




**PRINCIPAIS DESAFIOS ASSOCIADOS À LEI PROTEÇÃO DE DADOS**

**MAIN CHALLENGES ASSOCIATED WITH THE DATA PROTECTION LAW**

**PRINCIPALES DESAFÍOS ASOCIADOS A LA LEY DE PROTECCIÓN DE DATOS**

 <https://doi.org/10.56238/levv17n61-051>

**Data de submissão:** 17/05/2026

**Data de publicação:** 17/06/2026

**Ana Beatriz de Assis Honório**

Graduanda em Direito

Instituição: Centro de Ensino Superior de Ilhéus (CESUPI)

E-mail: [assishonorioanabeatriz@gmail.com](mailto:assishonorioanabeatriz@gmail.com)

**Ana Clara Costa de Souza Santos**

Graduanda em Direito

Instituição: Centro de Ensino Superior de Ilhéus (CESUPI)

E-mail: [costadesouzasantosa@gmail.com](mailto:costadesouzasantosa@gmail.com)

**Geovanna Nascimento de Moraes**

Graduanda em Direito

Instituição: Centro de Ensino Superior de Ilhéus (CESUPI)

E-mail: [geovannamoraess18@gmail.com](mailto:geovannamoraess18@gmail.com)

**Leandro Itauano Oliveira Rufino**

Graduando em Direito

Instituição: Centro de Ensino Superior de Ilhéus (CESUPI)

E-mail: [Leandroitauanooliveirarufino@gmail.com](mailto:Leandroitauanooliveirarufino@gmail.com)

**Rosely Teixeira do Carmo**

Graduanda em Direito

Instituição: Centro de Ensino Superior de Ilhéus (CESUPI)

E-mail: [Roselycarmofeliz1@hotmail.com](mailto:Roselycarmofeliz1@hotmail.com)

**Thyara Gonçalves Novais**

Docente

Instituição: Centro de Ensino Superior de Ilhéus (CESUPI)

E-mail: [thyarag@gmail.com](mailto:thyarag@gmail.com)

---

**RESUMO**

A crescente digitalização aumentou a geração e armazenamento de dados sensíveis, elevando riscos de segurança da informação individual e coletiva, pois viver em um mundo cada vez mais conectado, onde os dados pessoais como nome, endereço, CPF, e-mail e até nossas interações online estão por toda parte. Nesse sentido, com essa integração virtual, a segurança da informação virou um desafio extremo. Diante desse cenário, a pesquisa adota uma metodologia qualitativa para explorar e compreender profundamente as implicações da proteção de dados e serão destacados os principais

marcos legais. Para organizar e proteger a privacidade e segurança dos dados pessoais, o ordenamento brasileiro implementou a Lei Geral de Proteção de Dados (LGPD), inspirada no modelo europeu como o Regulamento Geral sobre a Proteção de Dados (GDPR). A LGPD funciona como um manual de regras para empresas e governos, exigindo transparência e responsabilidade no uso das nossas informações, garantindo direitos fundamentais, mais segurança e confiança nas relações digitais. Porém, a realidade mostra escândalos, como o da atriz Carolina Dieckman, em maio de 2012, teve fotos copiadas do computador pessoal e divulgadas na internet, nos provam que uma falha de segurança pode ter consequências gigantescas, em escala, afetando a política, a economia e até o nosso dia a dia.

**Palavras-chave:** Proteção de Dados. Direitos Fundamentais. LGPD.

### ABSTRACT

The article analyzes the main challenges related to personal data protection in the context of accelerated digitalization, focusing on how the Brazilian General Data Protection Law (LGPD), inspired by the European GDPR, seeks to safeguard fundamental rights such as privacy and informational self-determination. It adopts a qualitative approach to discuss the legal and technical foundations of data protection, detailing the LGPD's core principles (purpose, adequacy, necessity, transparency, security) and the legal bases for processing, as well as the historical and global background of data collection and regulation. The authors highlight practical obstacles to effective implementation, including the lack of organizational culture and training, the complexity of data governance, and the need for robust cybersecurity measures and “privacy by design/by default” practices, framed against emblematic global incidents like Cambridge Analytica, Yahoo and SolarWinds that illustrate the potential scale of harm from data breaches. The article also emphasizes the central role of Brazil's National Data Protection Authority (ANPD) in overseeing compliance, applying sanctions and consolidating legal certainty, concluding that continuous improvement of policies, technical standards and international cooperation is essential to build safer and more trustworthy digital environments for data subjects.

**Keywords:** Data Protection. Fundamental Rights. LGPD.

### RESUMEN

La creciente digitalización ha incrementado la generación y el almacenamiento de datos sensibles, aumentando los riesgos para la seguridad de la información individual y colectiva, ya que vivimos en un mundo cada vez más conectado donde los datos personales como nombre, dirección, CPF (número de identificación fiscal brasileño), correo electrónico e incluso nuestras interacciones en línea están presentes en todas partes. En este sentido, con esta integración virtual, la seguridad de la información se ha convertido en un desafío extremo. Ante este escenario, la investigación adopta una metodología cualitativa para explorar y comprender en profundidad las implicaciones de la protección de datos, y se destacarán los principales marcos legales. Para organizar y proteger la privacidad y la seguridad de los datos personales, el sistema legal brasileño implementó la Ley General de Protección de Datos (LGPD), inspirada en el modelo europeo del Reglamento General de Protección de Datos (RGPD). La LGPD funciona como un conjunto de normas para empresas y gobiernos, exigiendo transparencia y responsabilidad en el uso de nuestra información, garantizando derechos fundamentales, mayor seguridad y confianza en las relaciones digitales. Sin embargo, los escándalos de la telerrealidad, como el de la actriz Carolina Dieckman en mayo de 2012, donde se copiaron fotos de su ordenador personal y se filtraron en internet, demuestran que una brecha de seguridad puede tener consecuencias gigantescas a gran escala, afectando a la política, la economía e incluso nuestra vida cotidiana.

**Palabras clave:** Protección de Datos. Derechos Fundamentales. LGPD.



## 1 INTRODUÇÃO

A crescente digitalização de serviços e comunicações, somada à expansão das redes sociais e infraestruturas digitais, intensificou não apenas a geração e o armazenamento de dados sensíveis, mas também os riscos relacionados à segurança da informação.

A Lei Geral de Proteção de Dados Pessoais tem como objetivo proteger a privacidade e os direitos dos cidadãos, impondo regras para empresas, órgãos públicos e qualquer entidade que manipule dados pessoais: como nome, CPF, endereço, e até informações digitais.

Ela estabelece princípios, como o consentimento do titular, a finalidade específica para o uso dos dados e o direito de acesso, correção e exclusão dessas informações. Instituída pela Lei nº 13.709/2018, é a legislação que define como os dados pessoais devem ser tratados no Brasil. Seu propósito é assegurar que o uso de informações, inspirada no regulamento geral de proteção de dados europeu GDPR, a LGPD lei geral de proteção de dados pessoais surgiu para fortalecer a proteção da privacidade e garantir maior controle dos cidadãos sobre suas próprias informações, promovendo mais segurança e confiança nas relações digitais e responsabiliza quem descumpre as regras.

Nos últimos anos, casos emblemáticos como nas esferas política, econômica e social. Esses acontecimentos ressaltam a necessidade de aprimorar políticas de proteção de dados, fortalecer práticas de segurança cibernética e desenvolver mecanismos internacionais para mitigar impactos causados por vazamentos e ataques. Este artigo analisa os principais desafios e implicações associados à proteção de dados em escala global, com foco nas lições aprendidas a partir dessas violações, propondo diretrizes para a construção de processos mais complexos e seguros.

## 2 REFERENCIAL TEÓRICO

### 2.1 O DIREITO FUNDAMENTAL À PRIVACIDADE E A PROTEÇÃO DE DADOS NA ERA DIGITAL

Com o avanço tecnológico, as informações referentes os dados pessoais estão cada vez mais acessíveis e, com base na dinâmica da vida cotidiana atual, é certo que a maioria da população que possui acesso à internet, está exposta quanto aos seus dados, que de alguma forma foram disponibilizados neste meio.

Moraes e Prado (2018) abriu a discussão sobre o uso de dados individuais e opacidade sobre o faturamento dos gastos públicos em relação a tecnologia, segurança e no direito à privacidade e acesso aos dados, o que impacta linearmente ao tema desse trabalho. Pois, a exacerbada coleta e uso de dados pessoais pelo setor público, com o auxílio de tecnologias avançadas, nos alerta e causa preocupações e estranheza sobre como essas informações são tratadas e protegidas. A falta de clareza e detalhamento no faturamento de gastos com tecnologias de segurança pode também dificultar o controle social e a responsabilização dos gestores, criando um ambiente propício para irregularidades.

Carvalho et al (2019) em seu trabalho buscou explicar sobre as tecnológicas associadas com a transparência em uma lei dedicada à privacidade e como será o comportamento em relação à vigência da Lei. O ponto de partida é o reconhecimento da proteção de dados pessoais como um direito fundamental, uma garantia constitucional que evoluiu com o avanço da tecnologia da informação. É importante salientar que, os direitos à privacidade e proteção de dados pessoais estão elencados no art. 5º da Constituição Federal e que os direitos fundamentais são garantias com o objetivo de promover a dignidade humana e de proteger os cidadãos. O direito à privacidade e à proteção de dados pessoais é essencial à vida digna das pessoas, principalmente nesse contexto de total inserção na vida digital.

Costa (2018) abordou sobre a privacidade e manipulação de dados pessoais na internet bem como as implicações no âmbito social, econômico e político da manipulação das informações com desenvolvimento de novas tecnologias. Nesse contexto, cada manipulação de dados pode ter consequências sérias para a forma como vivemos em sociedade e como escolhemos cada ponto ou questão. No que tange a Privacidade *versus* Proteção de Dados, a literatura jurídica e de tecnologia distingue, embora interligue, os conceitos de privacidade (um direito mais amplo, ligado à esfera íntima do indivíduo) e a proteção de dados (um conjunto de regras que garante ao titular o controle sobre suas informações específicas).

No contexto Global e a Inspiração na GDPR, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) no Brasil foi fortemente inspirada pelo *regulamento de dados geral* (GDPR) da União Europeia.

Essa convergência regulatória global busca estabelecer padrões mínimos de segurança e direitos do titular, o que reforça a base teórica de que a proteção de dados transcende fronteiras nacionais. Embora esteja em voga no Brasil as repercussões causadas pelo advento da Lei Geral de Proteção de Dados, a temática tratamento de dados já vem sendo discutida na esfera legal, seja no Brasil ou no mundo. Levando em consideração que dados pessoais são informações de pessoas identificadas ou identificáveis, independentemente do modo de sua coleta e armazenamento, pois é possível observar que a coleta de dados está presente na sociedade humana através das realizações de censo, presentes em Roma desde a época em que era um reinado, época anterior à sua república e seu império, ou, ainda, desde 2238 a.c. na China.

## 2.2 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) COMO MARCO REGULATÓRIO

Com a incorporação da LGPD fica estabelecido as diretrizes para como os dados pessoais devem ser tratados no Brasil, com o objetivo de proteger a liberdade e a privacidade dos cidadãos, incluindo consentimento, finalidade, transparência e segurança, promovendo assim mais segurança e confiança nas relações digitais.

Agostine (2018) amplia essa perspectiva ao declarar que tinha como finalidade identificar a relevância de uma legislação específica para conduzir a forma de tratamento de dados pessoais por pessoas jurídicas de direito público e privado dentro da internet.

Os Princípios da LGPD são basilares e são abordados em seu referencial e servem como sustentação para todas as ações de tratamento de dados:

- **Finalidade, Adequação e Necessidade:** A coleta de dados deve ter um propósito legítimo, específico e transparente, limitado ao estritamente necessário para atingir a finalidade informada.
- **Segurança e Prevenção:** A obrigação de adotar medidas técnicas e organizacionais aptas a proteger os dados de acessos não autorizados e incidentes de segurança.
- **Transparência e Livre Acesso:** Garantir que o titular tenha acesso facilitado às suas informações e saiba como elas estão sendo usadas.
- **Bases Legais para o Tratamento:** A discussão teórica deve incluir as bases legais (como o consentimento, cumprimento de obrigação legal, legítimo interesse) que autorizam o tratamento de dados, ressaltando a importância de identificar a base correta em cada caso concreto.

### 2.3 PRINCIPAIS DESAFIOS NA IMPLEMENTAÇÃO E APRIMORAMENTO DE POLÍTICAS

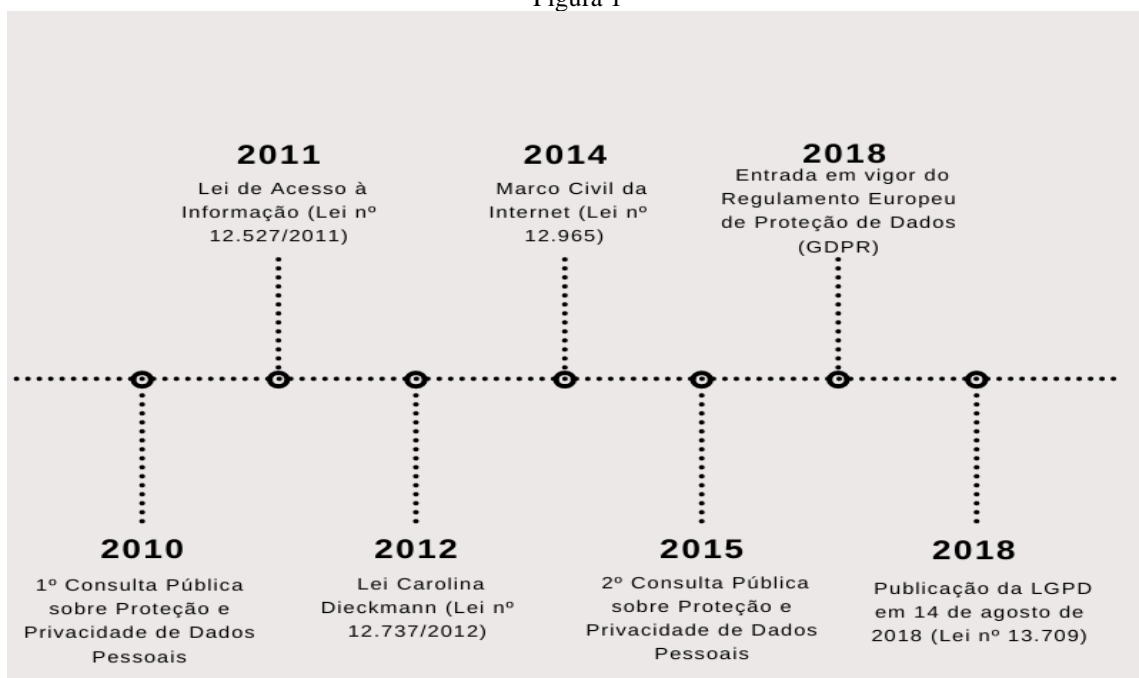
- A literatura acadêmica e técnica aponta diversos desafios na aplicação prática da LGPD, que vão além da mera conformidade legal e exigem o aprimoramento contínuo das políticas de segurança, tais como:
- **Cultura Organizacional e Capacitação:** Um dos maiores desafios é a falta de uma cultura de proteção de dados e ciber segurança. É fundamental investir em treinamento de funcionários e conscientização para mitigar riscos de erros humanos e falhas processuais.
- **Mapeamento e Governança de Dados:** Para cumprir a lei, as organizações precisam, primeiramente, saber quais dados possuem, onde estão armazenados e como são tratados. A **governança de dados** é, portanto, essencial para a conformidade, alinhando a estratégia de negócios e tecnologia.
- **Medidas Técnicas e de Segurança da Informação:** A digitalização crescente e a sofisticação dos ataques cibernéticos exigem a implementação de medidas robustas, como criptografia, anonimização e controle de acesso. Normas internacionais como a ISO/IEC 29100 podem servir como *frameworks* para a tradução de requisitos legais em práticas técnicas.
- **Privacy by Design e by Default:** A teoria da "privacidade desde a concepção" sugere que a proteção de dados deve ser integrada desde o início do desenvolvimento de novos produtos, serviços e sistemas, e não como um complemento posterior.

## 2.4 RESPONSABILIZAÇÃO E A ATUAÇÃO DA AUTORIDADE NACIONAL (ANPD)

O referencial deve abordar as consequências do descumprimento das regras, que incluem sanções administrativas e a obrigação de reparar danos patrimoniais ou morais aos titulares dos dados. Nesse contexto, a **Autoridade Nacional de Proteção de Dados (ANPD)** surge como o pilar que sustenta e concretiza os direitos e deveres estabelecidos pela LGPD.

- A criação da **Autoridade Nacional de Proteção de Dados (ANPD)** é um marco importante no cenário brasileiro, com a função de fiscalizar, regular e aplicar as penalidades previstas na lei, garantindo maior segurança jurídica ao ecossistema digital, sendo fundamental para que a lei não se resuma a um conjunto de normas abstratas.

Figura 1



Fonte: Autores.



## REFERÊNCIAS

AGOSTINELLI, Joice. **A importância da lei geral de proteção de dados pessoais no ambiente online**. Etic-encontro de iniciação científica-ISSN 21-76-8498, v. 14, n. 14, 2018.

COSTA, M.M.da. **A era da vigilância no ciberespaço e os impactos da nova lei geral de proteção de dados pessoais no Brasil: reflexos no direito à privacidade**. 2018. 93 f. TCC (Graduação) -Curso de Direito, Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2018.

CARVALHO, Luiz et al. **Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais**.In: **Anais do VII Workshop de Transparência em Sistemas**. SBC, 2019. p. 21-30.

MORAES, I. H. S. de; PRADO, L. A. **Saúde Coletiva e uma escolha de Sofia: defender a privacidade no ciberespaço**.*Ciência & Saúde Coletiva*, v. 23, p. 3267-3276, 2018.