coimbra: Almedina, 2010. ISBN 978-972-40-2758-6.

FIORILLO, Celso Antonio Pacheco – **O marco civil da Internet e o Meio Ambiente digital na Sociedade da Informação.** Comentários à Lei nº 12.965/2014. ISBN 978-85-02-62772-7.

GONÇAVES, Diogo Costa – **Pessoa e Direitos de Personalidade: fundamentação ontológica da tutela.** Coimbra: Almedina, 2008.

JHRERING, Rudolf von – **A luta pelo Direito**. Leme/SP: CL Edijur, 2016. ISBN 978-85-7754-070-9.

KELSEN, Hans – **O problema da Justiça** / tradução João Baptista Machado. 5ª ed. São Paulo: Martins Fontes, 2011.

LEAL, Luziane de Figueiredo Simão - **Crimes contra os direitos da personalidade na Internet: violações e reparações de direitos fundamentais nas redes sociais.** Curitiba: Juruá, 2015.

LIMA, Caio Cesar Carvalho. ***Proteção de Dados: desafios e soluções na adequação à lei***. Rio de Janeiro; Forense, 2020.

MACHADO, Ronny Max et al. ***A proteção de dados pessoais com o advento da lei geral de proteção de dados (LGPD): Boas práticas no tratamento e na proteção de dados pessoais em empresas nacionais.*** : Revista Direito em Debate: 2023, v.32 n.59. Disponível em: https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/12451. Acesso: 28/03/206.

MENDES, Laura Schertel. ***Privacidade, proteção de dados e defesa do consumidor***. São Paulo: Saraiva, 2014.

MOREIRA, Isabel – **A solução dos direitos, liberdades e garantias e dos direitos econômicos, sociais e culturais na Constituição Portuguesa.** Coimbra: Almedina, 2007.

OLIVEIRA, Elsa Dias – **A proteção dos consumidores nos contratos celebrados através da interne**t. Coimbra: Almedina, 2002.

PFEIFFER, Roberto Augusto Castellanos. **Proteção de Dados Pessoais como um Direito Fundamental: Consequências Amparo ao Diálogo de Fontes entre a LGPD e o CDC.** Revista de Direito do Consumidor | vol. 152/2024 | p. 59- 73 | Mar- Abr / 2024. Disponível em <https://www.mpgo.mp.br/portal/arquivos/2024/08/29/19_55_26_511_Prote_o_de_dados_pessoais_como_um_direito_fundamental.pdf>. Acesso em: 26/03/2026.

***RIBEIRO,*** R. P. L**.. *Privacidade, Proteção De Dados Pessoais E A Lei Geral De Proteção De Dados: Fundamentos, Princípios E Desafios Na Sociedade Da Informação.*** Revista DCS: 2025, 22(83), e3701. Disponível em: https://doi.org/10.54899/dcs.v22i83.3701. Acesso: 27/03/2026.

ROQUE, Ana – **Manual de Noções Fundamentais de Direito.** 2.ª ed. Almada: Quórum, 2012. ISBN: 972-99434-9-2.

ROQUE, Ana - **Noções essenciais de Direito Empresarial.** 4.ª ed. Quorum, 2014. ISBN 972-994-341-9.

SILVA, José Afonso da – ***Curso de direito constitucional positivo.*** 29.ª ed. São Paulo: Malheiros, 2007. ISBN 978-85-7420-777-3.

SILVA, Camila Rodrigues e - **O Direito Fundamental à Proteção de Dados Pessoais sob a perspectiva jurídica contemporânea brasileira: a vulnerabilidade do titular de dados enquanto pessoa humana**. Revista do CEPEJ. p.p 256-279. Disponível em

<https://revista.cepej.com.br/index.php/rcepej/article/download/125/51/800>. Acesso em: 26/03/2026.

TAMER, Maurício Antonio. ***Proteção de Dados: desafios e soluções na adequação à lei***. Rio de Janeiro; Forense, 2020, p. 213.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. ***Fundamentos do Direito Civil***. Rio de Janeiro: Forense, 2020.

VASCONCELOS, Pedro Pais de – **Teoria Geral do Direito Civil.** Coimbra: Almedina, 2014. ISBN 978-972-40-5011-9.