

LANA GESSICA VIEIRA GOMES

**LEI GERAL DE PROTEÇÃO DE DADOS Nº 13.709/2018: privacidade  
como direito fundamental**

CURSO DE DIREITO – UniEVANGÉLICA

2022

LANA GESSICA VIEIRA GOMES

**LEI GERAL DE PROTEÇÃO DE DADOS Nº 13.709/2018: privacidade  
como direito fundamental**

Monografia apresentada ao Núcleo de Trabalho de Curso do Curso de Direito da UniEVANGÉLICA, como exigência parcial para a obtenção do grau de bacharel em Direito, sob a orientação da Prof<sup>a</sup>. M.e Karla de Souza Oliveira.

ANÁPOLIS – 2022

LANA GESSICA VIEIRA GOMES

**LEI GERAL DE PROTEÇÃO DE DADOS Nº 13.709/2018: privacidade  
como direito fundamental**

Anápolis, \_\_\_\_\_ de \_\_\_\_\_ de 2022.

Banca Examinadora

---

---

## **AGRADECIMENTOS**

Agradeço a Deus, em primeiro lugar, pois sem ele eu não teria forças para essa longa jornada. Aos meu pais pela contribuição na formação do meu caráter. Obrigada por terem fé em mim e orgulho da minha trajetória. Aos meus amigos, pelo apoio incondicional. Minha eterna gratidão a todos os professores que me acompanharam durante a graduação, em especial ao Prof. Karla de Souza Oliveira, pela realização deste trabalho.

*Que você não poupe esforço para ser generosa,  
compartilhe o que você pode, nada mais, nada  
menos.*

*Que você saiba o significado da palavra  
felicidade.*

*Que você sempre lidere com paixão.  
Que você seja tratado como um convidado  
estimado.*

*Que você possa descansar, que você possa  
recuperar o fôlego e que o melhor do seu dia de  
hoje seja o pior do seu amanhã.*

**– Jason Mraz**

## RESUMO

O presente trabalho tem como objetivo abordar acerca da regulamentação da proteção dos dados pessoais a partir da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), ao demonstrar por meio de conceitos importantes a necessidade do surgimento de uma legislação específica que tutelasse a privacidade do titular dos dados pessoais frente a nova era da informação. A metodologia do estudo consiste inicialmente em apresentar o surgimento do direito à privacidade em e seus aspectos históricos, sucedendo-se uma análise de algumas legislações que se trata do tema exposto. Já o segundo capítulo examina o que é a LGPD e algumas terminologias usadas na Lei para adentrar-se em sua aplicação. Em seguida abordar-se-á os princípios e objetivos da referida Lei e, por fim, a pesquisa apresenta a temática Agência Nacional De Proteção De Dados (ANPD) e as sanções aplicáveis no ordenamento jurídico brasileiro. Posteriormente, buscou-se compreender a necessidade do consentimento do titular e o limite da utilização dos dados, destacando, ainda, a responsabilidade civil dos agentes de tratamento.

**Palavras-chave:** Privacidade. LGPD. Lei 13.709/2018. Proteção de Dados Pessoais.

## SUMÁRIO

<b>INTRODUÇÃO .....</b>	<b>01</b>
<b>CAPÍTULO I – DIREITO À PRIVACIDADE .....</b>	<b>03</b>
1.1 História do direito à privacidade.....	03
1.2 Era da informação .....	06
1.3 Proteção de dados como um direito fundamental .....	10
<b>CAPÍTULO II – LEI GERAL DE PROTEÇÃO DE DADOS.....</b>	<b>14</b>
2.1 Aplicação da LGPD .....	14
2.2 Princípios e objetivos .....	22
2.3 ANPD e as sanções aplicáveis.....	24
<b>CAPÍTULO III – CONSENTIMENTO DO TITULAR E A RESPONSABILIZAÇÃO DOS AGENTES DE TRATAMENTO.....</b>	<b>27</b>
3.1 Relação do ato de consentir com a LGPD .....	27
3.2 Consenso dentro da lei.....	29
3.3 Responsabilidade civil na Lei Geral de Proteção de Dados .....	33
<b>CONCLUSÃO .....</b>	<b>38</b>
<b>REFERÊNCIAS.....</b>	<b>40</b>

## INTRODUÇÃO

O presente trabalho tem por objetivo principal realizar uma análise legal, doutrinária e jurisprudencial no que se refere à proteção do tratamento de dados, os quais foram inseridos recentemente no ordenamento jurídico pátrio com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD). A monografia foi sistematizada, didaticamente, em três partes.

O primeiro capítulo versa sobre as raízes da Lei 13.709/2018- LGPD, inspirada na *General Data Protection Regulation* (GDPR), da União Europeia, que entrou em vigor no Brasil, estabelecendo novas regras tanto para pessoas jurídicas de direito privado, quanto para as de direito público, referentes a proteção da privacidade e segurança dos dados pessoais de usuários e clientes.

Antes da promulgação da referida lei, já havia fundamentos normativos como o direito à privacidade e a intimidade, consagrado no artigo 5º, X da Constituição Federal, surgindo a partir da Declaração Universal dos Direitos Humanos de 1948, como direito humano fundamental, juntamente com o artigo 21 do Código Civil, ressaltando que vida privada da pessoa natural é inviolável, e o Marco Civil da Internet (lei nº 12.965/2014) que tem por objetivo central disciplinar a relação entre empresas operadoras de produtos ou serviços associados à internet e os seus respectivos usuários dentro do território nacional.

Neste contexto, é importante salientar que, apesar de o direito à privacidade e a intimidade estarem descritos na Constituição Federal, não existia um inciso que abordasse especificamente a proteção de dados pessoais, sendo aprovado recentemente no dia 10 de março de 2022 a Emenda Constitucional 115, que incluiu



a proteção de dados pessoais entre os direitos e garantias fundamentais. O referido texto se encontra descrito no artigo 5º, LXXIX da Magna Carta.

No segundo capítulo, é apresentada a Lei Geral de Proteção de Dados (LGPD), com enfoque em sua aplicação, sendo conceituados os requisitos mínimos constantes no contrato para que o titular saiba com clareza os termos, condições e finalidades da captação dos dados. Além dos requisitos legais para a colheita dos dados, analisa-se quais as responsabilidades dos sujeitos envolvidos durante o tratamento e até que ponto são culpados por eventuais danos causados à terceiros.

Já no terceiro capítulo, tratar-se-á do ato de consentir do titular, ao proceder a autorização para os agentes utilizarem os dados pessoais, sendo o consenso de suma importância e o que irá acarrear o tratamento dos dados, devendo o agente informar de forma clara e objetiva o motivo da coleta. Nesse contexto, o não cumprimento das normas

O presente trabalho busca entender os aspectos gerais e legais que permite a LGPD assegurar os direitos dos titulares de dados em um cenário de proteção de dados. A aplicação do Regulamento já é uma realidade e os exemplos extraídos das diversas autoridades nacionais dos países membros da União europeia representam um caminho possível de interpretação das lides que serão geradas na aplicação da LGPD.

## CAPÍTULO I – DIREITO À PRIVACIDADE

O presente capítulo se propõe a examinar, exibir e levantar questões relacionadas ao direito à privacidade em e seus aspectos históricos, assim como a atual era da informação e, por fim o direito a proteção de dados como um direito fundamental e sua regulamentação na Constituição Federal Brasileira.

### 1.1 História

Vive-se atualmente uma revolução nas tecnologias de informação e comunicação com o advento da globalização. As informações pessoais sempre foram objeto de interesse por parte do Poder Público e dos particulares, com o objetivo de adquirir tais informações para posterior exploração, a partir de coleta, que poderá ter diversas finalidades.

Essas informações coletadas são cercadas de mecanismos de armazenamento do conteúdo produzido ou fornecido, denominado Banco de Dados, que pode ser definido como “uma coleção de dados inter-relacionados, representando informações sobre um domínio específico” (KORTH; SILBERSCHATZ, 1994).

Dessa maneira, o direito à privacidade tem tomado proporções e relevância nos debates atuais e nesse sentido, com o acesso significativo da sociedade a *internet* e a polarização dos Bancos de Dados, inúmeras atividades manuais cotidianas passaram a ser realizadas por meio da tecnologia, facilitando a coleta, a produção e o tratamento de informações de forma *online*. Como consequência, o direito, no decorrer dos anos tem se adequadado a uma nova forma de organização social e suas

exigências a fim de proteger o referido direito da personalidade e privacidade, enquadrado como direito fundamental humano.

A privacidade, como direito fundamental, passou por mudanças, desde o tradicional conceito elaborado por Warren e Brandeis com a publicação do artigo jurídico “*The right to privacy*”, em 15 de dezembro 1890, onde os autores buscavam reforçar a ideia de necessidade de proteção da vida íntima e da vida privada do ser humano, espaços nos quais cada um pode agir e expressar-se da forma como lhe aprouver, livre do olhar dos outros, até a concepção atual, caracterizada pela liberdade de autodeterminação informativa, isto é, a capacidade do titular em controlar suas informações pessoais.

A expressão “privacidade” (*privacy*) pode ser definida como o direito de estar só ou, ou talvez mais precisamente o “direito de ser deixado só” (“*right to be let alone*”). Dessa forma, a concepção de privacidade deve ser interpretada como sendo o “direito de ser deixado só”, que remete a interferência mínima estatal na vida do indivíduo. Todavia, deve-se entender a privacidade não apenas como a não interferência do Estado na vida do indivíduo, mas também como o poder de se reivindicar ao Estado a tutela dessa privacidade, protegendo o indivíduo de terceiros.

A partir do século XX, atrelados a outros fatores ao longo da história, surgiram diversos documentos solenes que declararam o direito à privacidade. Desta forma, em abril de 1948 foi editada a Declaração Americana dos Direitos e Deveres do Homem, aprovada na IX Conferência Internacional Americana, que em seu artigo V, prevê que “toda pessoa tem direito a proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar”.

Já em 10 de dezembro de 1948, foi proclamada pela Assembleia Geral das Nações Unidas a Declaração Universal dos Direitos do Homem (atualmente denominada como Declaração Universal dos Direitos Humanos), na qual, em seu artigo 12, dispõe sobre a privacidade como direito fundamental humano:

Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à

sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei. (FRANÇA,1948)

Alguns anos depois, em 1950, foi criada uma disposição parecida ao do citado dispositivo da DUDH, denominada como Convenção Europeia dos Direitos do Homem, que traz em seu artigo 8º o direito ao respeito pela vida familiar e privada, bem como guarida ao domicílio e correspondência e limitações ao Poder Público, nos seguintes termos:

1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros. (FRANCE,1950)

Além dos documentos anteriormente citados, outros foram criados pela comunidade internacional acerca da privacidade. Importante destacar que alguns países já tinham suas legislações sobre proteção de dados, como era o caso da Alemanha (*Bundesdatenschutzgesetz* de 21 de janeiro de 1977 e posteriores alterações), da Espanha (*Ley Orgánica* de 29 de outubro de 1992) e da França (*Loi Informatique et Libertés* Lei 17, de 6 de janeiro de 1978), que posteriormente promoveram a transposição da Diretiva UE 46/1995 para os seus respectivos ordenamentos. Em 2018 surge o Regulamento Geral de Proteção de Dados (GDPR) assume o lugar dessa diretiva, sendo diretamente aplicada a todos os países-membros da União Europeia.

Sob o recorte brasileiro, a Constituição Federal de 1988 prevê em seu artigo 5º, inciso X que “são invioláveis a intimidade, a vida privada a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. No mesmo dispositivo, ainda relação a privacidade, fala-se também, em sigilo (de correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas) e na inviolabilidade da casa.

Com base no texto constitucional, necessário especificar o que é privacidade e intimidade.

José Afonso da Silva mostra que o conceito de intimidade é geralmente empregado para designar a esfera secreta da vida do indivíduo, que busca evitar o conhecimento dos demais, como, por exemplo, suas relações sexuais. Já o conceito de privacidade engloba informações restritas da vida do indivíduo, como sua relação com familiares e amigos, o que o autor chama de vida interior, que envolve atividades que geralmente não são tornadas públicas, não devendo ser objeto de divulgações por terceiros.

Fato é que, no Brasil, previsto tanto na Constituição quanto na legislação Infraconstitucional, como no Código Civil de 2002 (Lei Federal n.º 10.406, de 10 de janeiro de 2002) o direito à privacidade é considerado direito fundamental e direito da personalidade, sendo uma figura jurídica que supera a dicotomia entre direito público e privado.

Ainda no âmbito nacional, existem também o Código do Consumidor, a Lei de Acesso à Informação e, em especial, o Marco Civil da Internet (Lei nº 12.965) que regulamenta o uso da *internet* no Brasil e estabelece princípios, garantias, direitos e deveres, bem como, determina diretrizes para a atuação dos entes federativos no país em relação à matéria.

Entretanto, os legisladores brasileiros sentiram a necessidade de preenchimento de algumas lacunas existentes na proteção dos usuários no ambiente tecnológico e informatizado, especialmente, na definição objetiva de padrões e normatizações acerca do assunto, dessa maneira, criaram então a Lei Geral de Proteção de Dados (LGPD).

## **1.2A era da informação**

Nos dias atuais, são indiscutíveis as facilidades surgidas e aperfeiçoadas por meio da “Era da Informação”, estamos constantemente nos expondo e a nossos dados pessoais, nossa vida, o que comemos, com quem estamos aonde vamos, e o

que estamos fazendo em todas as horas. A exemplo, o uso celulares, “*notebooks*”, “*tabletes*” e outros “*hardwares*” e a agilidade trazida com a utilização desses bens, bem como a fluidez com que os dados se dissipam em larga escala.

Nesse mesmo sentido, há uma dupla perspectiva no que se refere à multiplicidade de instrumentos tecnológicos e suas utilizações: a primeira se refere aos anseios por notícias e, portanto, vive-se em uma era de variados meios de comunicação, bem como, viabiliza-se a formação do conhecimento, razão pela qual a tecnologia minimiza as barreiras temporais e espaciais, colaborando para que o conteúdo chegue de modo imediato e expansivo aos usuários.

Em contrapartida, na segunda perspectiva, é notável o grande volume de informações a que se têm acesso pelas mídias, “*smartphones*”, *internet*, televisão, redes sociais, o que, muitas vezes, não permite análises críticas e aprofundadas de seu teor, sendo comum, por exemplo, a divulgação de “*fakenews*”, notícias falsas, em tradução livre.

A revolução tecnológica proporcionou não somente a facilidade na coleta e tratamento de dados, mas sim, a sua essencialidade em todos os ramos, se tornando a principal ferramenta estratégica das organizações, seja para fins comerciais e empresariais, como para fins educacionais e de pesquisa. Por certo, os avanços e modificaram as relações sociais e organizacionais, embora muitas pessoas ainda não tenham acesso aos benefícios da tecnologia.

Do mesmo modo, houve uma polarização de ferramentas tecnológicas para diversas finalidades, em destaque as ferramentas para gerir o armazenamento de dados e o uso de informações pessoais:

A disseminação do uso de computadores fez com que, nos dias atuais, não somente as agências governamentais que tradicionalmente coletavam dados pessoais, a exemplo dos Correios, os Departamentos de Trânsito e as repartições do Fisco, funcionassem como poderosos centros de processamento de informações pessoais, mas também todas as empresas privadas hoje adquiriram os meios para coletar, manipular, armazenar e transmitir dados de uma forma simples e a um custo relativamente baixo. (REINALDO, 2002).

Incluídos nesse processo, os usuários dessas tecnologias muitas vezes inserem dados pessoais, entendidos estes como sendo “qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, incluindo todo o endereço ou número de identificação de um terminal utilizado para conexão a uma rede de computadores”, conforme o Anteprojeto de Lei de Proteção de Dados Pessoais (BRASIL, 2018),

Ao vislumbrar este cenário e tratando da circunstância atual vivenciada pelos titulares de dados, deve-se atentar para o fato de que:

A utilização das novas tecnologias expande as possibilidades de recolha, tratamento e circulação de informação, virtualmente sem limites de tempo e de espaço. Confrontam-se, aqui, por um lado, o interesse do indivíduo na proteção das informações que lhe dizem respeito e, por outro, o interesse de entidades públicas ou privadas na eficiência das suas atividades. A informatização empola o grau de risco para o indivíduo na medida em que a interconexão de ficheiros e de bases de dados permite reunir informação diversa que poderá ser utilizada de modo abusivo, seja pelos poderes públicos, com intuídos repressivos, restritivos da liberdade dos cidadãos, seja por entidades privadas com fins discriminatórios (por exemplo, no recrutamento para determinados empregos) ou de mero enriquecimento (caso da venda de listas de nomes para fins de mala direta). Estas práticas podem funcionar, indiretamente, como condicionantes do próprio comportamento individual. (GONÇALVES, 2003)

Atualmente, devido a pandemia do Covid-19, intensificou-se ainda mais o uso de tecnologias da informação para atender as demandas do momento em que se vive, provocando a quase total virtualização das relações sociais e, multiplicando o número de serviços *onlines* para atender a demanda dessa evolução. Esse novo mundo, fez com que as pessoas a criassem dezenas, às vezes centenas, de credenciais pessoais de acesso. Em muitos casos, sem a devida atenção e orientação, muitas pessoas forneceram dados sem saber em que seriam utilizados, cometendo muitas vezes, atos de fragilização do nível de segurança.

É notável que as empresas acompanharam a necessidade de atender a demanda tecnológica, atualizando suas ferramentas, neste sentido vale destacar que:

A capacidade de tratamento de dados pessoais das mais diversas ordens vem aumentando exponencialmente, principalmente devido ao advento de tecnologias avançadas de inteligência artificial,

com o uso de algoritmos sofisticados e com a possibilidade de aprendizado por máquinas (*machine learning*). Significa dizer que o tratamento de “big data” literalmente, grandes bases de dados por meio de técnicas computacionais cada vez mais desenvolvidas pode levar a análises probabilísticas e resultados que, ao mesmo tempo que atingem os interesses de uma parcela específica da população, retiram a capacidade de autonomia do indivíduo e o seu direito de acesso ao consumo de bens e serviços e a determinadas políticas públicas, por exemplo (MULHOLLAND,2018).

As informações disponibilizadas por internautas na presente realidade da sociedade informacional, de certa forma, são extremamente valorizadas no mercado virtual, pois acabou se tornando necessário a regulação legal, para não serem tratadas como insumo do lucrativo mercado de dados na *internet*, que enaltece o potencial econômico da perda de privacidade.

Logo, além da órbita do mercado capitalista, os dados pessoais também são utilizados para fins políticos, como deriva do escândalo da *Cambridge Analytica*, elucidado na matéria “Entenda o escândalo de uso político de dados que derrubou valor do *Facebook* e o colocou na mira de autoridades” da BBC News publicada em 20 de março de 2018, empresa que materializou a coleta de dados pessoais por meio do gigante *Facebook*, para colaborar na eleição presidencial dos Estados Unidos em 2016.

Do exposto, nota-se que o comércio de dados pessoais dos usuários realizado entre os gigantes do mercado, como exemplo *Facebook*, *Instagram*, e *Twitter*, é um dos principais motivos que causam insegurança e temor aos usuários da *internet*.

Nessa situação, com os dados das pessoas transitando o tempo todo, os anúncios publicitários têm uma ampla vantagem ao poder direcionar seus produtos para determinados consumidores. Pode-se verificar, como exemplo, que os celulares detectam e enviam a localização física de seus donos, dando permissão para que a propaganda, de forma célere, chegue ao seu destino.

Apesar de todas as facilidades proporcionadas pela tecnologia e a atual era da informação, é notável a violação de dados pessoais, que por muitas vezes não



recebem o devido tratamento. A utilização ampla e não consentida por terceiros de informações pessoais, podem lesar o direito à privacidade, pois sem o seu consentimento, esses dados podem ter uma finalidade diferente da informada.

### **1.3A proteção de dados como um direito fundamental**

Inicialmente cabe explicar que um direito fundamental consiste em direitos protetivos, que garantem o necessário para proteger poderes e esferas de liberdade das pessoas dentro de uma sociedade administrada pelo Poder Estatal.

Os direitos fundamentais, dessa forma, decorrem de uma construção histórica e possuem como características, serem irrenunciáveis, ou seja, significa a não possibilidade de renúncia de tais garantias pelo seu titular, também são inalienáveis e invioláveis. Isto é, não podem ser transferidas a outrem. Além disso, são imprescritíveis. Ou seja, não se perdem com o tempo, vez que são sempre exercíveis e exercidos, não sendo perdidos pela falta de uso. Do mesmo modo são universais, significa que os direitos fundamentais são destinados, de modo indiscriminado, a todos os seres humanos.

Não obstante, diz que são concorrentes, pois podem incidir em concomitância a outros direitos fundamentais, e complementares, sendo necessário interpreta-los de forma conjunta com todos os outros direitos. Por fim, limitados, segundo a doutrina de Paulo Gustavo Gonet Branco, nenhum direito fundamental poderá ser considerado absoluto, sendo que tais direitos deverão ser interpretados e aplicados levando-se em consideração os limites fáticos e jurídicos existentes, sendo que referidos limites são impostos pelos outros direitos fundamentais.

Ao que se refere o direito à privacidade, a Constituição Federal de 1988, em seu artigo 5º, inciso X, traz explicitamente que são invioláveis a honra, a intimidade, a vida privada e a imagem das pessoas, assegurando ainda o direito à indenização por eventual dano sofrido, seja material ou moral. Observa-se que, este pertence ao gênero denominado como direito humano fundamental, onde o legislador

constituente, com base no entendimento da comunidade internacional, efetivou a proteção ao referido direito.

Importante salientar que, a proteção de dados pessoais, por sua vez, é uma evolução do direito à privacidade, sendo este um dos fundamentos que disciplinam a proteção dos dados pessoais, ou resumidamente, a privacidade está relacionada ao direito ao sigilo e, a proteção de dados se refere ao anteparo que a manipulação de dados pode provocar se forem usados de forma errônea.

Fazendo uma breve leitura do artigo 5º, inciso X da Constituição Federal, é possível notar que a garantia constitucional elencada se baseia somente ao termo privacidade, não abrangendo a complexidade do fenômeno, proteção de dados. Há uma desarmonia que separa a tutela da privacidade, constitucionalmente positivada, da tutela das informações pessoais, ou dos dados pessoais em si, que necessita de uma proteção mais direta para norteamento de outras leis.

Ainda na mesma perspectiva, é necessário explicar a diferenciação entre dado pessoal e informação pessoal que, de acordo com o art. 5º, inciso I, da Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709 de 2018, dado pessoal é a *“informação relacionada à pessoa natural identificada ou identificável”*. Já a Lei de Acesso à Informação (LAI) – Lei nº 12.527, de 2011, conceitua informação como *“dados, processados, ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato”*, e informação pessoal como *“aquela relacionada à pessoa natural identificada ou identificável”* art. 4º, incisos I e IV, respectivamente.

Assim, o “dado” apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécie de “pré-informação”, anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Mesmo sem aludir ao seu significado, na informação, já se pressupõe a depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza. (DONEDA, 2011)

Com relação ao uso e a proteção da privacidade dos dados pessoais, conforme já mencionado anteriormente, esse é um direito cada vez mais em pauta pelos cidadãos e, recentemente, o Senado aprovou no dia 20 de outubro de 2021, a Proposta de Emenda à Constituição (PEC) 17/2019, que torna a proteção de dados pessoais, inclusive em meios digitais, um direito fundamental garantido constitucionalmente a todo cidadão brasileiro.(SENADO NOTÍCIAS, 2021)

Dessa maneira, com a promulgação da PEC, não será mais permitido que novas leis sejam criadas com entendimento contrário à privacidade de dados em nenhum âmbito, sendo mais uma garantia ao cidadão de que seus dados pessoais não sejam violados.

Tratando sobre o tema, dados pessoais e direito fundamental, é notável que o Brasil está caminhando para entrar em compasso com a legislações de outros países:

Assim, no ano em que a Carta Constitucional brasileira completa vinte e cinco anos mostra-se oportuno e necessário trazer à discussão a ampliação do rol de direitos fundamentais, de modo a abarcar aqueles decorrentes do intenso desenvolvimento tecnológico experimentados nos últimos anos, notadamente na área da informação e comunicação. Essa reflexão não pode mais ser postergada, sobretudo porque o tratamento de dados pessoais na Internet oferece uma série de riscos ao seu titular, com claro potencial para fomentar discriminações e preconceitos de origem, raça, sexo, cor, idade, o que por certo viola a dignidade humana. O reconhecimento de novas categorias de direitos fundamentais, como os dados pessoais e a autodeterminação informativa, revela-se medida necessária não só para a concretização dos objetivos da República Federativa do Brasil, elencados no art. 3º da Carta Magna, como também para o alinhamento jurídico do país aos demais Estados que já adotaram igual postura em favor da dignidade da pessoa, a exemplo da União Europeia. Com efeito, enquanto a discussão sobre o tema é ainda incipiente no Brasil, a União Europeia se preocupa com a tutela desse direito desde 1995, momento em que os Estados integrantes perceberam a necessidade de garantir um adequado grau de proteção aos dados pessoais dos usuários das novas tecnologias, tratando-os como direitos fundamentais. (SILVA E SILVA, 2013)

Inserir esse direito na Constituição Federal significa dar a devida importância a inviolabilidade dos dados pessoais, tanto na esfera virtual dos cidadãos brasileiros, quanto na sua esfera íntima na realidade. Portanto, é considerada que a

proteção de dados pessoais é essencial aos cidadãos e deve ser levada em conta em conjunto com os demais preceitos fundamentais do nosso ordenamento jurídico brasileiro.

A doutrina brasileira sempre defendeu a necessidade de se reconhecer a proteção de dados pessoais como um direito fundamental autônomo, indo além da tutela da intimidade e da privacidade, por existirem leis esparsas que não adentravam aos conceitos de “dados pessoais”.

O tratamento autônomo da proteção de dados pessoais é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos e é caso emblemático de uma tendência que, a princípio, parecia apenas destinada a mudar determinado patamar tecnológico e a solicitar previsões pontuais no ordenamento, mas que, em seus desdobramentos, veio a formar as bases para o que vem sendo tratado, hoje, como um direito fundamental à proteção de dados. (DONEDA, 2011)

Neste sentido, pode-se afirmar que a proteção de dados pessoais garantida pela LGPD ganhou um reforço a mais, pois este pertencia a um meio genérico e, após a constitucionalização da proteção de dados se tornou um direito fundamental de status positivo, ou seja, é uma proteção prestada pelo Estado, pois o é este quem tem o dever de criar políticas e estabelecer órgãos públicos para garantir a proteção dos dados pessoais no Brasil e editar uma legislação asseguradora do referido direito, que é o caso da citada lei.

## **CAPÍTULO II – LEI GERAL DE PROTEÇÃO DE DADOS**

Inicialmente o presente capítulo irá conceituar o que é LGPD e algumas terminologias usadas na Lei para adentrarmos em sua aplicação. Em seguida aborda dar-se-á os princípios e objetivos da referida Lei e, por fim, a pesquisa apresenta a temática Agência Nacional De Proteção De Dados (ANPD) e as sanções aplicáveis no ordenamento jurídico brasileiro.

### **2.1 Aplicação da LGPD**

Inspirada pelo Regulamento Europeu de Proteção de Dados Pessoais, chamado de General Data Protection Regulation - GDPR, a Lei nº 13.709/2018. Também conhecida como Lei Geral de Proteção de Dados – LGPD, promulgada no dia 14 de agosto de 2018, foi criada para colocar limites na forma com que os dados e as informações são tratados, dando aos seus titulares a ciência de quais dados estão sendo utilizados, porque, para que e até quando serão utilizados.

Rememorando, a LGPD, propõe uma maneira eficaz de proteger os dados pessoais dos indivíduos tanto pela iniciativa privada quanto pelo poder público e, conforme já demonstrado no capítulo anterior, à proteção de dados pessoais, tem sua origem a partir do direito à privacidade, como produto de uma sociedade da informação. Dessa maneira, com a utilização em massa da *internet*, surgem os bancos de dados, que contém informações pessoais e quem os possui tem o controle desse poder.

A LGPD vinha sendo desenvolvida desde 2010 e insere o Brasil entre os países que têm legislações completas sobre proteção de dados. Seu texto, em cumprimento aos princípios estabelecidos pela Constituição Federal Brasileira de 1988, em consonância com o Código Civil, e em atualização e complemento ao Marco Civil da *Internet*, tem uma legislação mais abrangente em relação utilização de dados mais atuais. Denota a importância dada ao consentimento, tendo em vista que o instituto é apresentado diversas vezes ao longo do texto, além de ser agora adjetivado como “livre”, “informado” e “inequívoco” e servir como orientação para várias outras normas apresentadas pela legislação. (LUGATI; ALMEIDA, 2020, p. 02)

O artigo 1º bem como alguns aspectos inseridos no artigo 2º da Lei Geral de Proteção de Dados esclarecem e afirmam o compromisso desta legislação com os princípios constitucionais da dignidade, privacidade, intimidade, honra e outros direitos personalíssimos, e, não obstante, resume seus objetivos principais.

Art. 1º. Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, tendo como um de seus objetivos proteger os direitos fundamentais da liberdade e de privacidade previstos constitucionalmente, bem como o livre desenvolvimento da personalidade natural.

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.

(BRASIL,2018, *online*)

Conforme o exposto, os fundamentos da LGDP estão relacionados com o texto presente na Constituição Federal de 1988, sendo eles: artigo 5º, X, que considera invioláveis a vida privada e a intimidade, e o XII, que se refere a interceptação de comunicações telefônicas, telegráficas ou de dados, assim como o *Habeas Data*, descrito no inciso LXXII, sendo um remédio constitucional, que tem como finalidade a garantia dos direitos fundamentais de informação, privacidade e

intimidade do indivíduo, possibilitando o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados.

José Alfonso da Silva, esclarece em sua doutrina que:

[...] um remédio constitucional que tem por objetivo proteger a esfera íntima dos indivíduos contra: (a) usos abusivos de registros de dados pessoais coletados por meios fraudulentos, desleais ou ilícitos; (b) introdução nesses registros de dados sensíveis (assim chamados os de origem racial, opinião política, filosófica ou religiosa, filiação partidária e sindical, orientação sexual, etc.); (c) conservação de dados falsos ou com fins diversos dos autorizados em Lei. (2005, p.453).

Dessa forma, é importante evidenciar que, a LGPD tem como base a proteção e a garantia à privacidade, liberdade, segurança, justiça das pessoas, bem como a evolução econômica e social, assegurando assim, uma base legal para a tutela jurídica que envolve a proteção de dados.

Neste contexto, para o melhor entendimento da Lei Geral de Proteção de Dados, é necessário destacar o que diz respeito à conceituação de algumas expressões utilizadas na referida Lei, quais sejam: pessoa natural, pessoa jurídica, dados pessoais, titular dos dados, tratamento dos dados, dados pessoais sensíveis, consentimento, banco de dados, controlador e operador.

De forma breve e objetiva conceitua-se com a seguinte abordagem:

Em primeiro momento, é importante explicar que, a pessoa natural é sinônimo de pessoa física, é o ser humano considerado como sujeito de direitos e obrigações. Esse conceito se relaciona com o caput do artigo 1º do Código Civil, que estabelece que, pessoa natural é o ser humano capaz de direitos e obrigações na esfera civil;

No que concerne pessoa jurídica, é oportuno citar o esclarecimento de Maria Helena Diniz: “[...] a pessoa jurídica é a unidade de pessoas naturais ou de

patrimônios, que visa à consecução de certos fins, reconhecida pela ordem jurídica como sujeito de direitos e obrigações. ” (2012, p.264)

Geralmente, a pessoa jurídica possui aptidão para ser titular de direitos e obrigações e atuar na vida jurídica, com personalidade distinta dos indivíduos que fazem parte dela. Pode ser constituída por um grupo de pessoas, a quem a lei confere personalidade jurídica para atuar na ordem civil, tendo direitos e obrigações, como uma pessoa natural.

Já os dados pessoais referem-se a qualquer informação relacionada a uma pessoa natural, seja recém-nascido, criança, adolescente, idoso, absolutamente incapaz, relativamente incapaz, ou seja, todo ser humano nascido com vida. Nesse sentido, o titular dos dados é a quem pertence os dados pessoais que são objeto de tratamento. (BRASIL,2018)

Como se observa, considera-se titular de dados, uma pessoa singular identificável que possa ser identificada, direta ou indiretamente, por meio de um identificador. Pode-se dizer também que o titular exerce uma soberania de qualquer assunto relacionado ao tratamento de suas informações, tendo a capacidade de consentir, ou não, com o tratamento.

O tratamento dos dados é toda e qualquer operação realizada com dados pessoais, como, por exemplo ressalta a LGPD: coleta, recepção, produção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL,2018)

Este é um ponto importante porque esclarece o comportamento da lei que estabelece as regras para o uso de informações pessoais. Em poucas palavras, o tratamento de dados é toda operação realizada sobre dados pessoais, começando com o processo de coleta, e depois o armazenamento, uso e descarte eficiente da informação. A LGPD menciona explicitamente uma série de ações classificadas como tratamento de dados.



Os dados pessoais sensíveis são os dados que podem se relacionar a uma pessoa natural, com algum tipo de associação, movimento, sindicato, partido político ou até mesmo questões de ordem étnica, religiosas, políticas, filosóficas, vida sexual, dentre outros fatores, estando incluídos também dados médicos, biométricos e genéticos. (BRASIL, 2018)

Ao tratar os dados pessoais sensíveis, é de suma importância haver uma cautela ainda maior, justamente por serem dados coletados sobre a vida íntima do titular. Dessa forma, interpreta-se que ao tratar dados sensíveis existe uma necessidade de se ater ao princípio da privacidade.

O consentimento é a manifestação livre, informada e inequívoca pela qual o titular aceita o tratamento dos seus dados pessoais para uma finalidade determinada, podendo ser compreendido como um poder conferido à pessoa de modificar sua própria utilização de dados, com base na sua manifestação de vontade. Sua utilização gera um paradigma para a tutela dos dados pessoais, devendo ser observado antes e depois a concreta aplicação do que foi repassado, gerando o efeito de consentir no titular, para a utilização de seus dados. (BRASIL, 2018)

O banco de dados é o conjunto de informações pessoais estabelecido em um ou em vários locais. No sentido técnico do assunto, esses bancos são coleções de informações do mundo real armazenadas em um ambiente virtual. A estrutura geralmente é baseada em linhas e colunas para que todos os dados possam ser interpretados, organizados, gerenciados, modificados e atualizados. (BRASIL, 2018)

O Controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, tais como as finalidades e os meios do tratamento (art. 5º, VI). No âmbito da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados. (GOV., 2020)

O Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII), aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere. (GUIA LGPD,2020)

É importante salientar, conforme já mencionado anteriormente, que a LGPD é aplicável a todos que realizem o tratamento de dados pessoais, sejam elas pessoas de direito público ou privado, pessoa física ou jurídica, desde que estejam realizando qualquer tipo de operação que se enquadre em tratamento de dados pessoais.

A identificação dos Controladores depende necessariamente, em cada situação, da existência e capacidade de decidir sobre os meios e a finalidade do tratamento de dados. Assim, serão considerados controladores, por exemplo, os órgãos públicos que contratarem empresa privada para gerir seu registro de visitantes, na medida em que tal empresa agirá sob as ordens do órgão contratante.

Nessa ilustração, o órgão contratante (Controlador) não apenas estabelecerá a finalidade do tratamento, mas também exigirá da empresa contratada (Operador) a adoção dos meios técnicos necessários para garantir a observância dos princípios que regem o tratamento dos dados pessoais, especificados no art. 6º da LGPD. Para distinguir entre Controlador e Operador, portanto, é fundamental reconhecer qual ente possui autonomia decisória quanto a fins e meios de tratamento (Controlador), e qual possui escopo eminentemente executório (Operador), submetido aos desígnios de outrem. (GOV.BR, 2020, p.10)

Toda essa movimentação de tratamento de dados que envolve os agentes e os titulares, acontece por meio de ações, que podem ser denominadas também como, operação. No que tange ao exposto, se faz necessário conceituar a seguir, os termos que fazem parte das operações de tratamento.

O acesso é ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique. O armazenamento é a ação ou resultado de manter ou conservar em repositório um dado, e se difere do arquivamento que, consiste no ato ou efeito de manter registrado um dado em qualquer das fases do ciclo da informação, compreendendo os arquivos corrente, intermediário e permanente, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência.

A avaliação é o ato de analisar o dado com o objetivo de produzir informação, ponderando os riscos que podem ser advindos desta produção. Com a realização da avaliação de riscos, a empresa deve garantir que sejam implementados níveis apropriados de medidas técnicas e organizacionais para proteção dos dados pessoais e evitar que riscos ocorram.

Já a classificação é maneira de ordenar os dados conforme algum critério estabelecido, faz parte da organização. A coleta é recolhimento de dados com finalidade específica, ocorrendo após a comunicação, que é o ato de transmitir informações pertinentes a políticas de ação sobre os dados. O controle é ação ou poder de regular, determinar ou monitorar as ações sobre o dado. Essa ação pode ocorrer tanto por parte do titular, quanto por parte da ANPD.

A difusão é ato ou efeito de divulgação, propagação, multiplicação dos dados, e a distribuição, é o ato ou efeito de dispor de dados de acordo com algum critério estabelecido, desde que seja informado ao titular para posterior autorização livre e consentida.

A eliminação corresponde ao ato ou efeito de excluir ou destruir dado do repositório e, a extração é ato de copiar ou retirar dados do repositório em que se encontrava. A modificação é o ato ou efeito de alteração do dado. O processamento ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado. Já a produção criação de bens e de serviços a partir do tratamento de dados.

O ato de recepcionar consiste em receber os dados ao final da transmissão; A reprodução é a cópia de dado preexistente obtido por meio de qualquer processo; A transferência é a mudança de dados de uma área de armazenamento para outra, ou para terceiro, não podendo ser confundido com a transmissão que é movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.; e por fim, a utilização é o ato ou efeito do aproveitamento dos dados. (GOV.BR,2020, p.11, *online*)

Em princípio, o agente, antes de iniciar alguma atividade que envolva o tratamento de dados pessoais, deve certificar previamente que a operação esteja registrada de forma clara e explícita e os propósitos especificados e informados ao titular dos dados.

A lei traz garantias que o titular pode solicitar caso seus dados sejam deletados de um determinado servidor ou instituição, podendo ser transferidos para outro. Um bom exemplo é um usuário de uma determinada operadora telefônica que está insatisfeito com os serviços prestados. Ele pode a qualquer momento solicitar a portabilidade de seus dados para outra linha telefônica, como também solicitar que seus dados sejam deletados da primeira instituição citada.

Em contramão à aplicabilidade, a LGPD também possui algumas hipóteses quanto a inaplicabilidade da Lei, nos termos do artigo 4º a seguir:

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:  
I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;  
II - realizado para fins exclusivamente:  
a) jornalístico e artísticos; ou  
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;  
III - realizado para fins exclusivos de:  
a) segurança pública;  
b) defesa nacional;  
c) segurança do Estado; ou  
d) atividades de investigação e repressão de infrações penais; ou  
IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. (BRASIL, 2018, *online*)

Observa-se que a lei trouxe consigo uma certa limitação de aplicabilidade em relação a determinadas finalidades de coletas de dados que são regulados pela LGPD. Essas são as exceções que a LGPD prevê para sua própria aplicação, sendo importante lembrar que, nos demais casos, sempre que houver o tratamento de dados pessoais em território nacional, deverão ser aplicadas as disposições da Lei Geral de Proteção de Dados.

## 2.2 Princípios e objetivos

Visando a delimitação do tratamento de dados pessoais, para que os indivíduos obtenham o poder de controlar o fluxo de seus dados, a doutrina desenvolveu ao longo dos anos uma série de princípios norteadores da prática.

Seguindo esta premissa, é importante definir o que é princípio, utilizando a doutrina de Miguel Reale:

“Princípios são, pois verdades ou juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízos, ordenados em um sistema de conceitos relativos à dada porção da realidade. Às vezes também se denominam princípios certas proposições, que apesar de não serem evidentes ou resultantes de evidências, são assumidas como fundantes da validade de um sistema particular de conhecimentos, como seus pressupostos necessários”. (1986, p. 60, *online*)

É essencial a Lei utilizar-se de princípios como uma espécie de bússola, a qual deve nortear a aplicação das regras específicas previstas na LGPD. Dessa forma, a LGPD é baseada em dez princípios orientadores elencados no art.6º da referida Lei, no que se refere ao tratamento de dados pessoais:

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. (BRASIL, 2020, *online*).

A abordagem dos princípios constantes no artigo 6º, incisos I a X, da LGPD não exclui a existência de outros princípios no ordenamento jurídico brasileiro. A LGPD somente organizou os referidos princípios, já citados em leis esparsas, para dar uma ênfase maior a Lei.

Dessa forma, a limitação do uso de dados pessoais determinada pela legislação, respeita o princípio da dignidade da pessoa humana, que não está explícito na Lei, mas é mencionado como "dignidade" no inciso VII, do artigo 2º da LGPD, principalmente a proteção do direito à liberdade, a privacidade, a honra e a imagem pertencentes ao ser humano.

Assim, vale evidenciar que a privacidade desde a concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. A maneira de alcançar essa proteção é por meio de medidas seguras de privacidade baseadas na LGPD, com avisos apropriados e interfaces legíveis de fácil entendimento para o titular dos dados.

### 2.3 ANPD e as sanções aplicáveis

Em 9 de julho de 2019 foi sancionada a lei 13.853 que cria a Autoridade Nacional de Proteção de Dados (ANPD) tendo seu início efetivo em 05 de novembro de 2020. Entre as competências da ANPD estão: zelar pela proteção dos dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade e advertir, e caso de descumprimento da Lei, aplicar as sanções previstas em caso esta continue sendo descumprida.

Não obstante isso, um não após a criação da ANPD, foi aprovado pela Resolução CD 01/2021, no dia 29 de outubro de 2021, o regulamento do processo de fiscalização e processo administrativo sancionador pela ANPD (Autoridade Nacional de Proteção de Dados). O regulamento visa estabelecer procedimentos essenciais ao processo de fiscalização, que compreende as atividades de monitoramento, orientação e atuação preventiva, bem como as regras a serem observadas no âmbito do processo administrativo sancionador pela ANPD.

A ANPD possui natureza jurídica transitória, podendo ser transformada em autarquia vinculada à Presidência da República após dois anos, a critério do governo. O novo órgão tem a seguinte estrutura organizacional: Conselho Diretor, composto por cinco diretores; Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, composto por 23 representantes, incluindo membros da sociedade civil; Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidades administrativas necessárias à aplicação da lei. (BRASIL, 2018, *online*)

É importante ressaltar que a LGPD determina que o Controlador deverá comunicar tanto ao Titular quanto a ANPD sobre a ocorrência de algum incidente de segurança, que venha a resultar em um risco ao Titular. Assim, caberá ao Controlador implementar procedimentos ou práticas para gerir incidentes materializados e notificar brechas de segurança e vazamentos de dados. Essa comunicação será necessária nos casos em que dados pessoais tenham vazado acidental ou ilícitamente a destinatários não autorizados, que fiquem temporária ou permanentemente indisponíveis, ou ainda sejam alterados.

A notificação ao titular dos dados deve ocorrer sem demora injustificada, tendo a norma estipulado o prazo de 72 horas para a comunicação do ocorrido à Autoridade Nacional de Proteção de Dados. Vazamentos e acessos não autorizados a dados pessoais podem ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o Controlador estará sujeito à aplicação das penalidades da LGPD.

A LGPD prevê sanções para quem não tiver boas práticas que descritas no art. 52 da referida Lei, sendo elas:

- I - advertência, com indicação de prazo para adoção de medidas corretivas;
  - 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;
  - III - multa diária, observado o limite total a que se refere o inciso II;
  - IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
  - V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
  - VI - eliminação dos dados pessoais a que se refere a infração;
- (BRASIL, 2018, *online*)

A ANPD deve avaliar alguns parâmetros e critérios para a aplicação de sanções, sendo eles: a gravidade e a natureza das infrações e dos direitos pessoais afetados, a boa-fé do infrator, a vantagem auferida ou pretendida pelo infrator, a condição econômica do infrator; a reincidência, o grau do dano, a cooperação do infrator, a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, a adoção de política de boas práticas e governança, a pronta adoção de medidas corretivas, a proporcionalidade entre a gravidade da falta e a intensidade da sanção. (LGPD, 2018, *online*)

De toda forma, a aplicação de qualquer das penalidades pode ter impacto bastante negativo sobre a atividade que envolva a coleta de dados pessoais, principalmente no aspecto reputacional, sendo importante a empresas seguirem as regras de acordo com a Lei.



Conforme descrito nos típicos anteriores, o controlador é o responsável por indicar o operador, pessoa responsável pelo tratamento de dados pessoais. Além disso, o controlador deve informar claramente, de preferência em seu site, a identidade e os meios de contato do operador. Isso é necessário para que o titular possa entrar em contato com o operador, caso deseje. Após sua formação, a ANPD pode estabelecer outras atividades para o operador. Ao depender da organização, levando em consideração características como porte e volume do tratamento de dados, a Autoridade Nacional pode dispensar a necessidade desse profissional. (LARA,2021)

Logo, a ANPD promove a adoção de padrões técnicos mínimos para facilitar o controle de dados por parte dos próprios titulares. Assim, a Autoridade cumpre seu papel de não apenas aplicar a LGPD, mas também de conscientizar a população sobre os temas da lei.

## **CAPÍTULO III – CONSENTIMENTO DO TITULAR E A RESPONSABILIZAÇÃO DOS AGENTES DE TRATAMENTO**

O presente capítulo propõe exibir, examinar e levantar questões relacionadas ao consentimento do titular, abordando a forma com que a LGPD guia o titular e os limites do consentimento, bem como a responsabilização civil do agente de tratamento, caso não siga a diretrizes da referida lei.

### **3.1 A relação do ato de consentir com a LGPD**

A Lei Geral de Proteção de Dados – LGPD, visa preservar a privacidade dos usuários, estabelecendo regras e limites para a coleta, tratamento, armazenamento e compartilhamento de dados, para proteger os direitos fundamentais de liberdade e privacidade, enfatizando de início como requisito principal, o consentimento, sendo a primeira hipótese autorizativa do tratamento de dados pessoais.

Em vista disso, percebe-se que mesmo antes de entrar no capítulo sobre os Direitos do Titular, a lei menciona várias vezes que o consentimento é um elemento essencial para a realização do tratamento de dados. Os titulares têm o direito de solicitar que seus dados pessoais sejam processados apenas conforme autorizado por eles e, para efetivar esse direito, a LGPD estipula que o consentimento não deve ser ocultado ou disfarçado. O titular dos dados precisa estar plenamente ciente de que cabe a ele, em primeiro lugar, decidir se deve ou não processar os dados e as consequências de sua aceitação ou rejeição.

Nesse sentido, é válido adentrar na origem do termo consentimento, que historicamente, no direito privado brasileiro, a figura do consentimento sempre esteve atrelada no tema dos defeitos do negócio jurídico. Do erro à lesão, o bem jurídico tutelado é justamente assegurar que a declaração de vontade da pessoa seja livre e consciente. A expressão do ato de consentir de forma imperfeita é considerada como vício do consentimento sendo o negócio jurídico decorrente anulável. (BIONI, 2021, p. 183)

É importante observar que o consentimento estipulado na LGPD deve ser livre e espontâneo, sob pena de constituir vício de vontade, podendo torná-lo nulo. Nesse sentido, ressalta-se que existem diferenças significativas na forma como o Código Civil e a LGPD tratam os negócios jurídicos defeituosos, que devem ser foco dos agentes de processamento de dados. De fato, enquanto para o Código Civil as manifestações afetadas por vício de consentimento são geralmente anuláveis, na LGPD a mesma manifestação constitui hipótese de nulidade.

O consentimento é um requisito essencial para a formação de um negócio, nele é possível perceber o concurso da vontade, que é um elemento que atribui a voluntariedade e a liberdade, é importante ressaltar que o consenso se compreende na existência de duas vontades que tendem para um mesmo objetivo. Corresponde à anuência do manifestante na realização da relação jurídica sobre um objeto determinado. (RIZZARDO, 2015, p. 519)

O cuidado com o consentimento do titular mostrou-se muito importante no cenário tecnológico atual, onde uma grande quantidade de dados pessoais é coletada, sendo esses bens mercantilizados por uma série de sujeitos e pela ocorrência da falta de transparência no processamento de dados. Diante desta situação, tem-se aderido que a interpretação do consentimento deve ocorrer de forma restritiva, e que o agente não pode estender a autorização concedida para o tratamento dos dados para outras formas que não seja que se foi acordada, para posterior utilização de forma diversa, inclusive, para outras pessoas distintas da que foram informadas para o titular dos dados.

Nessa perspectiva, segundo a doutrina de Danilo Doneda, expõe que:

Neste momento, podemos voltar nossa análise para os efeitos do consentimento e então verificar como ponderar essa autodeterminação. E vemos que existem dois planos de análise possíveis: no primeiro, o consentimento é o instrumento por excelência dessa autodeterminação e, portanto, de um aspecto da tutela da pessoa. Em outro plano, porém, o consentimento representa o papel de instrumento de legitimação para que esses dados sejam, em alguma medida, utilizados por outra pessoa. E é preciso levar em conta que, muitas vezes, isso significa, conforme já ressaltamos, em alguma medida a transformação desses dados em uma determinada utilidade. (2020, p. 296/*online*)

Em outras palavras, o consentimento não legitima o tratamento de dados desnecessários, o consenso se dá para o que se foi informado, sendo necessário no ato, a participação de um agente ativo e um passivo do negócio, ou seja, as vontades de ambas as partes se comunicam e se relacionam por meio de propostas e aceitações. Uma parte faz uma proposta, ou faz uma declaração de intenção, a outra analisa a declaração do proponente e, podendo aceitá-la ou não. Portanto, há propostas e aceitações. Combinando as duas declarações de intenção, ou mesmo integrando-as, o consentimento é considerado mútuo e o negócio se inicia.

### **3.2 Consenso dentro da lei**

De acordo com a LGPD, o consentimento é caracterizado como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Ciente disso, fazendo uma breve análise, nota-se que a LGPD, entende a necessidade de que os contratos jurídicos digitais e até mesmo os físicos, possuam finalidade bem definidas e transparentes, constando todas as informações relevantes e precisas para garantir a liberdade do indivíduo na tomada de decisão.

Assim, o artigo 7º esclarece que o tratamento de dados somente pode ocorrer mediante consentimento do titular, esse consentimento segundo o artigo 8º, *caput*, deve ser por escrito ou por meio que demonstre a manifestação de vontade do titular. O ônus da prova do consentimento é do controlador de dados e é, como já explicitado no tópico anterior, para uma finalidade específica sendo nulas as autorizações genéricas. (BRASIL,2018)

Nesse sentido, é notável que para haver uma autorização, o consenso é fator mais relevante anterior ao tratamento. Posto isso, é essencial entender as principais características do consentimento, sendo este ato necessário para a formalização jurídica e tutelada da utilização dos dados pessoais.

Seguindo uma linha de raciocínio, de início é interessante aclarar que, a manifestação livre significa que o titular pode escolher entre aceitar ou rejeitar o uso de seus dados sem intervenção ou circunstâncias que prejudiquem seu consentimento. Logo, determina o artigo 7º, parágrafo 3º da referida Lei que, é vedado o tratamento de dados pessoais mediante vício de consentimento. Com relação a essa característica, é necessário analisar qualquer assimetria entre as partes e a vulnerabilidade de qualquer uma das partes para garantir que o consentimento realmente ocorra. (BRASIL, 2018)

Seguindo essa lógica, pode se dizer que a LGPD considera que, quando o fornecimento de dados pessoais for condição para o acesso a algum tipo de produto ou serviço, o cidadão deve ser informado a esse respeito e sobre os meios pelos quais ele pode exercer o seu direito, citando, por exemplo, a revogação do consentimento.

Acerca do assunto, Bruno Bioni esclarece que:

A questão principal que deve ser analisada é se há alguma forma de subordinação, que possa de certa forma viciar o consentimento e para isso, deve haver uma análise do caso concreto para concluir se o consentimento foi livre ou não. (2020, p.189)

Diante disso, a lei também estabelece que, se o tratamento dos dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer seus direitos enumerados no art. 18 da lei:

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:

- I - confirmação da existência de tratamento;
- II - acesso aos dados;
- III - correção de dados incompletos, inexatos ou desatualizados;

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;  
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;  
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;  
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.[...] (BRASIL, 2018, *online*)

É importante ressaltar, conforme mencionado acima, que o consentimento poderá ser revogado a qualquer momento, mediante manifestação expressa e objetiva do titular, por procedimento gratuito e facilitado. Argumenta-se a possibilidade de revogação incondicional desse tipo de consentimento com base no poder de escolha do titular e na proteção da personalidade, que tem entre seus atributos a indisponibilidade.

Assim sendo, com base no direito de alteração, e de se informar sobre a utilização de seus dados, em consonância com o art.18, o titular detém do ato de consentir ou não, mas fundamentalmente da possibilidade de fazê-lo de forma livre e racional, mesmo havendo desequilíbrio de forças entre os contratantes.

Ainda dentro das características do consentimento, o termo consentimento informado na LGPD, significa que o titular dos dados, deve ter ao seu dispor as informações necessárias e suficientes para avaliar corretamente a situação e a forma como seus dados serão tratados. A informação é fator determinante para a expressão de um consentimento livre e consciente, circunscrito, portanto, a certo tratamento, para determinado agente e sob determinadas condições. Para diminuir as assimetrias técnica e informacional existentes entre as partes, exige a lei que ao cidadão sejam fornecidas informações transparentes, adequadas, claras e em quantidade satisfatória acerca dos riscos e implicações do tratamento de seus dados. (TEPEDINO; TEFFÉ, 2020, p. 96)

Seguindo ainda na premissa do consentimento informado, o artigo 9º da LGPD dispõe que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados:

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; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. (BRASIL, 2018, *online*)

Em relação o consentimento, se for necessário e havendo mudanças em relação à finalidade para o tratamento dos dados não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo este revogar o consentimento, caso discorde das alterações.

É necessário explicar ainda a manifestação de vontade inequívoca, ou seja, não ambígua, evidente, e deve ocorrer de forma clara, sendo relevante analisar o grau e a qualidade de interação entre as partes. Nesse caso, mostra-se relevante analisar a expectativa do titular em uma relação específica, ou seja, deve existir o legítimo interesse, sendo necessário esculpir um qualificador que não seja contraditório em relações a situações nas quais se poderiam extrair possíveis usos de dados.

Por essa razão, os famosos *Cookies*, os termos de uso e políticas de privacidade pré-aceitos, ou seja, já marcados, não serão considerados adequados perante a LGPD, tendo em vista o não consentimento do titular. Da mesma forma, o silêncio não importará no consentimento. Ainda sobre essa qualificação do consentimento, cabe ressaltar que há questionamentos voltados a avaliar se a manifestação do titular de dados poderia se dar de forma tácita, a partir de um comportamento concludente. (SOMBRA, 2019, p. 137)

Isto posto, a manifestação de consentimento deve surgir quando for expressada uma finalidade determinada, de modo que autorizações sejam fornecidas diante do esclarecimento objetivo, de modo contrário, na impossibilidade de

acompanhamento pelo interessado do destino de seus dados, cabe àquele que pretende realizar o tratamento informar o interessado previamente de forma ampla. Cabe também assegurar que o interessado realmente tem condições de compreender as consequências do consentimento e que efetivamente as compreendeu.

### **3.3 Responsabilidade civil na Lei Geral de Proteção de Dados**

A responsabilidade civil encontra-se regulamentada na Seção III do Capítulo VI da LGPD, intitulada de “Da Responsabilidade e do Ressarcimento de Danos”. Nessa seção estão dispostas as regras de incidência de responsabilidade, solidariedade, inversão do ônus da prova e excludentes, sobre as quais se tratará a seguir. De antemão, é imprescindível a compreensão acerca do regime jurídico específico da responsabilidade na tutela Jurídica.

Relativo ao ramo do direito obrigacional, a responsabilidade civil é um instituto que decorre do reconhecimento dos direitos pessoais, ou seja, são normas que visam manter o bom convívio em sociedade, estando relacionada à noção de não prejudicar o outro, garantindo que, uma vez prejudicado determinado direito, haverá a reparação do dano que infligido. A violação, portanto, é ato ilícito que gera a obrigação de reparar e cria um vínculo jurídico que outorga a uma parte o direito de exigir da outra que cumpra determinada prestação (GONÇALVES, 2016).

No direito brasileiro a responsabilidade civil pode ser analisada sob a ótica de dois regimes, o da responsabilidade civil subjetiva e o da responsabilidade civil objetiva, sendo que o primeiro é necessário que o agente causador do dano tenha dolo ou culpa, e o segundo, o dano independe da intenção do ato, portanto, os dois se diferenciam pela necessidade ou não de demonstração de culpa do agente.

De um modo geral, para a configuração do dever de indenizar, deve existir, cumulativamente: a) ação ou omissão jurídica relevante; b)nexo causal; e c) dano. Esses elementos são comuns aos dois regimes jurídicos de responsabilização. Porém, enquanto a responsabilidade civil subjetiva exige a demonstração de culpa do agente, aqui compreendida enquanto culpa *latu sensu*, em que está inserido o dolo e a culpa *strictu sensu*, que decorre da negligência ou imprudência, a responsabilidade



civil objetiva fundamenta-se no risco inerente à atividade praticada. (GONÇALVES, 2016).

No que tange ao regime jurídico adotado pela LGPD, a legislação não estabeleceu de forma expressa a opção por um ou outro, o que tem gerado um intenso debate doutrinário. Enquanto parte da doutrina afirma haver um sistema baseado na responsabilidade objetiva, outros defendem a adoção do regime de responsabilidade subjetiva.

A despeito dos embates doutrinários, verifica-se que a Lei Geral de Proteção de Dados elegeu o sistema de responsabilidade civil subjetiva em perfeito alinhamento com o Código Civil, inserindo-se de forma harmoniosa no mosaico legislativo, o mesmo ocorrendo em relação ao Código de Defesa do Consumidor que, dado o tratamento Constitucional da defesa do consumidor, atrai para seu sistema de responsabilidade objetiva os fatos jurídicos dessa natureza. (TASSO, 2020, p. 113).

Nesse âmbito, ao ler o texto legal, percebe-se o enunciado do art. 42 da referida lei não é claro quanto ao regime de responsabilidade civil, subjetivo ou objetivo, ou seja, existe uma dubiedade, não bastando o mero desempenho da atividade de tratamento de dados para que seja possível imputar responsabilidade ao agente. Para se cogitar a responsabilidade subjetiva, é necessário um comportamento culposos, seja por violar diretamente a legislação de proteção de dados, seja por deixar de tomar medidas de segurança adequadas.

Para os que defendem que o regime da responsabilidade civil objetiva, o cerne da questão estaria disposto no Código Civil, artigo 927, parágrafo único, que utiliza o termo “independentemente de culpa”. Nesse sentido, a tutela estaria no risco da atividade desenvolvida e na maior proteção do direito fundamental dos titulares dos dados pessoais.

Partido dessa premissa, pode-se analisar que:

Essas limitações ao tratamento de dados, conjuntamente com a verificação de que a LGPD assume como regra a eliminação dos dados quando seu tratamento esteja encerrado (art. 16) e igualmente o aceno que faz em diversas oportunidades à necessidade de se levar

em conta o risco presente no tratamento de dados, indicam que a Lei procura minimizar as hipóteses de tratamento àquelas que seja, em um sentido geral, úteis e necessárias, e que mesmo estas possam ser limitadas quando da verificação de risco aos direitos e liberdades do titular de dados. Trata-se, dessa forma, de uma regulação que tem como um de seus fundamentos principais a diminuição do risco, levando-se em conta que o tratamento de dados apresenta risco intrínseco aos seus titulares. Assim justifica-se o legislador optar por um regime de responsabilidade objetiva no art. 42, vinculando a obrigação de reparação ao dano no exercício de atividade de tratamento de dados pessoais (MENDES; DONEDA, 2018, p. 477).

O artigo 42 da LGPD contém uma cláusula geral de responsabilidade, imputando a obrigação de indenizar ao controlador ou operador que, descumprindo a lei, causar dano patrimonial ou extrapatrimonial aos titulares dos dados pessoais violados. A LGPD estabeleceu, de forma similar ao Código de Defesa do Consumidor – CDC, Lei 8.078/90, a solidariedade dos agentes de tratamento que causarem lesão, art. 42, § 1º, I e II, e permitiu a inversão do ônus da prova por critério judicial, art. 42, § 2º, para mitigar a assimetria na relação entre controladores, operadores e titulares de dados pessoais.

Logo em seguida, no art. 43 da LGPD, está elencado que o dano deverá ser comprovado, mantendo o padrão de responsabilidade prevista no ordenamento pátrio, código civil e código de processo civil, onde o ofendido deverá alegar e provar a existência e extensão do dano. A reparação só poderá ser exigida de quem realizou o tratamento de dados de alguma forma. Se a cobrança é feita de agente que não participou, não há como configurar o nexo de causalidade entre dano e suposto ato ilícito. Sendo assim, o agente se desincumbe de reparar.

A mesma lógica da responsabilidade civil, encontra-se presente no art. 44 o conceito de tratamento irregular dos dados, que ocorrerá quando contrariar a disciplina legal ou quando não fornecer a segurança e legitimamente esperada pelo respectivo titular. Contrariamente, não pode ser tido como irregular o tratamento que observou a lei e que, concomitantemente, proveja a segurança que dele se espera.

Ao analisar as excludentes de responsabilidade verifica-se que há uma presunção legal quanto à autoria do tratamento por parte do agente a quem o tratamento é atribuído e quanto a violação à legislação de proteção de dados ou

irregularidade do tratamento, cabendo prova do contrário pelo agente (BIONI; DIAS, 2020). Portanto, caberia ao titular dos dados lesado provar a realização do tratamento de dados, o dano sofrido e o nexo causal.

Também viola direito aquele, operador ou o controlador, que não cumpra os deveres de segurança dos dados. Os artigos 46 ao 49 da LGPD, de forma muito elucidativa e atual, evidencia as condutas, omissivas e comissivas, que os agentes devem ter:

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

[...]

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

[...]

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. (BRASIL, 2018, *online*)

No quesito de segurança prévia e sanções, cabe à Autoridade ser informada de incidentes de segurança, notadamente quando possível de gerar danos aos titulares. Cabe, também, analisar o incidente, determinar as condutas para minimizar ou reverter os danos.

Por fim, pode-se concluir que as características inerentes à responsabilidade civil em questão, se manifesta, principalmente, na regulação detalhada das obrigações comportamentais dos agentes de tratamento. O foco deve ser voltado ao gerenciamento e prevenção de riscos, especialmente relacionado ao uso da inovação tecnológica, adaptando às especificidades da atividade de processamento de dados pessoais e aos requisitos de proteção que ele apresenta. Assim sendo, criou-se um modelo mais maduro de responsabilização civil, no qual se

vai além da responsabilidade dos agentes, tendo-se em vista, especialmente, evitar danos aos titulares dos dados.

## CONCLUSÃO

Conforme analisado durante o presente trabalho de conclusão de curso, a proteção de dados pessoais é de suma importância para a atual sociedade informacional, visto que sem uma regulamentação, a privacidade do cidadão em relação aos seus dados pessoais fica à mercê de empresas e instituições que mercantilizam esse tipo de bem.

A Lei brasileira foi fortemente influenciada pelo Regulamento europeu e sendo possível perceber os operadores do direito no Brasil se basearam das inúmeras orientações propostas pelas autoridades nacionais europeias. Pode se dizer que a LGPD visa um equilíbrio entre o direito à privacidade e o uso massivo das informações pessoais. Sua missão, portanto, não é outra, senão proteger direitos fundamentais, tais como a liberdade, a privacidade, o livre desenvolvimento e a personalidade.

Ao entrar em vigor, a LGPD implantou uma nova regulamentação relacionada aos dados pessoais. Com isto, proporcionou mecanismos efetivos e capazes na manutenção de garantias relacionadas à vida privada, com a devida transparência durante o processo de tratamento, observando o princípio da boa-fé, para garantir a efetividade da lei.

Como fundamentos da LGPD pode-se destacar o respeito à privacidade, liberdade de expressão, inviolabilidade da intimidade, livre iniciativa, defesa do consumidor, direitos humanos, dignidade e exercício da cidadania. Na prática, a LGPD se aplica aos governos e às empresas, tendo que garantir maior segurança aos dados pessoais, sempre observando a finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, responsabilização e a prestação de

contas de tudo que se refere aos dados pessoais, conforme bem explicado durante o presente trabalho.

De modo geral, os pontos mais importantes no quadro geral da LGDP podem ser assim resumidos em: a LGPD é a regra que vale para todo o país, ou seja ela cria o que são dados pessoais e como devem ser processados adequadamente; para processar dados pessoais, deve haver o consentimento de seu titular, exceto quando as normas legais dispuserem ao contrário; não importa se a organização está localizado no Brasil ou fora dele, seu escopo é extraterritorial, as penalidades são severas para as instituições que não cumprirem a legislação; a lei traz a definição de dados pessoais essenciais para um pleno entendimento do comando; a lei destaca as responsabilidades de cada agente de processamento e suas funções.

Por fim, cada vez mais os titulares pedem maior transparência no uso de seus dados pessoais e a proteção efetiva da privacidade não pode ser ignorada, caso contrário, surgirá uma insegurança no mercado global, se tornando inviável qualquer tipo de atuação. Portanto, a empresa ou instituição que coleta e processa os dados, deve deixar claro ao usuário a finalidade para a qual tais informações foram obtidas, como serão utilizadas, podendo o usuário exercer privilégios para autorizar ou não o processamento, ou seja, portanto, em controle efetivo de suas informações pessoais.

## REFERÊNCIAS

BBC NEWS. **Entenda o escândalo de uso político de dados que derrubou valor do facebook e o colocou na mira de autoridades.** São Paulo, 18 de março de 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751>. Acesso em 11 de outubro de 2021.

BIONI, Bruno Ricardo; 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*, Rio de Janeiro, v. 9, n. 3, p.1-23, 2020.

BIONI, Bruno. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 197.

BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** São Paulo; Saraiva, 2007.

BRASIL. **Lei nº 10.406**, de 10 de janeiro de 2002. Institui O Código Civil. Brasília, 2002.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014. Institui o Marco Civil da Internet.** Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm)

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018 . Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm).

CAPANEMA, Walter Aranha. **A responsabilidade civil na Lei Geral de Proteção de Dados.** (ARTIGO) *Cadernos Jurídicos*, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020 Disponível em: [https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii\\_6\\_a\\_responsabilidade\\_civil.pdf?d=637250347559005712](https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712)

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro. Teoria Geral do Direito Civil.** Volume 1. 29ª Ed. 2012.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais elementos da formação da Lei Geral de Proteção de Dados.** 2. ed. -- São Paulo : Thomson Reuters Brasil, 2020.

DONEDA, Danilo. **A proteção dos dados pessoais como um Direito fundamental.** Rio de Janeiro: Espaço Jurídico, 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2021.

FRANÇA. Assembleia Geral da ONU. **Declaração Universal dos Direitos Humanos (Resolução 217 A III)**. Paris, 1948. Disponível em: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>. Acesso em: 10 de out.2021

FRANCE. Council of Europe, **European Convention on Human Rights. 1950**, European Tribunal Europeu dos Direitos do Homem.

GONÇALVES, Maria Eduarda. **Direito da Informação: novos direitos e formas de regulação na sociedade da informação**. Coimbra: Almedina, 2003.

GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 17. ed. São Paulo: Saraiva, 2016.

Gov.br. **Guia de boas práticas lei geral de proteção de dados (lgpd)**. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia-boas-praticas-lgpd>. Gov.br. Brasília, 2020.

Korth, H.F. e Silberschatz, A. **Sistemas de Bancos de Dados**, Makron Books, 2ª edição revisada, 1994.

LARA, P. Rodrigo. **Enfim, a ANPD dá o primeiro passo**. Migalhas, 2021. Disponível em: <https://www.migalhas.com.br/depeso/346477/enfim-a-anpd-da-o-primeiro-passo>. Acesso em 14, de abril de 2021.

LUGATI, L.; ALMEIDA, J. **Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa**. Viçosa: Revista de Direito, 2020.

MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. *Revista de Direito do Consumidor*, São Paulo, v. 120. N. 27. p. 469- 483, 2018.

MULHOLLAND, Caitlin. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18)**. *Revista Dir. Gar. Fund.*, Vitória, v. 19, n. 3, p. 167 set./dez. 2018. Disponível em: 57 <http://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603>. Acesso em: 25 nov. 2021.

PINHEIRO, Patricia. P. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (lgpd)**. Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 04 out. 2021.

REALE, Miguel. **Filosofia do Direito**. 11. ed. São Paulo: Saraiva, 1986. P. 60.



REINALDO, Demócrito. **Direito da informática: temas polêmicos**. Bauru/SP: EDIPRO, 2002.

RIZZARDO, Arnaldo. **Introdução ao Direito e Parte Geral do Código Civil**, 8ª edição. [Rio de Janeiro]: Grupo GEN, 2015. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/978-85-309-6832-8/>. Acesso em: 01 mai. 2022.

SENADO NOTÍCIAS. **Senado inclui proteção de dados pessoais como direito fundamental na Constituição**. Brasília, 20 de outubro de 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protECAo-de-dados-pessoais-como-direito-fundamental-na-constituicao>

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 19ª ed. São Paulo: Malheiros Editores, 2005.

SILVA, José Afonso da. **Curso de direito constitucional Positivo**. 40ª. ed. São Paulo: Malheiros, 2017

SILVA, Rosane Leal; SILVA, Leticia Brum. **A proteção jurídica de dados pessoais na internet: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil**. Direito e novas tecnologias. Florianópolis: FUNJAB, 2013. Disponível em; [www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65](http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65)Acesso em: 1 dez. 2021.

SOMBRA, Thiago. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019. p. 137.

TASSO, Fernando Antonio. **A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor**. *Cadernos Jurídicos*, São Paulo, ano 21, n. 53, p. 97-115, jan./mar. 2020.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. **O Consentimento Na Circulação De Dados Pessoais**. *Revista Brasileira de Direito Civil – RBDCivil*, Belo Horizonte, v. 25, p. 83-116, jul./set. 2020