PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

PRO-REITORIA DE GRADUAÇÃO

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

ARTIGO CIENTÍFICO

A LEI GERAL DE PROTEÇÃO DE DADOS NO COMÉRCIO ELETRÔNICO:
IMPACTOS E DESAFIOS PARA A PROTEÇÃO AO CONSUMIDOR NO BRASIL

ORIENTANDO: GABRIEL BATISTA ARAÚJO

ORIENTADOR(A): CAROLINE REGINA DOS SANTOS

GOIÂNIA - GO

2024

GABRIEL BATISTA ARAÚJO

A LEI GERAL DE PROTEÇÃO DE DADOS NO COMÉRCIO ELETRÔNICO:
IMPACTOS E DESAFIOS PARA A PROTEÇÃO AO CONSUMIDOR NO BRASIL

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof.ª Orientador(a): Caroline Regina Dos Santos

GOIÂNIA

2024

GABRIEL BATISTA ARAÚJO

A LEI GERAL DE PROTEÇÃO DE DADOS NO COMÉRCIO ELETRÔNICO:
IMPACTOS E DESAFIOS PARA A PROTEÇÃO AO CONSUMIDOR NO BRASIL

Data da Defesa: 13 de maio de 2024

BANCA EXAMINADORA

Orientador(a): Prof. (a): Caroline Regina Dos Santos Nota

Examinador(a) Convidado(a): Prof.(a): Djalma Tavares de Gouveia Neto Nota

DEDICATÓRIA

Dedico este trabalho a Ana, meu amor, companheira de todos os momentos, cujo carinho e apoio foram indispensáveis em cada etapa desta jornada.

A Orismar e José, meus queridos pais, agradeço por cada ensinamento, pela paciência, e pelo amor incondicional que me guiou e fortaleceu em todos os desafios.

A Pedro, irmão e amigo, cuja parceria e cumplicidade sempre me motivaram a seguir adiante, e a Amanda, minha querida irmã, que com sua doçura e alegria ilumina nossos dias.

A vocês, pilares da minha vida, minha profunda gratidão e amor.

SUMÁRIO

RESUMO

O presente artigo tem como objetivo explorar a interseção entre a LGPD e o comércio eletrônico, com ênfase particular nos desafios e oportunidades que essa legislação apresenta para a proteção do consumidor no Brasil. A pesquisa aborda a contextualização da LGPD, seus princípios fundamentais e sua aplicação específica no comércio eletrônico. Examina-se como a lei reforça os direitos do consumidor, as responsabilidades impostas às empresas e os desafios enfrentados na implementação da LGPD. Além disso, são discutidas estratégias para a adequação e conformidade com a legislação. O papel das autoridades na regulação do mercado e na fiscalização da aplicação da lei é também analisado, destacando a necessidade de colaboração entre o setor público e privado. O artigo conclui que a LGPD tem um impacto profundo na proteção ao consumidor no comércio eletrônico, exigindo uma abordagem multidisciplinar para garantir a conformidade e promover um ambiente de e-commerce seguro e confiável.

Palavras-chave: Lei Geral de Proteção de Dados; Comércio Eletrônico; Direitos do Consumidor; Estratégias de Conformidade; Regulação do Mercado.

INTRODUÇÃO

A transformação digital tem revolucionado o cenário do comércio global, especialmente no âmbito do comércio eletrônico, onde as relações de consumo passaram por mudanças significativas. Esse progresso trouxe inúmeros benefícios, como maior conveniência e acesso ampliado a produtos e serviços. Contudo, também levantou preocupações críticas acerca da segurança e privacidade dos dados pessoais dos consumidores.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) emerge como uma ferramenta regulatória essencial, destinada a proteger os direitos individuais enquanto promove a inovação tecnológica. A LGPD foi criada para enfrentar os desafios relacionados à coleta, armazenamento e uso de dados pessoais, especialmente no comércio eletrônico, onde essas práticas são intensamente aplicadas.

O presente estudo se propõe a investigar a aplicação da LGPD no comércio eletrônico, destacando os principais desafios e oportunidades que a lei apresenta tanto para empresas quanto para consumidores. A análise começa com uma revisão do contexto legal anterior à LGPD, identificando a evolução da preocupação com a privacidade de dados em níveis nacional e internacional. Posteriormente, explora-se os princípios fundamentais da LGPD e sua aplicabilidade no e-commerce, avaliando as implicações práticas para todas as partes envolvidas.

Adicionalmente, este estudo aborda as estratégias necessárias para que as empresas se adaptem às exigências da LGPD, enfatizando a importância de políticas de governança de dados, sistemas de segurança robustos e práticas de transparência e consentimento. A pesquisa também examina o papel das autoridades reguladoras na fiscalização do cumprimento da lei e a colaboração entre o setor público e privado para criar um ambiente de comércio eletrônico seguro e confiável.

Ao longo deste trabalho, pretende-se não só compreender os impactos da LGPD no comércio eletrônico, mas também oferecer uma contribuição significativa ao debate sobre as melhores práticas e estratégias para a proteção dos direitos dos consumidores na era digital.

1 CONTEXTUALIZAÇÃO DA LGPD NO COMÉRCIO ELETRÔNICO

O surgimento da LGPD no cenário nacional reflete uma tendência global de fortalecimento da proteção de dados pessoais e da privacidade dos usuários na era digital. A necessidade de uma legislação específica para regular o tratamento de dados no Brasil tornou-se evidente diante do avanço tecnológico, do aumento exponencial do volume de dados gerados e do crescimento do cibercrime. A LGPD busca estabelecer um equilíbrio entre o desenvolvimento econômico e tecnológico e a proteção dos direitos dos titulares de dados.

No contexto do comércio eletrônico, a LGPD tem um impacto significativo, pois esse setor se baseia fortemente na coleta e análise de dados dos consumidores para personalizar a experiência de compra, direcionar campanhas de marketing e otimizar as operações de vendas. As empresas que operam no e-commerce devem se adaptar às exigências da Lei, implementando políticas de privacidade transparentes, obtendo o consentimento explícito dos usuários para o tratamento de seus dados e adotando medidas de segurança adequadas para proteger as informações coletadas.

A adequação à LGPD no comércio eletrônico não é apenas uma questão de conformidade legal, mas também uma estratégia competitiva. Empresas que demonstram compromisso com a proteção de dados tendem a conquistar a confiança dos consumidores, que estão cada vez mais conscientes de seus direitos e preocupados com a privacidade de suas informações.

1.1 HISTÓRICO DA LGPD

A Lei Geral de Proteção de Dados, Lei nº 13.709/2018, surgiu como uma resposta à crescente preocupação com a privacidade e a segurança de dados no Brasil e no mundo. O contexto histórico para a regulamentação de dados ganhou destaque em 2016, impulsionado pela General Data Protection Regulation (GDPR) da União Europeia, em meio aos escândalos de privacidade envolvendo o Facebook e a Cambridge Analytica.

> GDPR, General Data Protection Regulation (Regulamento Geral de Proteção de Dados), trata-se do conjunto de regulações a respeito de proteção de dados na União Europeia. A GDPR entrou em vigor em 2016 e

> sua equivalente no Brasil é a Lei Geral de Proteção de Dados (LGPD), que entra em vigor no país em agosto de 2020. (GALVÃO & SILVA ADVOCACIA, 2020).

Esses incidentes de repercussão mundial trouxeram o tema da proteção de dados para o centro das discussões políticas nacionais, evidenciando a ausência de uma legislação específica para garantir a segurança dos dados pessoais no país (GODOY, 2018).

Antes da LGPD, o Brasil já possuía legislações que asseguravam o direito à privacidade, como a Lei de Acesso à Informação (Lei nº 12.527/2011), a Lei Carolina Dieckmann (Lei nº 12.737/2012) e o Marco Civil da Internet (Lei nº 12.965/2014). No entanto, essas leis não eram específicas para a proteção de dados pessoais. A LGPD veio a alterar o Marco Civil da Internet, estabelecendo um marco regulatório para as transações envolvendo dados pessoais. Sancionada em agosto de 2018, a lei teve sua vigência inicialmente prevista para fevereiro de 2020, mas após a promulgação de uma medida provisória pelo Presidente Michel Temer, o prazo de vigência foi estendido para agosto de 2020, com as multas e sanções aplicáveis a partir de agosto de 2021. A LGPD entrou efetivamente em vigor em setembro de 2020.

A LGPD é inspirada na GDPR europeia e foi criada para preencher as lacunas existentes e trazer melhorias no tratamento de dados pessoais dentro do ordenamento jurídico brasileiro. A lei estabelece diretrizes para a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, visando proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural.

Os fundamentos da LGPD, estabelecidos em seu artigo 2º[1], incluem o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, a inviolabilidade da intimidade, o desenvolvimento econômico e tecnológico, a livre iniciativa, a defesa do consumidor e os direitos humanos. Esses fundamentos estão

[1] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

alinhados à Constituição Federal de 1988, reforçando o compromisso da lei com a proteção e garantia da privacidade, liberdade, segurança e justiça no tratamento de dados pessoais.

1.2 PRINCÍPIOS FUNDAMENTAIS E APLICAÇÃO NO E-COMMERCE

A Lei Geral de Proteção de Dados, estabelece um arcabouço de princípios fundamentais que norteiam o tratamento de dados pessoais, visando assegurar a proteção dos direitos dos titulares e a transparência nas operações de tratamento. Esses princípios, elencados no artigo 6º[2] da LGPD, são pilares essenciais para a construção de um ambiente digital seguro e confiável, especialmente no contexto do comércio eletrônico, onde a coleta e o tratamento de dados são atividades intrínsecas.

> Além da boa-fé, a LGPD estabelece a observância de 10 (dez) princípios para o tratamento de dados pessoais, dentre os quais importa destacar: finalidade, adequação, necessidade, livre acesso, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. (Controladoria Geral do Estado do Paraná, 2024).

O princípio da finalidade exige que o tratamento de dados tenha propósitos legítimos, específicos, explícitos e informados ao titular, vedando o tratamento posterior de forma incompatível com essas finalidades. Esse princípio está intrinsecamente ligado à transparência e ao respeito à autonomia do titular,

[2] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

garantindo que os dados pessoais sejam utilizados apenas para os fins para os quais foram coletados.

A adequação e a necessidade são princípios complementares que asseguram a compatibilidade do tratamento com as finalidades informadas ao titular e limitam o tratamento ao mínimo necessário para a realização dessas finalidades. Esses princípios impõem restrições ao uso indiscriminado de dados, evitando a coleta e o tratamento excessivos que não estejam alinhados com os objetivos declarados.

O livre acesso e a qualidade dos dados garantem aos titulares o direito de consultar seus dados pessoais de forma facilitada e gratuita, bem como asseguram a exatidão, clareza, relevância e atualização dos dados. Esses princípios são fundamentais para o exercício dos direitos dos titulares e para a manutenção da confiança nas relações digitais.

A transparência é um princípio-chave que permeia toda a LGPD, exigindo que as informações sobre o tratamento de dados sejam claras, precisas e facilmente acessíveis. No comércio eletrônico, a transparência fortalece a relação entre empresas e consumidores, promovendo um ambiente de confiança mútua.

Os princípios de segurança, prevenção e não discriminação estabelecem diretrizes para a proteção dos dados pessoais contra acessos não autorizados, situações acidentais ou ilícitas e práticas discriminatórias. A adoção de medidas técnicas e administrativas adequadas para salvaguardar os dados é essencial para mitigar riscos e prevenir danos aos titulares.

Por fim, o princípio da responsabilização e prestação de contas impõe aos agentes de tratamento a obrigação de demonstrar a observância das normas de proteção de dados e a eficácia das medidas adotadas. Esse princípio reforça a importância da governança de dados e da cultura de proteção de dados nas organizações, especialmente no setor de comércio eletrônico, onde a gestão responsável dos dados pessoais é um diferencial competitivo.

Em suma, os princípios fundamentais da LGPD estabelecem as bases para um tratamento de dados pessoais ético, transparente e seguro, contribuindo para a consolidação de um ambiente de comércio eletrônico que respeite a privacidade e os direitos dos consumidores.

2 IMPACTOS DA LGPD NA PROTEÇÃO AO CONSUMIDOR

A Lei Geral de Proteção de Dados impactou profundamente a maneira como as empresas coletam, armazenam, processam e compartilham as informações dos consumidores.

A lei exige que as empresas obtenham o consentimento explícito dos indivíduos para o tratamento de seus dados pessoais. Isso significa que os consumidores devem ser claramente informados sobre as finalidades para as quais suas informações serão utilizadas e devem concordar explicitamente com esses usos.

Além do consentimento informado, a LGPD confere aos consumidores direitos ampliados, como o direito de acessar, corrigir, excluir ou transferir seus dados pessoais. Esses direitos permitem que os consumidores tenham uma participação mais ativa no gerenciamento de suas informações, garantindo que possam revisar e modificar suas informações conforme necessário, ou até mesmo retirá-las completamente das bases de dados das empresas.

> [...] os agentes de tratamento enfrentam diversos desafios quanto a devida eliminação dos dados pessoais, pois deverão realizar análise quanto ao alcance da finalidade, criar mecanismos para que o seu titular revogue o consentimento de maneira facilitada, além de contar com tecnologia que permita que o apagamento de certos dados pessoais não prejudique o banco de dados remanescente. (TEIXEIRA; ARMELIN, 2019, p. 76 e 77).

As organizações são obrigadas a adotar medidas de segurança adequadas para proteger os dados contra acessos não autorizados e violações. Isso inclui a implementação de sistemas de segurança robustos e a adoção de práticas de governança de dados rigorosas. As empresas que não cumprirem as disposições da LGPD[3], podem enfrentar sanções severas, incluindo multas que podem chegar a até 2% do faturamento, limitadas a R$ 50 milhões por infração.

> A LGPD (Lei Geral de Proteção de Dados) entrou em vigor em primeiro de agosto de 2021 para os e-commerces. São artigos que regem multas e outras sanções que podem ser aplicadas aos Agente de Tratamento de Dados que infringem essas novas normas. (PERINA, 2021).

[3] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

A implementação eficaz da LGPD pode resultar em um aumento significativo na confiança dos consumidores nas relações comerciais, especialmente no ambiente digital. A proteção aprimorada de dados pessoais contribui para um ambiente de consumo mais seguro e confiável, o que é essencial para o desenvolvimento contínuo do comércio eletrônico e da economia digital no Brasil. Consumidores confiantes tendem a se engajar mais no mercado, favorecendo o crescimento sustentável das atividades comerciais online.

2.1. DIREITOS DO CONSUMIDOR REFORÇADOS PELA LGPD

A Lei Geral de Proteção de Dados trouxe significativos avanços para a proteção dos direitos dos consumidores no Brasil, complementando e ampliando os direitos já previstos no Código de Defesa do Consumidor (CDC)[4]. Esta legislação estabelece um novo paradigma nas relações de consumo, promovendo maior transparência e segurança no tratamento de dados pessoais.

A LGPD garante aos consumidores o direito de acesso às informações sobre o tratamento de seus dados pessoais. As empresas devem fornecer, de forma clara e acessível, detalhes sobre a finalidade, duração e forma de tratamento dos dados, além de informações sobre eventuais compartilhamentos (Art. 9º, LGPD).

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; eVII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Esse direito de acesso reforça a transparência nas relações de consumo, permitindo que os consumidores tenham conhecimento pleno sobre o uso de seus dados.

---

[4] Brasil. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor (CDC).** Diário Oficial da União, Brasília, DF, 12 set. 1990.

De maneira comparável, o Código de Defesa do Consumidor estabelece, em seu Art. 43, § 2º[5], que o consumidor deve ter acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como às suas respectivas fontes. O CDC determina que essas informações sejam disponibilizadas de forma clara e adequada, garantindo que o consumidor possa conhecer, corrigir e atualizar seus dados pessoais.

O CDC já previa o direito dos consumidores de corrigir dados inexatos (Art. 43, § 3º, CDC).

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

A LGPD amplia esse direito, permitindo a correção de dados incompletos, inexatos ou desatualizados (Art. 18, IV, LGPD).

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

Isso assegura que os consumidores possam manter suas informações pessoais precisas e atualizadas, evitando prejuízos decorrentes de dados incorretos. Embora não mencionado explicitamente na LGPD, o direito ao esquecimento é uma extensão do direito de exclusão de dados (Art. 18, VI, LGPD), os consumidores podem solicitar a eliminação de dados pessoais que não sejam mais necessários para a finalidade original ou que tenham sido tratados com base no consentimento.

O direito de portabilidade de dados (Art. 18, V, LGPD), permite que os consumidores transfiram seus dados pessoais de um fornecedor de serviços para outro. Esse direito facilita a mudança de fornecedores, promovendo a livre concorrência e a escolha do consumidor.

---

[5] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

Esse conceito pode ser comparado ao Art. 6º, V[6], do Código de Defesa do Consumidor (CDC), que garante ao consumidor a "modificação das cláusulas contratuais que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas." Embora não trate especificamente da portabilidade de dados, o CDC promove a flexibilização e a revisão de condições contratuais para proteger os interesses do consumidor, similarmente à LGPD, que facilita a transição entre fornecedores e fortalece a autonomia do consumidor.

A LGPD estabelece a responsabilidade dos agentes de tratamento de dados em caso de violação das normas de proteção de dados (Art. 42, LGPD), determinando que o controlador ou operador que cause dano patrimonial, moral, individual ou coletivo deve repará-lo. Isso inclui a responsabilidade solidária dos controladores diretamente envolvidos e a possibilidade de inversão do ônus da prova a favor do titular dos dados.

> Art. 42. 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 repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

---

[6] Art. 6º São direitos básicos do consumidor:
V - a modificação das cláusulas contratuais que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas;

Esse princípio pode ser comparado ao Art. 14[7] do Código de Defesa do Consumidor (CDC), que trata da responsabilidade pelo fato do produto e do serviço, determinando que o fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços.

Ambos os artigos reforçam a proteção dos consumidores, sejam eles de dados pessoais ou de consumo em geral.

A interseção entre o CDC e a LGPD reforça os direitos dos consumidores, especialmente no contexto digital. A LGPD amplia a transparência, o controle e a segurança sobre os dados pessoais, enquanto o CDC continua a ser um pilar fundamental na defesa dos direitos do consumidor. Juntas, essas legislações promovem um ambiente de consumo mais justo, seguro e transparente.

2.2. RESPONSABILIDADES E DESAFIOS DAS EMPRESAS

A entrada em vigor da Lei Geral de Proteção de Dados estabeleceu desafios significativos para as empresas no Brasil, destacando a importância de uma abordagem estratégica e consciente em relação à proteção de dados pessoais, demandando conformidade legal, e incentivando uma mudança cultural profunda dentro das organizações.

O principal desafio para as empresas é a necessidade de fomentar uma cultura de privacidade que permeie todos os níveis organizacionais. É crucial que a alta direção esteja engajada, promovendo e integrando práticas de privacidade em todas as operações da empresa. Conforme o Art. 50[8] da LGPD, é essencial formular políticas de boas práticas e governança, ajustadas à natureza e escala das operações, enfatizando a transparência e a proteção dos dados.

---

[7] Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

[8] Art. 50. 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 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.

Outro desafio significativo é a gestão de terceiros que processam dados em nome da empresa. É essencial estabelecer acordos rigorosos e procedimentos de auditoria para garantir que todos os parceiros e fornecedores cumpram as normas de proteção de dados. Além disso, investir em sistemas de segurança robustos e em auditorias regulares é fundamental para prevenir vazamentos e outras violações de segurança.

A conformidade com a LGPD pode implicar custos consideráveis, especialmente para pequenas e médias empresas. Isso inclui desde a contratação de profissionais qualificados até a implementação de tecnologias avançadas de proteção de dados. Além disso, a capacitação contínua dos colaboradores é vital para assegurar que todos entendam suas responsabilidades sob a nova legislação e possam agir de maneira adequada em relação à proteção de dados.

Para minimizar riscos e adaptar-se às exigências, as empresas podem adotar tecnologias que promovam a anonimização dos dados, Art. 5º, XI, LGPD[9], reduzindo a necessidade de obtenção de consentimento em situações específicas.

A implementação eficaz de sistemas de gestão de consentimento também é crucial para documentar de maneira transparente e acessível as permissões dos usuários.

A capacitação contínua dos colaboradores é essencial para assegurar que todos estejam cientes de suas responsabilidades e saibam como agir de acordo com as diretrizes de proteção de dados. Além disso, a nomeação de encarregado pelo tratamento de dados pessoais, art.º 41 LGPD[10], pode facilitar a coordenação das iniciativas de adequação e servir como ponto de contato com as autoridades reguladoras.

---

[9] XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

[10] Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
§ 2º As atividades do encarregado consistem em:
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Enquanto a LGPD apresenta desafios substanciais, também oferece às empresas a oportunidade de fortalecer a confiança dos consumidores e de se destacarem no mercado como entidades responsáveis e transparentes. A adoção de uma abordagem estratégica e o investimento contínuo em boas práticas de governança de dados são essenciais para garantir a conformidade e promover um ambiente de negócios sustentável e seguro.

2.3 ESTRATÉGIAS PARA ADEQUAÇÃO E CONFORMIDADE

A adequação à LGPD é um processo que exige um comprometimento organizacional com a segurança e a privacidade dos dados pessoais. As organizações devem desenvolver um plano de ação robusto que começa com a análise e o mapeamento detalhado dos dados pessoais que tratam. Este plano inclui a identificação de quais dados são coletados, porque são necessários, e como são usados e armazenados, assegurando conformidade com as normas estabelecidas pelos artigos 5º e 37º[11] da LGPD.

Central para a estratégia de conformidade é a implementação de Sistemas de Gerenciamento de Dados Pessoais (PDM), que ajudam na organização e segurança dos dados. Esses sistemas não só centralizam a informação, facilitando seu controle e acesso, mas também categorizam os dados para separar informações sensíveis das demais.

> Imagine as políticas de segurança da informação como um escudo que protege os dados valiosos de uma organização. Estas políticas estabelecem diretrizes claras e procedimentos robustos para garantir a integridade e confidencialidade dos dados. Desde a criptografia até as práticas de gestão de senhas, cada detalhe é cuidadosamente planejado para criar um ambiente seguro. (LOCUS IURIS, 2024).

A segurança desses dados é reforçada através da criptografia, que transforma informações sensíveis em formatos cifrados, acessíveis somente com chaves específicas. Isso é essencial não apenas para a proteção durante o armazenamento, mas também durante a transmissão de dados, formando uma barreira robusta contra acessos não autorizados.

---

[11] Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Além das tecnologias, a conformidade passa por uma gestão rigorosa de quem tem acesso aos dados. O controle de acesso é uma estratégia vital que utiliza autenticação forte, verificação biométrica, e políticas que definem claramente quem pode acessar o quê, baseando-se no papel ou na função do usuário dentro da organização.

Entretanto, a tecnologia por si só não é suficiente. É essencial que as políticas de privacidade e segurança da informação sejam claras, detalhadas e amplamente comunicadas a todos os envolvidos. Estas políticas devem explicar os direitos dos titulares dos dados e como a organização protege suas informações. Além disso, o treinamento regular dos colaboradores sobre essas políticas e a importância geral da proteção de dados ajuda a fortalecer a cultura de privacidade.

Um plano de resposta a incidentes bem definido completa a estratégia de conformidade, garantindo que a organização esteja preparada para responder a vazamentos de dados e outras violações de segurança de forma eficaz. Este plano deve incluir procedimentos claros para a notificação de incidentes às autoridades reguladoras e aos titulares dos dados afetados, conforme exigido pela LGPD.

Ao adotar essa abordagem integrada, combinando ferramentas tecnológicas avançadas com práticas de governança sólidas, as organizações podem não apenas cumprir com as exigências legais, mas também promover um ambiente de negócios digital que é seguro, transparente e confiável.

3 O PAPEL DAS AUTORIDADES E A COLABORAÇÃO NO CUMPRIMENTO DA LGPD

A implementação eficaz da Lei Geral de Proteção de Dados (LGPD) no comércio eletrônico requer uma atuação ativa e coordenada das autoridades reguladoras. Essas entidades têm a responsabilidade de assegurar que as empresas cumpram as disposições da lei, protegendo os direitos dos consumidores e promovendo um ambiente de negócios ético e transparente.

Essa coordenação abrange não apenas a aplicação das penalidades previstas pela lei, mas também a promoção de uma compreensão clara sobre as práticas de proteção de dados entre as empresas, especialmente aquelas que operam no âmbito digital. Ao mesmo tempo, a colaboração entre as autoridades e o

setor privado é fundamental para adequar as normas de proteção de dados às realidades tecnológicas e comerciais em constante evolução. Este esforço conjunto ajuda a mitigar riscos e fortalecer a confiança do consumidor no ambiente digital, o que é essencial para o crescimento sustentável do comércio eletrônico no Brasil. As próximas seções explorarão como a fiscalização e a colaboração são executadas na prática, detalhando o papel regulatório da ANPD e o impacto de suas atividades no dia a dia das operações comerciais online.

3.1. FISCALIZAÇÃO E APLICAÇÃO DA LGPD

A Autoridade Nacional de Proteção de Dados Pessoais (ANPD), é uma entidade especial ligada ao Ministério da Justiça e Segurança Pública, ela é responsável por supervisionar a proteção de dados pessoais e por garantir a aplicação da LGPD. Esta autoridade objetiva garantir uma observância completa e correta das normas da LGPD em território brasileiro, protegendo direitos fundamentais como a liberdade, a privacidade e o desenvolvimento da personalidade dos indivíduos. A ANPD também orienta e, quando necessário, impõe sanções a empresas que não respeitem as diretrizes de proteção de dados estabelecidas pela legislação.

Conforme estabelecido no Art. 52[12] da LGPD, as sanções administrativas aplicáveis em caso de violação das normas incluem advertências e multas que podem chegar a 2% do faturamento da empresa. Essas penalidades são aplicadas com o objetivo de assegurar o respeito aos direitos dos titulares de dados e incentivar as organizações a adotarem práticas adequadas de proteção de dados.

O propósito principal da ANPD, conforme estabelecido pelo Artigo 55-J da LGPD, é zelar pela proteção dos dados pessoais. Isso inclui garantir a aplicação das normas de proteção e aplicar sanções administrativas em caso de não conformidade. Além de fiscalizar e punir, a ANPD também tem o dever de promover a educação e a conscientização sobre as normas de proteção de dados. Ela elabora

[12] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

diretrizes e normativas que ajudam as organizações a se alinharem com a lei, incentivando a adoção de padrões que facilitam o controle dos indivíduos sobre seus próprios dados pessoais. Este aspecto é crucial, pois empodera os cidadãos e os informa sobre seus direitos, fortalecendo a transparência nas operações que envolvem dados pessoais.

A ANPD também promove a cooperação internacional, o que é fundamental em uma era onde os dados transpõem fronteiras com facilidade. A colaboração com autoridades de outros países ajuda a criar um ambiente de proteção de dados mais consistente e robusto em nível global.

Outra competência significativa da ANPD é a capacidade de elaborar normas simplificadas e diferenciadas para entidades de menor porte. Isso é especialmente importante em um país como o Brasil, onde pequenas e médias empresas constituem uma grande parte do tecido empresarial. Tais normas permitem que essas empresas implementem práticas de proteção de dados de maneira viável e eficaz, sem o peso excessivo que regras mais complexas poderiam representar.

O Art. 65[13] da LGPD, alterado pela Lei nº 14.010/2020, estabelece que as sanções administrativas previstas no art. 52 somente serão aplicadas após 1º de agosto de 2021. Essa disposição permitiu um período de adaptação para que as empresas pudessem se adequar às exigências da lei antes do início da aplicação das penalidades.

A criação da ANPD foi formalizada pela Medida Provisória nº 869/2018, que posteriormente foi convertida na Lei nº 13.853/2019. Esse ato normativo estabeleceu as competências e a estrutura do órgão, consolidando seu papel como autoridade reguladora na área de proteção de dados no Brasil.

A ANPD também é responsável por receber e analisar reclamações de titulares de dados que se sentirem lesados em seus direitos. O órgão pode iniciar investigações e processos administrativos para apurar possíveis infrações à LGPD. Nesse sentido, a ANPD atua como um intermediário entre os titulares de dados e as

[13] Art. 65. Esta Lei entra em vigor:
I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e
I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54;
II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.

empresas, buscando soluções para eventuais conflitos relacionados à proteção de dados.

Por fim, é importante ressaltar que a ANPD tem autonomia técnica e decisória, embora esteja vinculada à Presidência da República. Sua estrutura é composta por um Conselho Diretor, um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, além de órgãos de assessoramento, como o Comitê de Relações Institucionais e Governamentais e a Ouvidoria.

3.2. COLABORAÇÃO ENTRE SETOR PÚBLICO E PRIVADO

A colaboração entre o setor público e privado é essencial para promover a conscientização, o compartilhamento de melhores práticas e a implementação efetiva das normas de proteção de dados. O envolvimento ativo de ambos os setores é crucial para criar um ambiente de proteção de dados robusto e confiável.

Para alcançar uma colaboração eficaz, é importante promover o compartilhamento de conhecimento e experiências entre as empresas e as autoridades governamentais. Isso pode ser realizado por meio de workshops, seminários e treinamentos conjuntos que abordem os princípios e as obrigações estabelecidos pela LGPD. O Art. 55-J, inciso IX[14] da LGPD, atribui à ANPD a competência de promover ações de cooperação com autoridades de proteção de dados de outros países, o que pode incluir iniciativas de conscientização.

O Art. 50 da LGPD incentiva a formulação de políticas e a adoção de padrões práticos de proteção de dados, que podem ser desenvolvidos em colaboração entre os setores.

Outra forma de colaboração é o desenvolvimento de iniciativas conjuntas para promover a conformidade com a LGPD. Isso pode incluir a criação de guias práticos, ferramentas de avaliação de risco e programas de certificação para empresas. Essas iniciativas ajudam a garantir que as empresas do setor privado compreendam e implementem adequadamente as normas estabelecidas pela LGPD.

A participação de empresas e entidades do setor privado em fóruns e conselhos relacionados à proteção de dados também é uma forma importante de

[14] IX - Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

colaboração. Por exemplo, o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, inclui representantes de entidades da sociedade civil, instituições científicas, tecnológicas e de inovação, confederações sindicais representativas das categorias econômicas do setor produtivo e entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais. Essa participação permite que o setor privado contribua para a formulação de políticas e regulamentos relacionados à LGPD.

Em resumo, essa parceria entre o setor público e privado pode ajudar a superar desafios, promover a conformidade e garantir que os direitos dos titulares de dados sejam protegidos de forma eficaz.

CONCLUSÃO

Através desta pesquisa, foi possível observar o impacto profundo da LGPD no setor de e-commerce, especialmente na maneira como as empresas estão revisando suas práticas de coleta, armazenamento e uso de dados pessoais.

Os desafios enfrentados pelas empresas para a adequação são notáveis, especialmente em relação à mudança de cultura organizacional e à gestão de terceiros. Além disso, os custos financeiros associados com a conformidade podem ser significativos, impactando particularmente as pequenas e médias empresas. No entanto, as organizações que efetivamente se adaptam à legislação podem ganhar uma vantagem competitiva, reforçando a confiança dos consumidores e posicionando-se favoravelmente no mercado digital.

Para os consumidores, a LGPD reforça direitos fundamentais de acesso, correção, exclusão e portabilidade de dados pessoais. A maior transparência e o controle ampliado sobre suas informações pessoais contribuem significativamente para um ambiente de consumo digital mais seguro e confiável.

A Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel central na fiscalização da aplicação da lei, orientando empresas e promovendo uma cultura de proteção de dados no Brasil. A colaboração entre o setor público e privado emerge como um elemento crucial para garantir a eficácia da LGPD, sugerindo uma necessidade contínua de diálogo, educação e ajustes normativos para enfrentar os desafios emergentes.

Em conclusão, a LGPD representa um avanço significativo na legislação brasileira, alinhando o país com as tendências globais de proteção de dados e contribuindo para um ambiente de comércio eletrônico mais seguro e transparente. Contudo, para que o potencial da lei seja plenamente realizado, é essencial um esforço contínuo por parte de todas as partes envolvidas, visando a conformidade, a proteção dos direitos dos consumidores e o desenvolvimento sustentável do mercado digital. As futuras diretrizes da ANPD e a evolução das tecnologias de informação serão determinantes na moldagem das práticas de privacidade e proteção de dados no futuro.

REFERÊNCIAS

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.* Brasília: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 22 fev. 2024.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. *Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências.* Brasília: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 20 jan. 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: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 fev. 2024.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. Ministério da justiça e Segurança Pública. *Autoridade Nacional de Proteção de Dados.* Perguntas Frequentes – ANPD. Portal Gov.br, [Brasília], 10 fev. 2023. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd. Acesso em: 03 de maio de 2024.

Controladoria Geral do Estado do Paraná. *Cartilha de Boas Práticas no Tratamento de Dados Pessoais.* Este material tem por escopo prestar orientações sobre boas práticas para o adequado tratamento de dados pessoais em situações rotineiras do ambiente de trabalho, em especial ao que se refere a segurança da informação. Publicado no site em fevereiro de 2024. Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2024-02/boas%20pr%C3%A1ticas.pdf. Acesso em: 06 de maio de 2024.

GALVÃO & SILVA ADVOCACIA. *Lei GDPR em português.* 2020. Disponível em: <https://www.jusbrasil.com.br/artigos/lei-gdpr-em portugues/834170468#:~:text=GDPR%2C%20General%20Data%20Protection%20Regulation,pa%C3%ADs%20em%20agosto%20de%202020>. Acesso em: 27 fev. 2024.

GODOY, Larissa. *Cambridge Analytica, Facebook e GDPR: O impacto do vazamento de dados para o mercado*. **Agência Inbound**, São Paulo, 26 abr. 2018. Disponível em: https://www.agenciainbound.com.br/blog/cambridge-analyticafacebook-e-gdpr-o impacto-do-vazamento-de-dados-para-o-mercado. Acesso em: 27 fev. 2024.

LOCUS IURIS. *5 estratégias de adequação à Lei Geral de Proteção de Dados – LGPD.* 1 de março de 2024. Disponível em: https://locusiuris.com.br/estrategias-de-adequacao-lgpd/. Acesso em: 10 maio 2024.

PERINA, **Gustavo.** *Quais foram os impactos da LGPD no e-commerce?* 09 set. 2021. E-Commerce Brasil. Disponível em: https://www.ecommercebrasil.com.br/artigos/quais-foram-os-impactos-da-lgpd-no-e-commerce. Acesso em: 07 de março de 2024.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Lei Geral de Proteção de Dados Pessoais: Comentada artigo por artigo*. Salvador: Editora JusPodivm, 2019.