

**FACULDADE MAIS DE ITUIUTABA**

**RODRIGO DE PAULO SANTOS  
ROGÉRIO CALIL CORRÊA**

**A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) APLICADA PELAS  
EMPRESAS IMOBILIÁRIAS**

ITUIUTABA  
2023

RODRIGO DE PAULO SANTOS  
ROGÉRIO CALIL CORRÊA

**A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) APLICADA PELAS  
EMPRESAS IMOBILIÁRIAS**

Trabalho de conclusão de curso apresentado à banca avaliadora do curso de Direito da Facmais Ituiutaba como exigência parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. Ms. Leonardo Sebastião Delfino de Souza

ITUIUTABA  
2023

## SUMÁRIO

1.	5	
2.	Histórico da LGPD	6
3.	Aplicação da LGPD	7
3.1	Nomeação do Encarregado de Proteção de Dados	7
4	TRATAMENTO DOS DADOS	8
4.1	principais categorias de dados pessoais e suas finalidades	9
4.2	Bases legais para o tratamento de dados pessoais	10
4.3	Direitos dos titulares de dados pessoais	11
4.4	Eliminação de dados pessoais	12
5	INSTRUÇÕES DE SEGURANÇA WEB	12
5.1	Atualização da política de privacidade da imobiliária	14
6.	CONSIDERAÇÕES FINAIS	15
7.	REFERÊNCIAS	16

## A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Rodrigo De Paulo Santos

Rogério Calil Corrêa

**RESUMO:** O presente artigo versa sobre a Lei Geral de Proteção de Dados e direito imobiliário, se justifica porque é um tema atual e que impacta a vida de milhões de brasileiros devido a sua relevância no campo do direito civil. Definiu-se como pergunta problema: como a LGPD - Lei Geral de Proteção de Dados é aplicada pelas empresas imobiliárias? Para responder a essa pergunta-problema definiu-se alguns objetivos. Objetivo geral: Analisar a aplicação da Lei Geral de Proteção de Dados em empresas imobiliárias. E objetivos específicos: estudar o histórico da LGPD; verificar como a LGPD é aplicada e avaliar como as imobiliárias trabalham aplicando a LGPD em seu cotidiano. A pesquisa foi executada tomando como referência o método hipotético-dedutivo. Isto é utilizar-se-á das teorias já existentes e buscará aperfeiçoá-las, acrescentando-lhes novas explicações. De modo que se permita chegar a grandes generalizações na área estudada. Foi realizada uma pesquisa bibliográfica e documental, em obras doutrinárias, em boletins e jurisprudências. Este será um trabalho multidisciplinar conforme integrará Direito Civil e Direito Digital. Foi dividido em cinco tópicos, apresentou o histórico da LGPD, a seguir mostrou-se como ela é aplicada pelas empresas e em particular as empresas imobiliárias. Analisou-se todas as nuances do tratamento de dados, para finalmente exemplificar como se realiza segurança na WEB. Enfim se apresentam as considerações finais.

**Palavras chave:** Dados. Segurança. Web.

**ABSTRACT:** This article deals with the General Data Protection Law and real estate law, and is justified because it is a current topic that impacts the lives of millions of Brazilians due to its relevance in the field of civil law. The problem question was defined as: how is the LGPD - General Data Protection Law applied by real estate companies? To answer this question, some objectives were defined. General objective: Analyze the application of the General Data Protection Law in real estate companies. And Specific objectives: study the history of the LGPD. Check how LGPD is applied. Evaluate how real estate agencies work applying the LGPD in their daily lives. The research was carried out using the hypothetical-deductive method as a reference. That is, it will use existing theories and seek to improve them, adding new explanations to them. This allows us to reach broad generalizations in the area studied. Bibliographical and documentary research was carried out in doctrinal works, bulletins and jurisprudence. This will be a multidisciplinary work as it will integrate Civil Law and Digital Law. It was divided into five topics, presented the history of the LGPD, then showed how it is applied by companies and in particular real estate companies. It took all the nuances of data processing to finally exemplify how security is carried out at WEB. Finally, the final considerations are presented.

**Keywords:** Data. Security. Web.

## 1. INTRODUÇÃO

O assunto referente ao presente artigo é a Lei Geral de Proteção de Dados e direito imobiliário. Adotou-se como tema o Direito Digital.

Conforme a sociedade evolui, verifica-se constantes mudanças e evoluções no mundo social que impõem que o mundo jurídico acompanhe essas mudanças. Neste sentido os estudiosos e operadores do direito, precisam adequar as leis a essas mudanças, o que gera dúvidas sobre sua correta aplicação, bem como os efeitos que irão surtir no meio social (JACOMINO, 2018).

O tratamento de dados em unidade imobiliária se refere a qualquer tipo de atividade que utiliza um dado pessoal no cumprimento da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, dados estes que se encontram protegidos pela Lei nº 13.709/2018 (MARANHÃO, 2020).

Esse trabalho se justifica porque é um tema atual e que impacta a vida de milhões de brasileiros devido a sua relevância no campo do direito civil e, é importante para o futuro bacharel em Direito realizá-lo, porque é essencial saber analisar criticamente o tema para que possa atuar de forma moderna, agindo em prol do que necessitam da proteção de seus dados e também necessitam de serviços imobiliários.

Definiu-se como pergunta problema: como a LGPD - Lei Geral de Proteção de Dados é aplicada pelas empresas imobiliárias? Para responder a essa pergunta-problema definiu-se alguns objetivos. Objetivo geral: Analisar a aplicação da Lei geral de proteção de dados em empresas imobiliárias. E objetivos específicos: estudar o histórico da LGPD; verificar como a LGPD é aplicada e avaliar como as imobiliárias trabalham aplicando a LGPD em seu cotidiano.

A pesquisa foi executada tomando como referência o método hipotético-dedutivo. Isto é utilizar-se-á das teorias já existentes e busca aperfeiçoá-las, acrescentando-lhes novas explicações. De modo que se permita chegar a grandes generalizações na área estudada.

Foi realizada uma pesquisa bibliográfica e documental, em obras doutrinárias, em boletins e jurisprudências. Este será um trabalho multidisciplinar abordando áreas como Direito Civil e Direito Digital.

A leitura analítica foi realizada tendo como base os critérios analíticos temáticos e uma análise temática dos Boletins de jurisprudências a serem ainda catalogados pelo pesquisador.

A natureza dos dados operacionalizados foram primários e secundários. As fontes primárias são os documentos oficiais ou não oficiais, a jurisprudência e a legislação. Já as fontes secundárias foram os estudos realizados por outros pesquisadores, doutrinadores do Direito Pátrio.

As interpretações foram feitas de acordo com as linhas de teorias dos respectivos autores a fim de que se obtenha um resultado da análise em que permita uma conclusão sobre o tema.

Os aspectos analisados foram relativos à solução do problema proposto por este pesquisador, realizando-se um estudo dogmático jurídico, pois estudou-se a lei, a doutrina e a jurisprudência, realizando interpretações das normas elaboradas pelo legislador, investigando a sua intertextualidade com o tema proposto.

A seguir se apresenta o referencial teórico encontrado referente à LGPD. Este artigo contempla o uso e armazenamento de dados por empresas imobiliárias. Como coletam dados, armazenam e utilizam os mesmos.

## 2. Histórico da LGPD

Com o advento da internet e o uso *on line* de dados pessoais, uma vez que estes tornaram-se um produto para inúmeras empresas no ramo da tecnologia a preocupação com a proteção de dados dos cidadãos aumentou muito. Essa preocupação levou diversos países à iniciativa de normatizar o tema, caso que não foi diferente do Brasil, que buscou caminhos para garantir a proteção de dados e privacidade dos indivíduos que disponibilizaram seus dados (MARANHÃO, 2020).

O processo de criação da LGPD no Brasil começou com o Projeto de Lei nº 53/2018, que foi apresentado em fevereiro de 2018 e passou por várias revisões e emendas antes de ser aprovado (KUBIAK, 2022).

Como a Medida Provisória nº 959/2020 não foi convertida em Lei, a vigência da LGPD se inicia quando ela perder seu efeito: em setembro de 2020 (prevalecendo a redação anterior do art. 65, II, da LGPD). No entanto, as disposições relativas às penalidades (artigos 52, 53 e 54 a LGPD) que podem ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD) somente passaram a valer a partir de 1º de agosto de 2021 (art. 65, I-A, da LGPD). Sendo assim, a partir de setembro de 2020, todos deveriam estar adequados à LGPD (GARCIA, 2020).

A ANPD - Autoridade Nacional de Proteção de Dados é uma autarquia federal de natureza especial do Brasil que, atualmente, se encontra vinculada ao Ministério da Justiça e Segurança Pública e possui atribuições relacionadas a proteção de dados pessoais e da privacidade e, sobretudo, deve realizar a atuação como agência fiscalizadora, vinculada à Presidência da República, com autonomia técnica e decisória. Desde de agosto de 2021, a ANPD poderá aplicar sanções administrativas como, advertência, multa simples de até 2% do faturamento da pessoa jurídica (máximo de 50 milhões de reais), multa diária, exposição da infração, bloqueio e eliminação de dados pessoais, suspensão parcial do banco de dados, suspensão da atividade de tratamento de dados e proibição de atividades relacionadas a tratamento de dados (art. 52 da LGPD). No entanto, essas punições ainda precisam ser regulamentadas pela própria ANPD e serão objeto de consulta pública, conforme determina o art. 53 da LGPD (MARANHÃO, 2020).

Neste cenário foi aprovada a Lei nº 13.709/2018, chamada de Lei Geral de Proteção de Dados – LGPD, que teve o objetivo garantir a privacidade dos dados pessoais no Brasil e regulamentar as atividades relacionadas a qualquer tipo de uso de dados pessoais coletados e armazenados pelas organizações (JACOMINO, 2018).

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que regula o tratamento de dados pessoais no país. Sua história inclui várias etapas e influências de outras regulamentações de proteção de dados em todo o mundo. Foi sancionada pelo então presidente Michel Temer em agosto de 2018. No entanto, a data de entrada em vigor da lei foi adiada para setembro de 2020. Foi fortemente influenciada pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, que entrou em vigor em maio de 2018 e o mundo veio a adotar regulamentações semelhantes (KUBIAK, 2022).

O Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) é uma regulamentação de proteção de dados pessoais que entrou em vigor em 25 de maio

de 2018, na União Europeia. Ele tem como objetivo estabelecer regras claras e abrangentes para o tratamento de dados pessoais e fortalecer a proteção da privacidade dos cidadãos europeus. O GDPR substituiu a Diretiva 95/46/CE, que datava de 1995, e trouxe mudanças significativas nas práticas de coleta, armazenamento, processamento e transferência de dados pessoais (ANASTASIA; LARA, 2019).

A Lei Geral de Proteção de Dados (LGPD) entrou em vigor em 18 de setembro de 2020, no Brasil. Um dado de vigiância foi estabelecido após um período de transição desde a sanção da lei, permitindo que empresas e organizações se adequassem às suas disposições e cumprissem os requisitos de proteção de dados pessoais. A LGPD tem como objetivo regulamentar o tratamento de dados pessoais no Brasil, proteger a privacidade dos cidadãos e estabelecer direitos e responsabilidades claras em relação ao processamento de informações pessoais. A LGPD faz parte de um movimento global em direção a regulamentações de proteção de dados mais robustas e é projetada para proteger a privacidade das pessoas e garantir que as empresas processem dados pessoais de forma adequada e segura. Seu histórico inclui influências do GDPR e um processo legislativo que levou à criação dessa importante lei de proteção de dados no Brasil (GARCIA, 2020).

### **3. Aplicação da LGPD**

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que visa proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural. A LGPD entrou em vigor em setembro de 2020 e tem como objetivo regulamentar o tratamento de dados pessoais por organizações públicas e privadas (ANASTASIA; LARA, 2019).

A aplicação da LGPD implica em uma série de obrigações e direitos para as empresas que lidam com dados pessoais. As principais práticas e ações relacionadas à LGPD serão apresentadas a seguir. Primeiramente as empresas devem designar um encarregado de Proteção de Dados, responsável por mediar as relações entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (ANASTASIA; LARA, 2019.).

#### **3.1 Nomeação do Encarregado de Proteção de Dados**

A nomeação do encarregado de Proteção de Dados (DPO, do inglês Data Protection Officer) é uma obrigação imposta pela Lei Geral de Proteção de Dados (LGPD) no Brasil. O DPO é uma figura-chave na implementação e conformidade com as práticas de proteção de dados. Sobre a nomeação do DPO de acordo com a LGPD seguem as orientações abaixo.

Em conformidade com a LGPD, a nomeação do DPO é obrigatória para drivers e inovação que realizam o tratamento de dados pessoais. A obrigação de designar um DPO aplica-se a organizações de qualquer porte que realizem o tratamento de dados pessoais de maneira regular e em grande escala, ou que tratem dados de forma sensível (MARANHÃO, 2020).

O DPO deve ser uma pessoa natural, com conhecimento especializado em privacidade e proteção de dados. Pode ser um profissional interno da organização ou ter suas funções desempenhadas por um terceiro, como um serviço terceirizado (KUBIAK, 2022).

O DPO desempenha um papel fundamental na supervisão do cumprimento da LGPD. Ele orienta a organização quanto às suas obrigações, fornece aconselhamento sobre a avaliação do impacto à proteção de dados, monitora a conformidade com a legislação e é ponto de contato com a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados. O DPO deve exercer suas funções de maneira independente, sem sofrer influências indevidas. Não deve haver conflito de interesses entre as funções do DPO e outras atividades de organização. A nomeação do DPO deve ser registrada e divulgada pela organização (GARCIA, 2020).

As informações de contato do DPO deverão ser disponibilizadas publicamente para que os titulares dos dados e a ANPD possam contatá-los facilmente. A nomeação do DPO é uma medida importante para garantir que as organizações estejam em conformidade com a LGPD, promovendo a transparência, a responsabilidade e a proteção efetiva dos dados pessoais. O DPO desempenha um papel crucial na implementação de boas práticas de privacidade e na mitigação de riscos relacionados ao tratamento de dados (ANASTASIA; LARA, 2019).

As organizações devem realizar um mapeamento detalhado de todos os dados pessoais que coletam, processam e armazenam. Esses dados devem ser classificados de acordo com sua sensibilidade. O tratamento de dados pessoais requer o consentimento explícito do titular, que deve ser informado de forma clara e acessível especificamente para o tratamento (GARCIA, 2020).

Os titulares dos dados têm vários direitos, como o acesso aos seus dados, a correção de informações incorretas, a exclusão de dados desnecessários e o direito de revogar o consentimento. As empresas são obrigadas a adotar medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados ou situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (MARANHÃO, 2020).

Quando houver compartilhamento de dados com terceiros, as organizações devem garantir que esses terceiros também estejam em conformidade com a LGPD. Em caso de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares, as empresas deverão comunicar à ANPD e, quando cabível, aos titulares dos dados. Em determinadas situações, as organizações devem realizar uma AIPD, avaliando os riscos do tratamento de dados pessoais para a privacidade (JACOMINO, 2018).

A ANPD é o órgão responsável por fiscalizar e aplicar sanções em caso de descumprimento da LGPD. As deliberações podem incluir advertências, multas de até 2% do faturamento da empresa (limitadas a R\$ 50 milhões por infração), bloqueio de dados pessoais até a regularização e a eliminação dos dados.

A aplicação da LGPD é fundamental para garantir a proteção da privacidade dos indivíduos e promover a transparência e a responsabilidade no tratamento de dados pessoais no ambiente digital (KUBIAK, 2022).

#### **4 TRATAMENTO DOS DADOS**

O GDPR - General Data Protection Regulation se aplica a todas as empresas, organizações e indivíduos que processam dados pessoais de cidadãos do Brasil, independentemente de onde estejam localizados no mundo. Isso significa que as empresas fora do Brasil também devem cumprir o regulamento ao lidarem com dados de pessoas. O GDPR estabelece que o consentimento para o tratamento de dados pessoais deve ser claro, específico e voluntário. Os titulares de dados devem ser

informados sobre o motivo e especificamente da coleta de seus dados (JACOMINO, 2018).

O regulamento concede aos indivíduos diversos direitos, incluindo o direito de acessar, concordar, apagar, limitar o processamento e portar seus dados pessoais. As organizações são responsáveis por adotar medidas técnicas e específicas para garantir a segurança e a proteção dos dados pessoais que tratam (GARCIA, 2020).

O GDPR exige que as organizações notifiquem as autoridades de proteção de dados e os titulares de dados afetados em caso de violação de dados pessoais, a menos que a violação seja denunciada de resultar em riscos para os direitos e liberdades dos titulares de dados. O RGPD estabelece as Autoridades de Proteção de Dados em cada Estado-Membro da UE, que são responsáveis pela supervisão do cumprimento das regras do regulamento (ANASTASIA; LARA, 2019).

O GDPR prevê multas substanciais para empresas que não cumpram suas disposições, com prejuízos que podem chegar a 20 milhões de euros ou 4% do faturamento anual global da empresa, o que é maior. O GDPR teve um impacto significativo no cenário global de proteção de dados e influenciou a criação de leis semelhantes em outros países, incluindo a Lei Geral de Proteção de Dados (LGPD) no Brasil. Ele visa garantir a privacidade e a segurança dos dados pessoais dos cidadãos europeus e promover a transparência no tratamento desses dados por parte das organizações (JACOMINO, 2018).

A entrada em vigor da LGPD foi adiada em alguns benefícios, principalmente devido à pressão de empresas e organizações que alegavam não estar preparadas para cumprir as novas regras (GARCIA, 2020).

A LGPD entrou em vigor efetivamente em setembro de 2020. A partir desses dados, as empresas e organizações no Brasil tiveram que cumprir suas disposições e começar a se adequar às regras de proteção de dados pessoais. A LGPD é distribuída à Autoridade Nacional de Proteção de Dados (ANPD) como o órgão responsável por fiscalizar e fazer cumprir a lei, além de fornecer orientações sobre a conformidade (JACOMINO, 2018).

A LGPD tem um grande impacto na privacidade dos cidadãos brasileiros e impõe obrigações significativas às empresas que tratam dados pessoais. Ela estabelece direitos para os titulares de dados, como o direito de acessar, concordar, excluir e portar seus dados pessoais (KUBIAK, 2022).

#### **4.1 Principais categorias de dados pessoais e suas finalidades**

As categorias de dados pessoais e suas especificidades podem variar de acordo com a natureza da organização, a legislação aplicável e o contexto específico do tratamento de dados. No entanto, algumas categorias gerais de dados pessoais e suas finalidades comuns incluem desde dados de Identificação como por exemplo: nome, sobrenome, número de identificação, número de documentos. A identificação do titular dos dados, criação de registros, autenticação (FORNASIER, 2020).

Os dados de contato, exemplos: endereço de e-mail, número de telefone, endereço postal. Esses dados têm como finalidades a comunicação, notificações, entrega de produtos ou serviços (MARANHÃO, 2020).

Também são coletados dados demográficos, por exemplo, idade, gênero, estado civil, nacionalidade, a fim de realizar análise demográfica, personalização de serviços, direcionamento de marketing. Dados de Localização, como dados de GPS, endereço IP, já que há serviços baseados em localização, análise de tráfego, personalização de conteúdo.

São ainda coletados dados financeiros, por exemplo, números de contas bancárias, cartões de crédito. A fim de processar transações, faturamentos e prevenção de fraudes (FORNASIER, 2020).

Também são coletados dados de saúde, como histórico médico, informações sobre condições de saúde, para as melhores formas de prestação de cuidados de saúde, pesquisa médica, seguros.

Dados de Emprego como cargo, histórico de emprego, salário, são guardados para facilitar processos de recrutamento, gestão de recursos humanos, pagamento de mudança (BASAN; FALEIROS JÚNIOR, 2020).

Há coleta de dados de comportamento *online*, por exemplo histórico de navegação, visualizações *online*, para facilitar trabalhos em publicidade direcionada, personalização de conteúdo, análise de mercado (JACOMINO, 2018).

Para autenticação, segurança, controle de acesso são armazenados dados biométricos como impressões digitais, reconhecimento facial (ANASTASIA; LARA, 2019).

Os dados genéticos, visam monitorar informações relacionadas ao DNA, pesquisa médica, diagnóstico genético, genealogia (BASAN; FALEIROS JÚNIOR, 2020).

Assim, com ampla gama de dados coletados é de suma importância que as organizações e no caso em tela as empresas imobiliárias identifiquem e documentem as categorias específicas de dados pessoais que coletam e processam, bem como as específicas para que esses dados sejam utilizados. Além disso, é fundamental obter o consentimento adequado dos titulares dos dados quando necessário, e garantir que o tratamento esteja em conformidade com as leis de proteção de dados aplicáveis (KUBIAK, 2022).

## 4.2 Bases legais para o tratamento de dados pessoais

O tratamento de dados pessoais deve ter uma base legal de acordo com as leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regulamento Geral de Proteção de Dados (GDPR) na Europa, entre outras regulamentações em diferentes jurisdições existentes pelo mundo. As bases legais para o tratamento de dados pessoais geralmente variam muito de país para país, mas uma das bases mais conhecidas é a autorização do titular dos dados. Isso significa que uma pessoa autoriza explicitamente o tratamento de seus dados para uma finalidade específica. O consentimento deve ser livre, informado e inequívoco (JACOMINO, 2018).

O tratamento de dados pode ser realizado quando necessário para a proteção da vida ou a integridade física do titular dos dados ou de terceiros. O tratamento de dados pode ser necessário para a tutela da saúde, como o diagnóstico médico, a prestação de cuidados de saúde ou tratamentos médicos (JACOMINO, 2018).

O tratamento de dados pode ser necessário para o cumprimento de uma missão de interesse público ou para o exercício regular de direitos em processo judicial, administrativo ou arbitral (FORNASIER, 2020).

Para as imobiliárias é muito importante na execução do contrato dar o devido tratamento de dados pode ser necessário para a celebração de um contrato, não importando qual pessoa seja parte, ou para medidas preliminares relacionadas a um contrato. Por exemplo, a coleta de informações de contato, emprego e financeira para a realização de um contrato de aluguel (MARANHÃO, 2020).

O tratamento de dados pode ser necessário para o cumprimento de uma obrigação legal a qual o controlador está sujeito. Isso inclui situações em que o processamento é necessário para cumprir obrigações fiscais ou regulatórias (FORNASIER, 2020).

O tratamento de dados pode ser justificado com base nos interesses legítimos do controlador, a menos que os interesses ou direitos e liberdades fundamentais do titular dos dados prevaleçam sobre esses interesses (ANASTASIA; LARA, 2019).

O tratamento de dados pode ser justificado para a proteção do crédito, desde que seja realizado de acordo com as normas legais aplicáveis (JACOMINO, 2018).

É importante que as imobiliárias identifiquem e documentem claramente a base legal para o tratamento de dados pessoais em conformidade com as leis locais de proteção de dados. Além disso, é fundamental garantir que o tratamento seja proporcional especificamente à qualidade dos dados que foram perdidos e que os direitos dos titulares dos dados sejam respeitados (KUBIAK, 2022).

### **4.3 Direitos dos titulares de dados pessoais**

A LGPD (Lei Geral de Proteção de Dados) garante aos titulares de dados pessoais uma série de direitos para proteger a privacidade e a autonomia sobre suas informações pessoais (LIMA, et al. 2020). Os principais direitos conferidos aos titulares de dados pela LGPD serão apresentados a seguir:

Os titulares têm o direito de confirmar se uma entidade está tratando seus dados pessoais e, quando confirmados, têm o direito de acessar esses dados. Têm o direito de corrigir dados pessoais incompletos, inexatos ou desatualizados. Têm o direito de solicitar a eliminação de seus dados pessoais, desde que o tratamento não esteja em conformidade com a lei (O'NEIL, 2020).

Os titulares têm o direito de receber seus dados pessoais em um formato estruturado, de uso comum e leitura automática, para transferência para outro fornecedor de serviço, têm o direito de serem informados de forma clara e transparente sobre o tratamento de seus dados pessoais, incluindo especificamente, formas de tratamento, prazos de armazenamento, entre outros (JACOMINO, 2018).

Os titulares podem oferecer determinados tipos de tratamento de dados pessoais, como para fins de *marketing* direto. Quando o tratamento de dados é baseado no consentimento do titular, este tem o direito de revogar este consentimento a qualquer momento, sem prejudicar a legalidade do tratamento realizado antes da revogação (PINHEIRO, 2018).

Os titulares têm o direito de solicitar a revisão de decisões tomadas unicamente com base no processamento automatizado de dados pessoais que afetem seus interesses. Tem o direito de não serem submetidos a decisões automatizadas ou a tratamento discriminatório que vise à formação de perfis comportamentais, salvo se houver consentimento, fornecimento de serviços ou produtos equivalentes, ou outros motivos previstos na lei (KUBIAK, 2022).

Ainda têm o direito de serem informados sobre as entidades públicas ou privadas com as quais o controlador realizou o uso compartilhado de dados. Esses direitos visam garantir que os titulares tenham controle sobre seus dados pessoais e possam exercer escolhas informadas sobre como suas informações são coletadas, processadas e compartilhadas. Cabe ressaltar que o exercício desses direitos está sujeito a certas condições e limitações previstas na legislação. Além disso, a Autoridade Nacional de Proteção de Dados (ANPD) pode fornecer orientações adicionais sobre a aplicação desses direitos (JACOMINO, 2018).

#### 4.4 Eliminação de dados pessoais

Os titulares de dados têm diversos direitos pessoais garantidos pelas leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e outras legislações semelhantes em diferentes jurisdições (BASAN; FALEIROS JÚNIOR, 2020). Os principais direitos dos titulares de dados estão listados abaixo.

Direito de acesso (ou direito de Conhecimento) se refere ao direito que os titulares têm o direito de obter confirmação de que seus dados pessoais estão sendo processados e, se for o caso, acessar esses dados (RUARO; GLITZ, 2020).

Direito de retificação, onde os titulares têm o direito de corrigir dados pessoais imprecisos ou incompletos que sejam processados por uma organização. Direito de exclusão (ou "direito ao esquecimento"), os titulares têm o direito de solicitar a exclusão de seus dados pessoais, especialmente quando os dados não são mais necessários para a finalidade específica para a qual foram coletados (SARLET, 2021).

Direito à portabilidade de dados, os titulares têm o direito de receber os dados pessoais que fornecem uma organização em um formato estruturado e comumente usados, e têm o direito de transmitir esses dados a outra organização, quando tecnicamente viável (MARANHÃO, 2020).

Direito de oposição ao processamento, no qual os titulares têm o direito de se opor ao processamento de seus dados pessoais em determinadas circunstâncias, como para fins de *marketing* direto. Direito à limitação do processamento, onde os titulares têm o direito de solicitar a limitação do processamento de seus dados em determinadas situações, como quando contestam a precisão dos dados ou quando o processamento é considerado ilegal (BASAN; FALEIROS JÚNIOR, 2020).

Direito de não ser submetido a decisões automatizadas, no qual os titulares têm o direito de não estarem sujeitos a decisões baseadas unicamente em processamento automatizado, incluindo a criação de perfis, quando essas decisões têm efeitos significativos sobre eles (TEFFÉ, 2020).

Direito ao consentimento informado, os titulares têm o direito de dar seu consentimento de forma livre, informada, específica e inequívoca para o processamento de seus dados pessoais. Eles também têm o direito de cancelar o registro a qualquer momento (ZUBOFF, 2019).

Direito de recuperação, na qual os titulares têm o direito de apresentar reclamações às autoridades de proteção de dados se considerarem que o processamento de seus dados pessoais viola as leis de proteção de dados (KUBIAK, 2022).

Esses direitos têm como objetivo garantir a transparência, a privacidade e o controle sobre os dados pessoais dos indivíduos. As organizações que tratam dados pessoais devem estar cientes desses direitos e implementar práticas e políticas para garantir o seu respeito (JACOMINO, 2018).

## 5 INSTRUÇÕES DE SEGURANÇA WEB

A implementação de medidas de segurança na web é fundamental para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD) no Brasil. As instruções de segurança específicas para a web, considerando os princípios e requisitos da LGPD serão apresentadas abaixo:

O uso de criptografia de Dados é indicado, por isso é importante que se utilize conexões seguras (HTTPS) para garantir a criptografia dos dados no trânsito entre o

navegador do usuário e o servidor web. É muito indicado que se armazene dados sensíveis de forma criptografada, tanto em trânsito quanto em segurança (MARANHÃO, 2020).

Acredita-se que as empresas devem implementar políticas rigorosas de controle de acesso para garantir que apenas usuários autorizados tenham acesso aos dados pessoais, inclusive é importante utilize autenticação forte, como autenticação de dois fatores, sempre que possível (BASAN; FALEIROS JÚNIOR, 2020).

A fim de garantir a segurança é importante manter o monitoramento e a auditoria da empresa por meio do estabelecimento de sistemas de monitoramento contínuo para identificar e responder às atividades suspeitas. Com relação aos registros de auditorias detalhadas é importante que estes sejam rastreáveis sobre quem acessa, modifica ou exclui dados pessoais (MIRAGEM, 2020).

Manter todos os sistemas, servidores e aplicativos da web atualizados com as últimas correções de segurança para evitar vulnerabilidades conhecidas (MAGRANI, 2020).

Para isso sugere-se implementar firewalls e sistemas de detecção/prevenção de intrusões para proteção contra-ataques, como injeção de SQL, *cross-site scripting* (XSS) e *cross-site request forgery* (CSRF) (LIMA, et al. 2020).

Há sugestões de que se realize testes de segurança regularmente para identificar e corrigir vulnerabilidades potenciais. Com relação a políticas de retenção de dados, as empresas precisam estabelecer políticas claras de retenção de dados para garantir que os dados pessoais não sejam armazenados por mais tempo do que o necessário (KAISER, 2020).

Assim, sugere-se que sejam implementados processos automatizados para exclusão ou anonimização de dados após o término do período de retenção (GROSSI, 2020).

A empresa também precisa ter um plano de resposta a incidentes que inclua procedimentos claros para notificar as autoridades e os titulares dos dados em caso de violação de segurança (KUBIAK, 2022).

A respeito dos funcionários é de suma importância que eles sejam treinados é proporcional ao treinamento regular em segurança da informação para funcionários envolvidos no tratamento de dados pessoais a segurança de seus usuários. A imobiliária precisa ter uma cultura de segurança conscientizando os colaboradores sobre a importância da proteção de dados (GARCIA, 2020).

Um plano de privacidade por Design e por Padrão, é importante de ser implementado, já que os princípios de privacidade desde a concepção (*privacy by design*) e, sempre que possível, configure sistemas para coletar apenas os dados necessários (*privacy by default*) (FORNASIER, 2020).

Com relação à política de cookies e rastreamento, é importante que a empresa forneça informações claras sobre o uso de cookies e outras tecnologias de rastreamento, recebendo o consentimento adequado dos usuários quando necessário (JACOMINO, 2018).

Essas instruções representam diretrizes gerais, mas é importante adaptá-las às especificidades da imobiliária como no caso desta temática sugere e aos requisitos específicos da LGPD. Além disso, uma imobiliária precisa considerar a consultoria de profissionais de segurança da informação pode ser útil para garantir uma implementação eficaz das medidas de segurança (DONEDA, 2020).

## 5.1 Atualização da política de privacidade da imobiliária

A atualização de políticas de conformidade com a Lei Geral de Proteção de Dados (LGPD) é uma prática essencial para garantir que as organizações estejam em conformidade contínua e atendam aos requisitos em constante evolução (KUBIAK, 2022). Segue as orientações sobre como proceder com a atualização da política da LGPD:

Uma imobiliária precisa estabelecer um cronograma regular para revisar e, se necessário, atualizar a política da LGPD. Isso pode ser anual ou sempre que haja alterações significativas nas operações ou na legislação (CZYMMEC, 2019).

A empresa precisa realizar avaliação de Impacto à Proteção de Dados (AIPD), neste sentido deve realizar avaliações de impacto à proteção de dados para identificar e avaliar os riscos associados ao tratamento de dados pessoais. Isso ajuda a determinar se as configurações na política são necessárias (MARANHÃO, 2020).

Observar as mudanças na legislação mantendo a imobiliária atualizado sobre as alterações na legislação de proteção de dados. Se houver alterações nas leis, ajustar sua política de acordo (BASAN; FALEIROS JÚNIOR, 2020).

E tornou-se muito importante dar feedback aos titulares de dados, considerando obter feedback dos titulares de dados sobre a política. Isso pode ser feito por meio de pesquisas, formulários de feedback ou outras formas de comunicação bidirecional (JACOMINO, 2018).

No que tange a treinamento e conscientização, uma imobiliária precisa constantemente atualizar os programas de treinamento para funcionários em relação às políticas atualizadas. Certificando-se de que todos os funcionários estejam cientes das mudanças e compreendam suas responsabilidades (BIONI; DIAS, 2020).

E na ocorrência de inclusão de novos requisitos, sugere-se a inclusão de todos os novos requisitos ou padrões que possam surgir na última atualização. Isso pode incluir melhores práticas de segurança da informação e protocolos de resposta a incidentes tornando a empresa mais eficiente (BIONI, 2019).

Referente ao uso de política de cookies e rastreamento, como já foi dito anteriormente a empresa precisa constantemente se atualizar, se a organização utiliza cookies ou outras tecnologias de rastreamento, é fundamental revisá-la e atualizá-la regularmente para garantir que esteja em conformidade com as regulamentações de consentimento (JACOMINO, 2018).

A respeito de responsabilidades e funções, a empresa deve manter-se atualizada, com as cláusulas da política que descrevem as responsabilidades e funções dos diferentes envolvidos no tratamento de dados, incluindo o Encarregado de Proteção de Dados (DPO) (BASAN; FALEIROS JÚNIOR, 2020).

Com relação à revisão de contratos com processadores de dados, o responsável deve compartilhar dados com aceleração de dados, revisando-os e atualizando-os para garantir que incluam cláusulas de proteção de dados aplicáveis (MARANHÃO, 2020).

Toda empresa precisa ter uma comunicação transparente, por isso deve informar seus usuários sobre as mudanças na política seja transparente e facilmente compreensível para os titulares dos dados. Manter o registro claro dos dados de revisão e atualização da política pode ser útil para demonstração em auditórios ou em caso de questionamentos (KUBIAK, 2022).

O dono de uma imobiliária e seus colaboradores devem se lembrar que a LGPD enfatiza a transparência e a responsabilidade no tratamento de dados pessoais. Portanto, é crucial manter as políticas atualizadas e comunicar de maneira eficaz as

práticas de tratamento de dados aos titulares e às outras partes interessadas (JACOMINO, 2018).

Esta Política de Privacidade e Proteção de Dados Pessoais poderá ser alterada a qualquer tempo caso haja necessidade. Por isso, recomenda-se que seja consultada com regularidade e verificada a data de modificação (KUBIAK, 2022).

## **6. CONSIDERAÇÕES FINAIS**

A Lei Geral de Proteção de Dados (LGPD) entrou em vigor no Brasil desde setembro de 2020. A LGPD é uma legislação que tem como objetivo regulamentar o tratamento de dados pessoais por organizações públicas e privadas. Ela é inspirada no Regulamento Geral de Proteção de Dados (GDPR) do Brasil e visa garantir a privacidade e a segurança das informações pessoais dos cidadãos.

Analisa pontos importantes relacionados ao avanço trazido pela LGPD, a seguir se apresentam as conclusões obtidas:

A LGPD reforça o direito à privacidade e estabelece princípios para o tratamento adequado de dados pessoais. Isso promove uma cultura de respeito à privacidade, encorajando as organizações a adotarem práticas mais transparentes e éticas em relação ao uso de dados.

A LGPD atribui responsabilidade às empresas que coletam e processam dados pessoais. Elas são obrigadas a adotar medidas de segurança para proteger essas informações e garantir que seu uso seja consentido pelos titulares dos dados.

A legislação exige que as empresas obtenham o consentimento explícito dos titulares dos dados antes de coletar e processar suas informações. Além disso, as organizações devem ser transparentes quanto às especificidades para quais dados serão utilizados.

A LGPD concede aos titulares dos dados diversos direitos, como o acesso aos seus dados, a correção de informações incorretas e o direito de exclusão. Isso fortalece a posição dos indivíduos em relação ao controle de suas informações pessoais.

Impacto nas Empresas: A implementação da LGPD pode exigir esforços significativos das empresas para se adequarem às novas regulamentações. Isso inclui a revisão e o aprimoramento de políticas internacionais, a designação de encarregados pela proteção de dados, e a implementação de medidas de segurança robustas.

A LGPD também contribui para a conscientização sobre a importância da proteção de dados. Ela incentiva a educação contínua das empresas e da população em geral sobre boas práticas de privacidade e segurança.

A LGPD estabelece deliberações para o descumprimento das normas, incluindo multas significativas. Isso cria um incentivo para que as organizações estejam em conformidade e reforcem a importância da fiscalização para garantir o cumprimento das regras.

No geral, a LGPD representa um avanço significativo na proteção da privacidade e no tratamento responsável de dados pessoais no Brasil. A sua implementação bem-sucedida requer um compromisso contínuo por parte das empresas e uma mudança cultural em relação à privacidade e segurança da informação.

## 7. REFERÊNCIAS

ANASTASIA, Vittoria Alvares; LARA, Caio Augusto Souza. **O Escândalo Cambridge Analytica: A Manipulação de Dados na Era Digital**. volume 04, nº 31. Curitiba: 2019, pp. 164 - 167.

BASAN, Arthur Pinheiro; FALEIROS JÚNIOR, José Luiz de Moura. **A proteção de dados pessoais e a concreção do direito ao sossego no mercado de consumo**. *civilistica.com*, vol. 9, nº 3, pág. 1 – 27, 2020.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 1ª edição. Rio de Janeiro: Forense, 2019.

BIONI, Bruno; DIAS, Daniel. **Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor**. *Civilistica.com*, vol. 9, n. 3, pág. 1-23, 2020.

BRASIL. Supremo Tribunal Federal (plenário). **Ação Direta de Inconstitucionalidade 6.387/DF**. Relatora: Ministra Rosa Weber. Data do julgamento: 07 de maio de 2020. Data da publicação: 12 de novembro de 2020.

CZYMMECK, Anja. **Proteção de Dados Pessoais: Privacidade Versus Avanço Tecnológico**. Cadernos Adenauer XX, nº3. Rio de Janeiro: Fundação Konrad Adenauer, 2019.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2ª edição, revista e atualizada. São Paulo: Thomson Reuters, 2020.

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge **Analytica: Escândalo, Legado e Possíveis Futuros para a Democracia**. Revista Direito em Debate, volume 29, nº 53, pp. 182-85195, 26 de maio de 2020. Disponível em: <<https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033>>. Acesso em: 29 de abril de 2023.

GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados Pessoais (LGPD): guia de implantação**. São Paulo: Editora Edgard Blucher, 2020.

GROSSI, Bernardo Menicucci. **Lei Geral de Proteção de Dados: uma análise preliminar da lei 13.709/2018 e da experiência de sua implantação no contexto empresarial**. Porto Alegre: Editora Fi, 2020.

JACOMINO, Sérgio. **Sistema de Registro de Imóveis eletrônico**. 2018. Disponível em: <http://bit.ly/2V49S13>. Acesso em 20 de jul de 2023

KAISER, Brittany. **Manipulados: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque**. 1ª edição. Rio de Janeiro: Harper Collins, 2020.

KUBIAK, Alexander **Santos A implementação da Lei Geral de Proteção de Dados no setor de corretagem imobiliária de Santana do Livramento**. 125 p. Trabalho de Conclusão de Curso (Graduação) -- Universidade Federal do Pampa, Direito, 2022.

LIMA, Ana Paula Moraes Canto de; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. **LGPD - Lei Geral de Proteção de Dados: sua empresa está pronta?** São Paulo: Literare Books International, 2020.

LIMA, Ana Paula Moraes Canto de; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. **LGPD - Lei Geral de Proteção de Dados: sua empresa está pronta?** São Paulo: Literare Books International, 2020.

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2ª edição. Porto Alegre: Arquipélago Editorial, 2019.

MARANHÃO, Juliano Souza de Albuquerque. **Proteção de Dados e o Registro Imobiliário**. 2020. Disponível em: <https://near-lab.com/>. Acesso em: 20 de set de 2023.

MIRAGEM, Bruno. **A Lei Geral de Proteção de Dados (lei 13.709/2018) e o direito do consumidor**. Revista dos Tribunais, vol. 1009, novembro, 2019. Disponível em: <<https://brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-doconsumidor.pdf> >. Acesso em 28 de abril de 2023.

MOROZOV, Evgene. **BIG TECH: a Ascensão dos Dados e a Morte da Política**. 6ª edição. São Paulo: Ubu Editora, 2018.

O'NEIL, Cathy. **Algoritmos de Destruição em Massa: Como o Big Data aumenta a desigualdade e ameaça a democracia**. 1ª edição. Santo André: Editora Rua do Sabão, 2020.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: comentários à Lei nº 13.709/2018 (LGPD)**. São Paulo: Saraiva Jur, 2018.

RUARO, Regina Linden; GLITZ, Gabriela Pandolfo Coelho. **Panorama geral da Lei Geral de Proteção de Dados pessoais no Brasil e a inspiração no Regulamento Geral de Proteção de Dados pessoais europeu**. Revista de Estudos e Pesquisas Avançadas do Terceiro Setor, v.6, nº2, p.340-356, Jul-Dez. Brasília, 2019.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. **A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) - L.13.709/2018**. Revista direitos fundamentais & democracia. Curitiba, vol. 26, n. 2, pág. 81-106, mai./ago., 2021.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. Civilistica. com, vol. 9, n. 1, pág. 1-38, 2020.

ZUBOFF, Shoshana. **A Era do Capitalismo da Vigilância: a luta por um futuro humano na nova fronteira do poder**. 1ª edição. Rio de Janeiro: Editora Intrínseca, 2019.

