

GABRIEL DUARTE PIRES

**PRERROGATIVAS E LIMITES NO MANUSEIO DOS DADOS PESSOAIS**

**O CONSENTIMENTO E SUAS IMPLICAÇÕES**

Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).

Prof. (a) Orientador (a) - Pós-doutor  
Nivaldo dos Santos.

**GOIÂNIA-GO**

**2023**

**GOIÂNIA-GO**  
**2023**

“A felicidade pode ser encontrada mesmo nas horas mais difíceis, se você se lembrar de acender a luz.”

Alvo Dumbledore, Harry Potter e o Prisioneiro de Azkaban

## AGRADECIMENTOS

Gostaria de expressar minha gratidão a todas as pessoas e instituições que desempenharam um papel fundamental na realização deste trabalho e na minha jornada acadêmica. Este é um momento de reconhecimento e apreço por todos que estiveram ao meu lado, oferecendo apoio, incentivo e orientação ao longo dessa trajetória.

Primeiramente, quero agradecer à minha mãe, que sempre foi meu pilar de força e apoio incondicional. Sua dedicação, amor e incentivo foram essenciais para que eu pudesse chegar até aqui. Sem o seu apoio, nada disso teria sido possível.

Aos meus amigos, que estiveram ao meu lado durante toda a jornada, quero expressar minha gratidão. Suas amizades me moldaram e me fizeram evoluir não apenas intelectualmente, mas também como pessoa. Cada conversa, cada experiência compartilhada, contribuiu para o meu crescimento, seja no aspecto profissional, mental ou físico. Obrigado por serem parte essencial da minha vida.

Agradeço também a mim mesmo, por acreditar na possibilidade de ingressar na faculdade, mesmo quando as circunstâncias financeiras eram desafiadoras. A concessão da bolsa integral do Prouni abriu portas que eu nunca imaginei, e isso só foi possível graças à minha dedicação e esforço.

Meu sincero agradecimento também vai para o meu orientador, Nivaldo dos Santos, que desempenhou um papel crucial na realização deste trabalho. Sua orientação, paciência e conhecimento foram fundamentais para a construção deste TCC. Agradeço por acreditar em mim e me guiar ao longo deste processo.

Por fim, agradeço à Pontifícia Universidade Católica de Goiás por me oferecer não apenas uma educação de qualidade, mas também uma perspectiva de futuro promissor. Esta instituição abriu portas no mercado de trabalho e me preparou para os desafios que estão por vir, que tornou tudo isso possível. A Pontifícia Universidade Católica me proporcionou uma educação de alta qualidade e a oportunidade de explorar meu potencial acadêmico. Além disso, agradeço aos profissionais do Ministério Público, que me proporcionaram conhecimentos valiosos e insights que enriqueceram o conteúdo deste trabalho.

A todos vocês, meu sincero agradecimento. Este trabalho e esta jornada não seriam os mesmos sem cada um de vocês. Suas contribuições e apoio moldaram meu caminho e me ajudaram a alcançar este marco.

## RESUMO

A Lei Geral de Proteção de Dados (LGPD), em vigor no Brasil desde setembro de 2020, representa um marco regulatório significativo no que diz respeito à proteção de dados pessoais. Este trabalho de conclusão de curso (TCC) tem como objetivo analisar os direitos conferidos aos titulares de dados e os limites impostos às organizações sob a égide da LGPD. A LGPD estabelece uma série de direitos fundamentais, garantindo aos titulares de dados o controle sobre suas informações pessoais. Os principais direitos incluem o direito de consentimento informado e explícito, o direito de acesso aos dados, o direito de correção de informações imprecisas, o direito de exclusão de dados, o direito de portabilidade de dados e o direito de oposição ao tratamento. Estes direitos conferem aos indivíduos maior autonomia sobre suas informações pessoais e promovem a transparência nas práticas de tratamento de dados. Além disso, a LGPD impõe limites claros às organizações que tratam dados pessoais. As principais restrições incluem a necessidade de obter consentimento explícito dos titulares de dados, a definição de bases legais para o tratamento de dados, a limitação do tratamento de dados às finalidades específicas, a minimização na coleta de informações, a exigência de transparência nas práticas de tratamento, a imposição de medidas de segurança para proteção de dados, e a proibição de transferência internacional de dados sem observar os requisitos de segurança. Este TCC abordará detalhadamente cada um desses direitos e limites, analisando também os desafios práticos enfrentados pelas organizações na conformidade com a LGPD. Será considerada a jurisprudência e a aplicação da lei em casos reais, bem como as implicações para o cenário empresarial. Por meio desta análise crítica, o TCC busca contribuir para uma compreensão aprofundada dos direitos e limites estabelecidos pela LGPD, bem como para o debate sobre a importância da proteção de dados pessoais no contexto atual, onde a privacidade e a segurança das informações se tornaram temas centrais.

**Palavras-chave:** Dados pessoais. Lei Geral de Proteção de Dados. Privacidade. Intimidade. Privacidade. Liberdade. Direitos e limites pela LGPD.

## **LISTA DE SIGLAS**

LGPD	Lei Geral de Proteção de Dados
GDPR	General Data Protection Regulation
DP	Dados Pessoais
PbD	Privacy by Design
ANPD	Autoridade Nacional de Proteção de Dados Pessoais
RIPD	Relatório de Impacto de Proteção de Dados

## SUMÁRIO

<b>RESUMO.....</b>	<b>5</b>
<b>1. INTRODUÇÃO.....</b>	<b>7</b>
<b>2. CAPÍTULO I - EVOLUÇÃO HISTÓRICA DA PROTEÇÃO AOS DADOS PESSOAIS E PRINCÍPIOS.....</b>	<b>12</b>
2.1 AVANÇOS INICIAIS.....	12
2.2 REPERCUSSÃO DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS NO BRASIL.....	16
2.3 INTRODUÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS.....	16
2.4 PRINCÍPIOS.....	17
<b>3 CAPÍTULO II - INTRODUÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS.....</b>	<b>21</b>
3.1 CONTEXTO ATUAL.....	21
3.2 CONCEITOS E AGENTES DE TRATAMENTO DE DADOS.....	22
<b>3.2.1 Conceitos ainda vigentes.....</b>	<b>22</b>
<b>3.2.2 Agentes de tratamento de dados.....</b>	<b>24</b>
3.2.2.1 Titular dos dados.....	24
3.2.2.2 Controlador.....	26
3.2.2.3 Operador.....	27
3.2.2.4 Encarregado.....	28
3.2.2.5 Autoridade Nacional de Proteção de Dados.....	29
<b>4. CAPÍTULO III – AS PERMISSÕES E OS LIMITES IMPOSTO PELA LEI GERAL DE PROTEÇÃO DE DADOS.....</b>	<b>31</b>
4.1 O PAPEL DO CONSENTIMENTO.....	32
4.2 A IMPORTÂNCIA DA TRANSPARÊNCIA EM TODAS AS ETAPAS DO MANUSEIO DOS DADOS.....	34
4.3 CASOS EM QUE O CONSENTIMENTO É DISPENSADO.....	37
<b>4.3.1 Hipóteses para o Tratamento de Dados Pessoais sem Consentimento do Titular...37</b>	<b>37</b>
<b>4.3.2 Outras Disposições Relevantes.....</b>	<b>38</b>
4.4 LEGÍTIMO INTERESSE.....	39
4.5 SANÇÕES ADMINISTRATIVAS DA LGPD: GARANTINDO O CUMPRIMENTO DA LEI COM RESPONSABILIDADE.....	40
<b>4.5.1 Responsabilidade Proativa e Governança.....</b>	<b>41</b>

<b>CONCLUSÃO.....</b>	<b>43</b>
<b>REFERÊNCIAS.....</b>	<b>45</b>

## 1. INTRODUÇÃO

É inegável a importância das informações no decorrer da história, isto é, quem as tem inicia revoluções, obtém vantagens econômicas, ganha guerras. Pode-se tirar essa conclusão ao ler o clássico livro “A Arte da Guerra” de Sun Tzu (500 a.c.), em que aborda a relevância de avaliar e planejar, tendo conhecimento de cinco informações e fatores que podem influenciar diretamente os planos: terreno, caminho, as estações, a liderança e a gestão.

E o valor da informação vem aumentando cada vez mais a cada dia que passa. O período quaternário<sup>1</sup> demonstrou que a importância da obtenção e do manuseio da informação é extremamente relevante para atingir a finalidade desejada, independente de qual seja. Com a chegada da rede mundial de computadores, as informações se tornaram cada vez mais fáceis de serem coletadas, manuseadas, repassadas, e, até mesmo, modificadas.

A informação é importante para tudo em nossas vidas, mesmo nos setores mais improváveis, e quando o assunto se trata de comércio e economia, a coleta e o manuseio da informação se destacam exponencialmente na atualidade. Dessa forma, a maneira como as informações pessoais vão ser tratadas, os limites e as ferramentas para coibirem o mau uso de dados coletados dos clientes devem ser motivo de intensa discussão.

Existem dois opostos nessa relação, quem vai dispor de seus dados e quem vai coletar esses dados. Geralmente, quem disponibiliza os dados são os clientes, já do outro lado, normalmente é a empresa que presta serviços ou vende produtos que coletam esses dados.

Quanto à finalidade, de um lado, tem-se o empresário, possuidor dos meios de produção, visando sempre potencializar o lucro e diminuir os gastos, bem como expandir os horizontes da sua empresa. E para que consiga atingir seus objetivos, é preciso que os produtos e os serviços da empresa cheguem até seus potenciais clientes.

Do outro lado, tem-se o cliente, lado fraco da relação existente entre os dois, buscando sempre o melhor produto, melhor serviço, menor preço, etc. E para que ele alcance esses interesses, é importante que produtos e serviços disponíveis no mercado venham ao seu conhecimento.

Assim sendo, tanto o empresário quanto o cliente precisam da tão aclamada informação.

---

<sup>1</sup> O período quaternário teve início há 2,6 milhões de anos atrás e se perpetua até os dias atuais. INFOESCOLA. **Período Quaternário. Disponível** em: <https://www.infoescola.com/geologia/periodo-quaternario/>. Acesso em: 15 de junho de 2023.

O empresário buscando atingir o seu público-alvo e o cliente buscando o melhor produto.

Eis que surgem algumas perguntas: “quanto vale os dados pessoais de cada indivíduo?” “Como as empresas podem consegui-los?” “Qual a liberdade que as empresas possuem para manusear e compartilhar esses dados?” “As empresas podem compartilhar os dados pessoais de seus clientes?” “Elas podem, dentro de uma rede interna, movimentar os dados e publicá-los como bem entender?”

Assim, o direito à privacidade e a proteção de dados pessoais tem sido um tema cada vez mais discutido no mundo inteiro. Com o advento da internet e da tecnologia digital, a facilidade de coleta e utilização de dados pessoais cresceu exponencialmente, tornando-se um tipo de mercadoria para empresas e prestadores de serviços.

Dessa forma, sendo necessário discutir as principais dificuldades e desafios no campo da proteção de dados pessoais. Entre os quais, um dos principais obstáculos é o conflito entre a proteção de dados pessoais e outros direitos fundamentais, como a liberdade de expressão, a liberdade de informação, a segurança pública, dentre outros.

De igual forma, outra necessidade é a de se estabelecer um equilíbrio entre os interesses comerciais e os direitos dos titulares dos dados pessoais. A atividade econômica não pode ser um obstáculo à proteção de dados pessoais, mas também não pode ser limitada de maneira desproporcional.

Assim, o objetivo deste é analisar o papel do consentimento na proteção de dados pessoais, adentrando em temas mais específicos, como: compreender os limites determinados às empresas no manuseio de dados pessoais; entender a liberdade das empresas quanto ao manuseio de dados pessoais de clientes; e abordar a atual regulamentação de dados pessoais.

E para alcançar esses objetivos, alguns problemas deverão ser abordados, como o contexto histórico que levou a criação das normas atuais, os princípios, os principais elementos, o papel do consentimento, o papel da transparência, a insuficiência do consentimento em proteger efetivamente a privacidade dos indivíduos, a governança de dados e a regulação atual que detém várias brechas.

Quanto ao consentimento, precisa-se questionar o modelo atual de proteção de dados, que se baseia principalmente no consentimento do titular dos dados. Uma vez que o consentimento pode ser problemático e insuficiente para proteger efetivamente a privacidade dos indivíduos. Por outro lado, no que tange a governança de dados, tem-se a necessidade de transparência e prestação de contas nas práticas de coleta e uso de dados.

Nessa mesma linha, uma vez que a atual regulação de dados não oferece a segurança

jurídica que precisamos, ver-se-á, mais à frente, que surge a necessidade de uma regulação mais robusta dos dados pessoais, incluindo leis que estabeleçam limites claros para a coleta, uso e compartilhamento de informações pessoais.

Quanto à problemática, tem-se, também, que questionar o atual modelo de consentimento, é preciso analisar a necessidade de outras abordagens, como a implementação de medidas técnicas de privacidade e a criação de novos direitos de proteção de dados, podem ser mais eficazes do que o consentimento para proteger a privacidade dos indivíduos, conforme será abordado no presente.

Já no que se refere a governança de dados, ver-se-á, também, que é importante destacar a importância da transparência e prestação de contas nas práticas de coleta e uso de dados. Sugerir que as empresas e organizações devem ser mais transparentes em relação à coleta e uso de dados pessoais, e que os titulares dos dados devem ter mais controle sobre suas informações pessoais.

Por último, mas não menos importante, que é preciso analisar a atual regulação de dados, argumentar sobre a possibilidade de uma regulação mais robusta dos dados pessoais, incluindo a criação de leis que estabeleçam limites claros para a coleta, uso e compartilhamento de informações pessoais. Sugerir, que as leis de proteção de dados devem ser aplicadas de forma mais rigorosa e que as autoridades de proteção de dados devem ter mais recursos para fiscalizar as práticas das empresas e organizações.

Ante o exposto, tendo em vista o tema a ser tratado, o trabalho será realizado mediante pesquisa bibliográfica, já que é uma metodologia que consiste na revisão sistemática da literatura existente sobre o tema de estudo. Essa metodologia é útil para fundamentar teoricamente o trabalho, contextualizar o tema e identificar lacunas de conhecimento que podem ser abordadas na pesquisa.

## 2. CAPÍTULO I - EVOLUÇÃO HISTÓRICA DA PROTEÇÃO AOS DADOS PESSOAIS E PRINCÍPIOS

### 2.1. AVANÇOS INICIAIS

É inegável a importância da informação, independentemente do tema, quanto mais se sabe algo, maior a probabilidade de lograr êxito no objetivo almejado. Quase tudo que é importante gera lucro. E quando se fala em dinheiro, em lucro, inevitavelmente o mercado se torna o protagonista da história (Smith, 2023). Ele é, ao mesmo tempo, protagonista e antagonista na evolução da raça humana, conforme visto no decorrer da evolução humana (Marriot, 2015).

Se por um lado, protagonista quando se fala em riqueza, melhoria na infraestrutura, progresso econômico e social, dignidade e conforto. Por outro, paradoxalmente, o mercado, também, é algoz dos mais fracos. Sendo que os mais fracos são os trabalhadores, que eram/são sempre os hipossuficientes da relação. A história está aí para quem quiser a prova categórica, basta voltar há alguns anos atrás, com a compra de escravos, a revolução industrial e outros eventos (Marriot, 2015).

Com isso, chega-se à conclusão de que, sempre que puder, o empregador vai sugar toda força de trabalho que puder de seu empregado, independente dos danos causados a este. Fazendo-se, assim, necessária a intervenção do estado para a proteção dos mais fracos. Contudo, tudo que é extremo é pútrido, e a intervenção exacerbada do estado na economia e política não foge à regra, conforme Friedrich Hayek (2010), em que é conhecido por sua defesa do liberalismo clássico e é um crítico da intervenção estatal na economia. Em seu livro, "O Caminho da Servidão", ele argumenta que a interferência excessiva do estado na economia pode levar a ineficiências, restrições à liberdade individual e distorções nos mecanismos de mercado.

Na mesma linha de pensamento, o renomado autor Jorge Orwell (1944), por exemplo, no final da Segunda Guerra Mundial, demonstrou em seu livro, 1984, sua preocupação com a inobservância do Estado aos direitos à privacidade, temendo o controle desmedido do "Grande Irmão"<sup>2</sup> sobre os cidadãos, devido ao contexto histórico do pós-guerra com os governos

---

<sup>2</sup> Termo inventado e utilizado por Orwell para se referir ao personagem que exerce controle total da sociedade em seu romance, ou à qualquer excesso de controle ou autoridade por uma figura, ou tentativa por parte do governo no excesso de vigilância que culminam em violação e invasão de privacidade, usada no livro 1984.

GRINBERG, Keila. **Quem é o Grande Irmão?**. Rio de Janeiro: Universidade federal do Rio de Janeiro, Instituto Ciência Hoje, 2023. Disponível em: < <https://cienciahoje.org.br/coluna/quem-e-o-grande-irmao/> >. Acesso em: 19

totalitaristas.

À vista disso, analisando superficialmente a história mundial através dos olhos de Karl Marx, a única constante nessa equação é o cidadão “comum”, à mercê de quem detém os meios de produção (1867). Conforme expõe no livro "O Capital", Marx discute a dinâmica do capitalismo e argumenta que, nesse sistema, os trabalhadores são da classe social explorada. Ele sustenta que, sob o modo de produção capitalista, os empregados são colocados em uma posição de desvantagem em relação aos empregadores.

Assim sendo, com o passar do tempo, no contexto global do fim da Segunda Guerra Mundial, já começou a aparecer, implicitamente, dentro do direito à privacidade, elementos genéricos da Lei Geral de Proteção de Dados, no artigo 12 da Declaração Universal dos Direitos Humanos, de 1948, vejamos: “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.”.

É prevista a mesma proteção à privacidade no artigo 11, II, do Pacto San José da Costa Rica, assinado em 22 de novembro de 1969 e ratificado pelo Brasil em setembro de 1992, vejamos:

#### ARTIGO 11

##### Proteção da Honra e da Dignidade

1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.
2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.
3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

No âmbito europeu, a salvaguarda da privacidade também é mencionada de forma geral na Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, adotada em 1950, especificamente no seu artigo 8º:

## ARTIGO 8º

### Direito ao respeito pela vida privada e familiar

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 económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

Internacionalmente, a proteção de dados começou a ganhar destaque nos anos 1970, com o aumento do uso de tecnologias de processamento de dados e a preocupação crescente com a privacidade das informações pessoais (Westin, 1967).

Alan Westin, professor de ciência política, escreveu o livro "Privacy and Freedom" em 1967, que discutia questões de privacidade e a crescente coleta de informações pessoais na era da computação. Embora tenha sido publicado antes dos anos 1970, sua obra teve um impacto significativo na conscientização sobre a importância da proteção de dados.

Em 1980, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) publicou suas Diretrizes sobre Proteção de Privacidade e Fluxos Transfronteiriços de Dados, que estabeleceram princípios básicos para a proteção de dados em nível internacional.

Importante destacar que a evolução da internet foi categorizada em três fases distintas: Web 1.0, Web 2.0 e Web 3.0. A primeira fase, conhecida como Web 1.0, foi marcada pela abundância de informações disponíveis para os usuários, porém sem a capacidade de editar ou alterar o conteúdo, limitando-os a um papel de meros espectadores. Além disso, os serviços disponíveis na rede eram predominantemente controlados por licenças, além de serem pagos, o que impulsionou o crescimento financeiro das empresas (Paesani, 2014).

Coutinho e Júnior (2017) ressaltam que, inicialmente, a internet era de difícil acesso, mas com o tempo ocorreu uma democratização e evolução tecnológica, tornando-a mais acessível. Em 2004, surgiu o termo Web 2.0, que trouxe uma nova perspectiva para a internet, não apenas como meio de disseminação de informações e comercialização de serviços, mas como uma plataforma para colaboração, cooperação e interação entre os usuários.

De acordo com Trein e Schlemmer (2019), a transição da Web 1.0 para a Web 2.0 aconteceu rapidamente, com o surgimento de diversas metodologias, como Wikipédia, Podcasts e Blogs. Essa mudança permitiu que os usuários se tornassem produtores e consumidores de

conteúdo, facilitando a criação e edição de informações digitalmente, além de expandir a variedade de métodos disponíveis e aumentar o número de servidores que ofereciam páginas online gratuitamente.

Morais, Lima e Franco (2017) enfatizam que a Web 3.0 apresenta programas capazes de analisar informações de forma mais precisa e com menor esforço, tornando os computadores mais eficientes na organização e análise de dados disponíveis online. Isso possibilita aos dispositivos interpretarem as preferências dos usuários e auxiliá-los em suas navegações.

No âmbito global, foram estabelecidas regulamentações para o direito e proteção na internet, e isso foi concretizado por meio do Marco Civil da Internet. Essa lei tem o propósito de regular o acesso à internet e a proteção de dados.

O Brasil é considerado um pioneiro ao adotar o princípio da neutralidade, que garante a mesma qualidade de acesso à internet para todos os usuários, sem qualquer tipo de discriminação. Essa regulamentação representa um avanço importante na normatização do uso da internet, uma vez que busca controlar e restringir as ações daqueles que fazem mau uso dos recursos disponíveis (Guerra, 2014).

Antes do Marco Civil, não existia uma legislação específica para tratar de situações prejudiciais ocorridas no ambiente digital, como a divulgação indiscriminada de imagens e dados, sem a devida proteção ao usuário. Era essencial aplicar leis que nem sempre forneciam total amparo às situações concretas, como o Código Civil (Pereira, 2016). Vale ressaltar que o Código Civil era utilizado para resolver conflitos provenientes das relações virtuais, como invasões de privacidade e o envio de mensagens não solicitadas, entre outros.

Lemos (2014) destaca a importância do Marco Civil da Internet para a sociedade, especificamente no que diz respeito à privacidade e proteção das informações. É importante lembrar que a internet não pertence a um único país, mas é uma ferramenta global que não deve ser controlada exclusivamente por uma nação. Além disso, a proteção dos direitos humanos, o exercício da cidadania no meio digital e o desenvolvimento da personalidade são assegurados, garantindo que tanto os direitos humanos quanto os direitos fundamentais e de personalidade sejam protegidos no ambiente online.

O autor também destaca a defesa da pluralidade e diversidade, sem qualquer forma de discriminação. A internet deve ser aberta, livre e colaborativa, garantindo seu desenvolvimento de maneira que abranja os interesses sociais, a inovação, a liberdade de criação e o desenvolvimento de negócios, fundamentados na livre iniciativa, na defesa do consumidor e na livre concorrência.

Segundo o magistrado Paulo Gustavo Gonet Branco, é necessário reconhecer o direito à privacidade, ou seja, o direito de não ser alvo de observação por terceiros e de não ter seus dados, informações pessoais e assuntos particulares expostos ao público em geral (Branco, 2021).

Nesse sentido, entende-se que o Marco Civil determina que os provedores de conexão à internet não interfiram no conteúdo acessado pelo usuário, ou seja, não discriminem aplicativos, sites e plataformas com base em preços elevados ou separados do pacote. Essa é uma decisão relevante, especialmente porque as empresas já estavam bloqueando serviços de download de torrents. Ao garantir que todos os dados trafeguem com a mesma velocidade, busca-se preservar a neutralidade de rede, ou seja, o tratamento igualitário das informações, independentemente do tipo de conteúdo (Pereira, 2016).

A partir da exposição realizada, fica evidente que o Marco Civil da Internet tem como objetivo garantir que todos os usuários tenham uma experiência tecnológica digna, assegurando sua cidadania digital, o desenvolvimento de sua personalidade desde o acesso até o processamento de dados, e a responsabilidade pelos danos causados, vigorando até os dias atuais.

## 2.2. REPERCUSSÃO DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS NO BRASIL

Após a implementação do Marco Civil da Internet, a General Data Protection Regulation (GDPR) passou a receber maior destaque. A GDPR, ou Regulamento Geral Sobre a Proteção de Dados, em português, foi introduzida pelo Parlamento Europeu em abril de 2016, como parte da revisão dos regulamentos da União Europeia relacionados à proteção de dados.

O Marco Civil da Internet tinha como objetivo principal estabelecer uma regulamentação mais abrangente no ambiente digital. Até então, os brasileiros contavam apenas com a Lei de Defesa do Consumidor para reivindicar seus direitos, a qual demonstrava defasagem quando se tratava do meio digital e deixava a desejar na relação entre consumidores e empresas na internet (Carvalho, 2021).

A GDPR representa um marco significativo no avanço do tratamento de dados pessoais, pois estabeleceu que os estados-membros da União Europeia poderiam comercializar ou prestar serviços envolvendo dados pessoais, desde que a legislação do país parceiro fosse pelo menos minimamente semelhante às suas, artigo 44 da GDPR. Essa imposição impulsionou muitos

países a criarem ou reavaliarem suas abordagens em relação aos dados pessoais.

Por fim, chegamos à importante questão discutida neste material científico: a introdução da Lei nº 13.709/18 (LGPD - Lei Geral de Proteção de Dados) no sistema jurídico brasileiro. Em linhas gerais, a LGPD viabilizou e garantiu a privacidade das pessoas, estabelecendo diretrizes adequadas para o tratamento de dados pessoais, incluindo o acesso, edição e exclusão desses dados, dando o primeiro passo no correto tratamento dos dados pessoais.

### 2.3. INTRODUÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que foi promulgada em agosto de 2018 e entrou em vigor em setembro de 2020. No entanto, sua origem remonta a um processo mais amplo de desenvolvimento e discussão sobre a proteção de dados pessoais no Brasil e no mundo.

No Brasil, a discussão em torno da proteção de dados pessoais começou a ganhar impulso principalmente no início do século XXI. Em 2010, o Brasil aprovou a Lei nº 12.527, conhecida como Lei de Acesso à Informação, que estabeleceu regras para o acesso a informações públicas pelo cidadão.

Em paralelo, a União Europeia (UE) aprovou o Regulamento Geral de Proteção de Dados (GDPR) em 2016, estabelecendo um marco legal rigoroso para a proteção de dados pessoais em toda a UE. A GDPR teve um impacto global significativo e influenciou diretamente a elaboração da LGPD no Brasil.

A partir dessas influências internacionais e da necessidade de regulamentar a proteção de dados no país, a LGPD foi promulgada no Brasil em 2018. Ela foi criada com o objetivo de estabelecer regras claras e específicas para o tratamento de dados pessoais, além de garantir a proteção dos direitos fundamentais de privacidade e liberdade dos cidadãos.

A LGPD define princípios, direitos e deveres para o tratamento de dados pessoais, exigindo consentimento explícito para a coleta e uso desses dados, além de impor responsabilidades às empresas e organizações que lidam com dados pessoais.

É importante ressaltar que a LGPD também cria a Autoridade Nacional de Proteção de Dados (ANPD), um órgão responsável por fiscalizar e aplicar a legislação, bem como orienta e fornece diretrizes para as empresas em relação ao tratamento de dados. Esta importante autarquia de natureza especial será abordada mais adiante com mais aprofundamento.

## 2.4. PRINCÍPIOS

Quando abordamos os princípios que fundamentam o sistema jurídico brasileiro, é relevante destacar a visão do jurista, advogado e professor Celso Antônio sobre esse instituto normativo, conforme segue:

Mandamento nuclear de um sistema, verdadeiro alicerce dele, disposição fundamental que se irradia sobre diferentes normas compondo-lhes o espírito e sentido servido de critério para sua exata compreensão e inteligência, exatamente por definir a lógica e a racionalidade do sistema normativo, no que lhe confere a tônica e lhe dá sentido harmônico (Mello, 2009. p. 882 – 883).

A doutrina procura elucidar os princípios jurídicos, que são considerados como fonte ou origem, fornecendo a base para a criação de uma norma jurídica. Conforme mencionado pelo renomado jurista 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”. (REALE, 1986, p. 60).

Portanto, pode-se afirmar que todos os tipos de normas possuem princípios presentes em seu texto, seja de forma explícita ou implícita. Esses princípios são fundamentais para fornecer base, garantir a efetividade da legislação em conformidade com outras leis e atestar a constitucionalidade de seus dispositivos.

O artigo 6º da LGPD contém explicitamente todos os princípios. Vejamos:

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 integridade 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.

Em primeiro lugar, temos o Princípio da Finalidade, que visa garantir que os dados sejam utilizados apenas para propósitos legítimos, específicos, explícitos e informados ao titular. Isso impede o tratamento posterior dos dados de forma incompatível com essas finalidades (Brasil, 2018).

O Princípio da Adequação assegura a compatibilidade dos dados coletados com sua finalidade, exigindo que o receptor dos dados justifique e garanta que os dados sejam pertinentes para o assunto em questão. Segundo o Tribunal Regional Federal da 3ª Região (2020), os dados devem ser tratados de acordo com sua destinação, de forma compatível com a atividade para a qual são utilizados.

O Princípio da Necessidade, conforme estabelecido no artigo 6º, inciso III, da Lei nº 13.709/18, restringe a coleta de dados à finalidade de sua utilização, evitando o excesso na coleta de dados pessoais. Esse princípio garante que os dados coletados estejam estritamente alinhados com a finalidade inicial, evitando a coleta e o armazenamento de dados desnecessários, o que resulta em economia em relação à manutenção desses dados pessoais arquivados.

Outro princípio importante na LGPD é o Princípio do Livre Acesso, descrito no artigo 6º, inciso IV, da lei. Esse princípio garante aos titulares dos dados o direito fácil e gratuito de acessar e obter informações sobre o tratamento de seus dados pessoais, incluindo a forma como serão utilizados e o período de tempo em que serão mantidos para atingir a finalidade estabelecida.

O Princípio da Qualidade dos Dados é a garantia de que os dados sejam precisos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento, conforme afirma o Ministério da Cidadania (2021). Esse princípio busca garantir a veracidade e a atualidade da base de dados.

A Transparência é outro princípio destacado na LGPD e possui respaldo constitucional.

De acordo com o artigo 6º, inciso VI, da lei, os titulares dos dados têm o direito de receber informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados pessoais, bem como sobre os agentes responsáveis pelo tratamento, observando-se os segredos comerciais e industriais.

Os princípios da Segurança e da Prevenção estão ligados à proteção dos dados. O Princípio da Segurança, conforme estabelecido no artigo 6º, inciso VII, exige a utilização de medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou divulgação. Já o Princípio da Prevenção, conforme o artigo 6º, inciso VIII, envolve a adoção de medidas para prevenir danos decorrentes do tratamento de dados pessoais, como afirmado por Marcio Pestana (2020), professor e advogado.

Por fim, temos os princípios da Não Discriminação e da Responsabilização e Prestação de Contas, tratados nos incisos IX e X do artigo 6º da LGPD. O Princípio da Não Discriminação busca coibir a prática de atos ilícitos e abusivos, enquanto o Princípio da Responsabilização e Prestação de Contas implica o dever do responsável pelo tratamento dos dados de informar sobre a eficiência das medidas adotadas para garantir a proteção dos dados.

No periódico de 2019, a Fundação Instituto de Administração - FIA discute a relevância da incorporação da Lei Geral de Proteção de Dados (LGPD) no sistema brasileiro, como pode ser observado abaixo:

Nesse contexto, a criação da LGPD é importante para dar mais clareza ao assunto, para que a determinação do que pode e o que não pode no tratamento de dados pessoais não seja subjetiva, questão de intuição ou opinião. Assim, além dos usuários terem mais confiança em relação aos sistemas que coletam seus dados, as empresas podem ajustar seus processos com maior segurança jurídica, sem o risco de cometer ilegalidades sem saber. (Fundação Instituto de Administração – FIA, 2019)

Diante do exposto, fica evidente a preocupação da LGPD em incluir em sua estrutura normas fundamentais que fundamentam seu conteúdo jurídico, seguindo o padrão de outras legislações. Isso demonstra a importância e seriedade dessa lei na missão de proteger os dados pessoais.

### **3. CAPÍTULO II - INTRODUÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS**

Para poder compreender o alcance que uma empresa pode alcançar dentro dos limites estabelecidos em lei, primeiro deve-se observar o contexto atual, os conceitos estabelecidos em lei e os sujeitos que integram a relação que existe durante o tratamento de dados pessoais, uma vez que sem a compreensão de tais elementos se torna extremamente difícil interpretar a LGPD. Todos esses tópicos serão abordados agora.

#### **3.1. CONTEXTO ATUAL**

A promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou LGPD) representa um marco essencial para a nossa integração na economia digital. Antes disso, já tínhamos disposições de proteção abrangentes em vigor. A Constituição Federal garantia os direitos à intimidade, vida privada e sigilo de dados, incluindo o habeas data.

O Código de Defesa do Consumidor (Lei nº 8.078/1990) estabeleceu importantes direitos relacionados aos registros de consumidores, como acesso, comunicação, correção e limitação temporal, que prefiguraram princípios fundamentais das leis de proteção de dados pessoais. As Leis do Cadastro Positivo (Lei nº 12.414/2011), de Acesso à Informação (Lei nº 12.527/2011) e o Marco Civil da Internet (Lei nº 12.965/2014) também contribuíram significativamente para a proteção de dados pessoais.

No entanto, a LGPD representa a primeira lei no Brasil a tratar sistematicamente e de forma coesa da proteção de dados pessoais, estabelecendo regras e procedimentos estruturantes para esse campo emergente do direito. Isso teve um impacto significativo na vida das pessoas, empresas e entidades dos setores público e privado em geral.

A importância da LGPD foi tão notável que o Supremo Tribunal Federal, durante o período de *vacatio legis*, em uma decisão histórica em maio de 2020, reconheceu o direito fundamental autônomo à proteção de dados pessoais.

Isso ocorreu ao suspender a Medida Provisória nº 954/2020, que obrigava as operadoras de telefonia a compartilharem dados identificadores de seus clientes com o IBGE.

O tribunal argumentou que, no mundo atual, com o contínuo avanço da tecnologia da informação, nenhum dado é neutro. Qualquer informação que possa identificar uma pessoa pode ser usada para criar perfis de informações valiosos para o Estado e empresas privadas, potencialmente ameaçando o direito à autodeterminação informacional.

O autor Bruno Bioni desempenha um papel importante na compreensão deste novo campo do direito. Seu trabalho, desde sua dissertação de mestrado, que deu origem ao livro "Proteção de dados pessoais: a função e os limites do consentimento" (Rio de Janeiro, Forense, 2019), aborda temas cruciais como consentimento, legítimo interesse e o regime jurídico de proteção de dados pessoais públicos ou manifestamente públicos.

Este livro será inestimável tanto para pesquisadores em busca de ideias originais como para profissionais do direito que buscam orientação sólida na implementação da nova lei diante das diversas dificuldades práticas.

### 3.2. CONCEITOS E AGENTES DE TRATAMENTO DE DADOS

Posto que a Lei Geral de Proteção de Dados dispõe de uma importância ímpar para o funcionamento dos empreendimentos, nada pode ser deixado de lado, fazendo-se necessário que seja abordado todos os conceitos ainda vigentes na referida lei, bem como o aprofundamento nos seus aspectos mais relevantes, nos quais esses conceitos serão apresentados no próximo tópico e, posteriormente, analisados alguns de seus pontos mais relevantes.

#### 3.2.1. Conceitos ainda vigentes

Primeiramente, antes de abordar os pontos mais relevantes do artigo 5º da LGPD, imperioso se faz a apresentação de todos os conceitos nele ainda dispostos, nada mais claro que a lei, senão vejamos:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;  
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o

tratamento de dados pessoais em nome do controlador;

(...)

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

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

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

(...)

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e

(...)

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Em resumo, os conceitos da LGPD representam uma resposta importante às complexidades da era digital, onde os dados pessoais são uma moeda valiosa. Eles servem como alicerce para a proteção da privacidade, a promoção de práticas éticas e transparentes, a garantia de segurança de dados e a responsabilização das organizações. Ao fazê-lo, eles desempenham um papel essencial na construção de uma sociedade mais justa e segura em relação ao tratamento de informações pessoais.

### 3.2.2. Agentes de tratamento de dados

Abordar-se-á neste tópico os sujeitos: o titular dos dados, fazendo sua interligação com o artigo 16 e 18; o controlador; operador; encarregado, fazendo sua conexão com os artigos 39; e a autoridade nacional com os seus pontos mais relevantes.

#### 3.2.2.1. Titular dos dados

A Lei Geral de Proteção de Dados (LGPD) no Brasil representa um avanço significativo na proteção da privacidade e dos direitos dos cidadãos em relação ao tratamento de seus dados pessoais. O Artigo 17 da LGPD estabelece, de maneira categórica, que toda pessoa natural possui a titularidade de seus dados pessoais, garantindo, assim, os direitos fundamentais de liberdade, intimidade e privacidade, conforme disposto na própria lei. Este artigo confere aos cidadãos o controle sobre suas informações pessoais, possibilitando-lhes decisões informadas sobre como esses dados são tratados.

O artigo 18 da LGPD estabelece os direitos do titular de dados pessoais em relação ao controlador que os trata. Esses direitos representam uma série de garantias essenciais para que os cidadãos possam exercer sua titularidade de dados de forma efetiva. Esses direitos incluem:

**Confirmação da existência de tratamento:** O titular tem o direito de saber se seus dados estão sendo tratados pelo controlador.

**Acesso aos dados:** O titular pode solicitar o acesso às suas informações pessoais que estão sendo tratadas.

**Correção de dados incompletos, inexatos ou desatualizados:** O controlador deve corrigir quaisquer dados pessoais que sejam imprecisos ou desatualizados.

**Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei:** O titular pode solicitar a anonimização, bloqueio ou eliminação de dados pessoais que não sejam mais necessários ou que estejam sendo tratados de forma inadequada.

**Portabilidade dos dados a outro fornecedor de serviço ou produto:** O titular tem o direito de solicitar a transferência de seus dados pessoais para outro fornecedor de serviço ou produto, de acordo com a regulamentação da autoridade nacional.

**Eliminação dos dados pessoais tratados com o consentimento do titular:** O controlador deve apagar os dados pessoais quando o consentimento do titular for revogado, exceto nas

hipóteses previstas na lei.

**Informação sobre uso compartilhado de dados:** O titular tem o direito de ser informado sobre as entidades públicas e privadas com as quais o controlador compartilhou seus dados pessoais.

**Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa:** O titular deve ser informado sobre as implicações de recusar o fornecimento de consentimento para o tratamento de seus dados.

**Revogação do consentimento:** O titular pode revogar seu consentimento, de acordo com os termos especificados na LGPD.

Os direitos do titular de dados devem ser exercidos mediante requerimento expresso do titular ou de seu representante legal, direcionado ao agente de tratamento. O controlador é obrigado a fornecer respostas adequadas, sem custos para o titular, em conformidade com os prazos e termos estabelecidos em regulamentações específicas.

Além disso, a LGPD prevê que os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo. Essa disposição visa proteger os interesses dos cidadãos que buscam exercer seus direitos de forma legítima.

A LGPD também aborda a possibilidade de revisão de decisões tomadas com base em tratamento automatizado de dados pessoais. O titular tem o direito de solicitar a revisão de tais decisões, bem como o direito de obter informações claras e adequadas sobre os critérios e procedimentos utilizados para a decisão automatizada, desde que essas informações não revelem segredos comerciais ou industriais.

A proteção dos direitos do titular de dados não se limita apenas à LGPD, uma vez que o titular também pode buscar a defesa de seus interesses e direitos em juízo, individualmente ou coletivamente, de acordo com a legislação aplicável.

Em resumo, a LGPD estabelece um robusto conjunto de garantias e responsabilidades para proteger os direitos do titular de dados pessoais. Ela fornece as bases para a proteção da privacidade, da liberdade e da intimidade dos cidadãos, ao mesmo tempo em que impõe obrigações aos controladores para garantir o tratamento adequado dos dados pessoais. Essas disposições têm o objetivo de equilibrar as necessidades das organizações com os direitos dos indivíduos em um mundo cada vez mais digital e orientado por dados.

Por outro lado, o artigo 16 da LGPD estabelece diretrizes claras para a conservação e eliminação de dados pessoais. De acordo com esse artigo, os dados pessoais devem ser eliminados após o término de seu tratamento, considerando as limitações técnicas das

atividades. No entanto, a lei permite a conservação dos dados em situações específicas, vejamos:

**Cumprimento de Obrigação Legal ou Regulatória:** O controlador dos dados pessoais pode manter essas informações quando houver uma obrigação legal ou regulatória que assim o determine. Isso garante que as organizações cumpram as obrigações legais, mesmo após o término do tratamento dos dados.

**Estudo por Órgão de Pesquisa:** Dados pessoais podem ser utilizados em estudos conduzidos por órgãos de pesquisa. É fundamental, no entanto, que, sempre que possível, os dados sejam anonimizados para proteger a privacidade dos titulares.

**Transferência a Terceiros:** Os dados pessoais podem ser transferidos a terceiros, desde que sejam respeitados os requisitos de tratamento de dados estabelecidos na própria LGPD. Isso assegura que a transferência seja realizada de maneira adequada, protegendo os direitos dos titulares.

**Uso Exclusivo do Controlador:** Os dados pessoais podem ser mantidos para uso exclusivo do controlador, desde que sejam anonimizados e que o acesso por terceiros seja vedado. Isso garante que os dados sejam usados apenas internamente e de forma a preservar a privacidade do titular.

Essas diretrizes refletem o compromisso da LGPD em equilibrar a proteção da privacidade dos cidadãos com a necessidade legítima de retenção de dados em determinadas circunstâncias. A conservação e eliminação adequadas de dados pessoais são elementos essenciais para garantir a conformidade com a lei e para proteger os direitos dos titulares, promovendo uma gestão responsável de informações pessoais (Bioni, 2019).

### 3.2.2.2. Controlador

O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem compete tomar decisões relacionadas ao tratamento de dados pessoais. Em outras palavras, são as próprias empresas que recebem os dados dos titulares, sejam eles consumidores e/ou empregados, entre outros. O controlador recebe os dados e prepara a estrutura para recebê-los, tratá-los, destiná-los e eliminá-los, transmitindo todas as diretrizes para a materialização do tratamento ao operador (Bioni, 2019).

É responsabilidade do controlador:

Expor que obteve o consentimento do titular dos dados e instruí-lo sobre qualquer

modificação no consentimento para o tratamento de dados, com destaque especial para as mudanças de finalidade, prazo, controlador e compartilhamento de dados (Art. 8, § 2º e 6º) (Brasil, 2018);

Elaborar o relatório de impacto sobre a proteção de dados pessoais (Art. 38) (Brasil, 2018);

Implementar medidas para garantir a transparência no tratamento de dados e fornecer acesso ao relatório de impacto sobre a proteção de dados pessoais à ANPD, quando solicitado (Art. 10, § 2º e 3º) (Brasil, 2018);

Atender às solicitações do titular de dados pessoais, incluindo a comprovação da existência do tratamento de dados, bem como permitir o acesso, correção, anonimização, bloqueio ou eliminação desses dados, conforme as disposições da Lei (Art. 18) (Brasil, 2018);

Desenvolver orientações para o tratamento de dados realizado pelo operador, observando as próprias normas e regulamentos sobre o assunto (Art. 39) (Brasil, 2018).

Nomear o encarregado, exceto nos casos de dispensa, a critério da ANPD (Art. 41) (Brasil, 2018);

Informar à autoridade nacional e ao titular a ocorrência de incidentes de segurança que possam resultar em riscos ou danos significativos aos titulares (Art. 48) (Brasil, 2018).

### 3.2.2.3. Operador

O operador, seja pessoa física ou jurídica, quer seja de direito público ou privado, assume a responsabilidade pela efetiva execução do tratamento de dados pessoais em nome do controlador. Ele é o agente prático encarregado de conduzir o processo de tratamento de dados, podendo ser um funcionário da empresa que recebe os dados (controlador), uma entidade terceirizada ou até mesmo um profissional autônomo.

A figura do operador de dados é um elemento fundamental na Lei Geral de Proteção de Dados (LGPD) no Brasil, e a doutrina de renomados autores, como Danilo Doneda, desempenha um papel crucial na compreensão de suas implicações e responsabilidades.

A LGPD estabelece claramente a diferença entre o controlador e o operador de dados, reconhecendo que ambos desempenham papéis distintos no tratamento de informações pessoais. O controlador é aquele que define os propósitos e os meios de processamento dos dados, enquanto o operador é encarregado de executar o processamento em nome do controlador.

Danilo Doneda (), um autor amplamente respeitado na área de proteção de dados e direito digital, tem contribuído significativamente para a compreensão desses conceitos. Em sua obra, Doneda pode enfatizar a importância da distinção entre controlador e operador, bem como suas respectivas obrigações.

Essa distinção é crucial para garantir que os direitos dos titulares de dados sejam respeitados, que o tratamento de dados seja transparente e que as medidas de segurança adequadas sejam implementadas.

Os operadores desempenham um papel crítico no cumprimento da LGPD, uma vez que são encarregados de realizar as operações diárias de tratamento de dados de acordo com as instruções do controlador.

Isso abrange atividades como coleta, armazenamento, processamento e proteção de dados pessoais. A responsabilidade dos operadores é agir em estrita conformidade com as instruções do controlador e garantir que todas as operações de tratamento sejam realizadas em conformidade com a lei e os princípios de proteção de dados.

Essa abordagem cuidadosa de distinguir entre controlador e operador visa promover a transparência e a responsabilidade no tratamento de dados pessoais. A LGPD impõe obrigações específicas a ambas as partes e exige a celebração de contratos e acordos claros para garantir que as operações de tratamento de dados sejam realizadas em conformidade com as normas de proteção de dados.

Em resumo, a figura do operador de dados, como definida na LGPD, é essencial para garantir a proteção da privacidade e dos direitos dos titulares de dados no contexto digital. Autores respeitados, como Danilo Doneda, desempenham um papel importante na explicação e interpretação desses conceitos, contribuindo para uma aplicação eficaz da legislação de proteção de dados no Brasil (Brasil, 2018).

A distinção clara entre controlador e operador é fundamental para garantir que o tratamento de dados pessoais seja ético, transparente e em conformidade com a lei. Contudo, o controlador e operador atuam em conjunto, desempenhando o papel de agentes de tratamento, conforme estabelecido no Artigo 39 da legislação (Brasil, 2018).

#### 3.2.2.4. Encarregado

A função do encarregado envolve atuar como intermediário entre o titular dos dados, o controlador e a ANPD, com total liberdade para supervisionar o tratamento dos dados,

monitorar tanto o operador quanto o controlador e relatar possíveis irregularidades (Brasil, 2018, art. 5, VIII). É obrigação do controlador nomear o encarregado, conforme estabelecido no artigo 41 da legislação (Brasil, 2018). Além disso, o artigo 23 impõe a mesma obrigação de nomear um encarregado para o tratamento de dados pessoais por pessoas jurídicas de direito público (Brasil, 2018).

### 3.2.2.5. Autoridade Nacional de Proteção de Dados

A Autoridade Nacional de Proteção de Dados (ANPD) tem o papel de atuar junto à sociedade e as instituições, trazendo mais segurança e estabilidade para a aplicação da Lei Geral de Proteção de Dados. Patrícia Peck, ao abordar o tema, esclarece que:

A ANPD tem um papel fundamental como elo entre diversas partes interessadas que vão do titular ao ente e ao ente público, passando pela necessidade alinhamento com demais autoridades reguladoras e fiscalizadoras, bem como os três poderes Executivo, Legislativo e Judiciário que deverão continuar a compreender a temática da dinâmica dos dados pessoais em um contexto não apenas nacional mas principalmente 28 internacional para que o Brasil saiba se posicionar no mercado digital global. (Patrícia Peck, 2020, p. 49)

Por outro lado, de acordo com Lima (2021, p. 125), o estabelecimento de limites para as atividades das empresas nos mercados de tecnologia, relacionados à coleta, uso e tratamento de dados, apresenta um desafio notável. Isso ocorre devido à confrontação de interesses diversos e à necessidade de, na maioria das situações, decidir entre a prevalência de um interesse sobre o outro.

Contudo, o reconhecimento da LGPD de tratar o poder econômico e regular a atividade das empresas de tecnologia representa o ponto de partida incontornável. Da mesma forma, a análise dos dados e informações como ativos da empresa, com destaque para sua base de dados, deve não apenas ser reconhecida pelo sistema de proteção de dados, mas também ser considerada na aplicação de todo o Direito Comercial (Lima, 2021p. 125).

Em 2022, a Medida Provisória 1124/22 estabeleceu a transformação da Autoridade Nacional de Proteção de Dados (ANPD) em uma autarquia de natureza especial. A referida medida altera a Lei Geral de Proteção de Dados Pessoais (LGPD) e foi oficialmente publicada no Diário Oficial da União, sendo, posteriormente, transformada em norma jurídica.

A ANPD é responsável por editar normas, fiscalizar procedimentos e aplicar sanções relacionadas à proteção de dados pessoais. Inicialmente, a ANPD foi criada como um órgão

transitório vinculado à Presidência da República. No entanto, a Lei 13.853/19 estabeleceu um prazo para que o Poder Executivo avaliasse a conveniência de transformá-la em uma autarquia.

Conforme o Decreto-Lei 200/67, que trata da organização da administração federal, uma autarquia é um serviço autônomo criado por lei, com personalidade jurídica, patrimônio e receita próprios. Sua finalidade é executar atividades típicas da administração pública que requerem gestão administrativa e financeira descentralizada.

Os ministros da Economia, Paulo Guedes, e da Casa Civil, Ciro Nogueira, afirmaram, conforme publicado na Agência Câmara de Notícias, na exposição de motivos da MP que o Brasil adotou o modelo de autarquia especial para as autoridades reguladoras, visando promover especialização técnica, estabilidade jurídica e proteção contra interferência política.

Esse modelo, amplamente utilizado em contextos internacionais, como nos Estados Unidos e na Europa, proporciona uma estrutura especializada e descentralizada de atuação estatal, com autonomia administrativa e poderes de supervisão, fiscalização e normatização de atividades.

Segundo o portal Agência Câmara de Notícias (2022), a medida provisória cria um cargo comissionado para o diretor-presidente da ANPD, sem gerar aumento de despesas, e realoca os atuais servidores na nova autarquia. Além disso, determina que a estrutura organizacional e as competências da ANPD, conforme previstas na Lei Geral de Proteção de Dados, serão mantidas.

Em resumo, a LGPD surgiu como uma resposta às demandas crescentes por proteção de dados pessoais, seguindo um contexto histórico global de preocupação com a privacidade e a necessidade de regulamentação adequada do tratamento de dados.

#### **4. CAPÍTULO III – AS PERMISSÕES E OS LIMITES IMPOSTO PELA LEI GERAL DE PROTEÇÃO DE DADOS**

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), em vigor no Brasil desde setembro de 2020, estabelece um conjunto de permissões e limites relacionados ao tratamento de dados pessoais por organizações, com base em dispositivos legais específicos:

**Consentimento informado e explícito (Artigo 7º, I):** A LGPD determina que o tratamento de dados pessoais requer o consentimento explícito do titular, devendo ser obtido de forma clara e específica para cada finalidade de processamento. Isso coloca o controle sobre os dados nas mãos dos indivíduos.

**Base legal para o tratamento (Artigo 7º):** A lei estipula que o tratamento de dados pessoais deve ter uma base legal, como o cumprimento de obrigações legais, o cumprimento de contratos, o legítimo interesse da empresa ou o consentimento do titular dos dados, delimitando os limites para a coleta e o uso de dados.

**Finalidade (Artigo 6º):** A LGPD estabelece que o tratamento de dados pessoais deve ser feito para finalidades específicas e legítimas, não permitindo desvios dessas finalidades sem um novo consentimento ou base legal. Isso evita a coleta excessiva ou o uso inadequado de informações.

**Minimização de dados (Artigo 11):** As organizações são obrigadas a coletar apenas os dados estritamente necessários para a finalidade pretendida, evitando a coleta excessiva de informações.

**Transparência (Artigo 9º):** A lei exige que as organizações forneçam informações claras e acessíveis sobre como os dados serão usados, quem terá acesso a eles e os direitos dos titulares dos dados. Isso permite que os indivíduos compreendam como suas informações estão sendo tratadas e exerçam seus direitos de forma eficaz.

**Direitos dos titulares (Artigos 17 a 21):** A LGPD concede diversos direitos aos titulares dos dados, incluindo o direito de acesso aos seus dados, a correção de informações incorretas, a exclusão de dados, a portabilidade de dados e a possibilidade de se opor ao processamento. As organizações são obrigadas a respeitar e atender a esses direitos, representando um limite importante para o tratamento de dados pessoais.

**Segurança (Artigo 46):** A LGPD estabelece que as organizações devem implementar medidas adequadas para proteger os dados pessoais contra acesso não autorizado, vazamentos ou outras ameaças, garantindo a integridade e a confidencialidade das informações.

Esses limites e permissões da LGPD, baseados nos dispositivos legais da própria lei, buscam promover uma cultura de respeito à privacidade, equilibrando os interesses das organizações com a proteção dos direitos individuais e assegurando a conformidade com as normas de privacidade e proteção de dados. Qualquer violação desses limites pode resultar em sanções, de acordo com as disposições legais da LGPD.

#### 4.1. O PAPEL DO CONSENTIMENTO

O conceito de consentimento na LGPD é fundamental, e a definição de consentimento na lei pode ser encontrada na obra de Bruno Bioni (2021), renomado especialista em privacidade e proteção de dados. Segundo ele, o consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Essa definição enfatiza que o consentimento deve ser voluntário, ou seja, a pessoa deve dar seu consentimento de espontânea vontade, após ter sido devidamente informada sobre como seus dados pessoais serão usados.

O consentimento inequívoco é um dos princípios-chave da proteção de dados pessoais, e sua importância reside na garantia de que o tratamento de dados seja feito de maneira ética, transparente e com o devido respeito aos direitos e à privacidade dos titulares dos dados. Isso beneficia tanto as organizações quanto os indivíduos, ao estabelecer uma base sólida para o processamento de informações pessoais.

Além disso, o consentimento deve ser específico para cada finalidade de tratamento de dados, ou seja, o titular dos dados deve saber para que exatamente seus dados serão utilizados.

Essa definição de consentimento na LGPD visa garantir que as pessoas tenham controle sobre o uso de seus dados pessoais e que suas informações sejam tratadas de maneira transparente e responsável por organizações que coletam e processam esses dados.

O consentimento desempenha um papel de extrema relevância na Lei Geral de Proteção de Dados (LGPD), sendo uma das pedras angulares da regulamentação de privacidade no Brasil. Isso se evidencia a partir das citações dos dispositivos legais da LGPD:

Legitimidade do Tratamento (artigo 7º e 11): O consentimento é uma das bases legais para o tratamento de dados pessoais, conforme estabelecido no artigo 7º da LGPD. Sem o consentimento, o tratamento de dados só pode ocorrer em situações específicas, como o cumprimento de obrigações legais (artigo 7º, II), o cumprimento de contratos (artigo 7º, V), ou

o legítimo interesse da organização (artigo 7º, IX).

Cumprimento da LGPD (artigo 52): A obtenção de consentimento adequado é uma obrigação legal para as organizações que desejam cumprir a LGPD. O artigo 52 da LGPD prevê sanções para o não cumprimento da lei, o que inclui a obtenção de consentimento de forma inadequada.

Flexibilidade para o Titular dos Dados (Artigo 18): O consentimento pode ser revogado a qualquer momento pelo titular dos dados, conforme estipulado no Artigo 18 da LGPD. Isso dá aos indivíduos maior controle sobre suas informações e a capacidade de interromper o tratamento de dados quando desejarem.

Relevância para o Mercado e a Confiança do Consumidor: A conformidade com a LGPD, incluindo a obtenção de consentimento, é fundamental para a construção de confiança entre as organizações e seus clientes. Os consumidores tendem a confiar mais em empresas que respeitam sua privacidade, o que pode ter um impacto positivo nos negócios (Bioni, 2021).

Em resumo, o consentimento desempenha um papel crucial na LGPD, garantindo a proteção da privacidade e dos direitos dos titulares dos dados, promovendo a transparência nas práticas de tratamento de dados e estabelecendo uma base legal sólida para o tratamento de informações pessoais, conforme respaldado pelos dispositivos legais da própria lei. É uma ferramenta fundamental para a conformidade com a LGPD e para a construção da confiança entre organizações e seus clientes.

A discussão em torno da Lei Geral de Proteção de Dados (LGPD) provocou transformações significativas no mercado, uma vez que essa legislação estabelece requisitos essenciais para o tratamento de dados pessoais ou sensíveis. A LGPD coloca a proteção da privacidade no centro das operações, exigindo que o responsável por esses dados obtenha o consentimento explícito do titular antes de coletá-los ou divulgá-los.

Além do mais, a LGPD categoriza os dados em duas principais classes no seu artigo 5º: dados pessoais, que incluem informações como nome, RG, data de nascimento, entre outros; e dados sensíveis, que englobam uma gama de informações delicadas, como origem racial, opiniões políticas, dados genéticos, biometria, informações de saúde, crenças religiosas, filosofias, filiação a sindicatos e orientação sexual.

É fundamental ressaltar que, de acordo com a Lei Geral de Proteção de Dados (LGPD), o ônus da prova de que o consentimento foi obtido em conformidade com a legislação recai sobre o controlador de dados, conforme estabelecido no artigo 15 da LGPD.

O consentimento do titular dos dados, conforme disposto nos artigos 5º e 8º da LGPD,

pode ser tanto expresso, por escrito, quanto tácito. No entanto, é importante observar que o titular tem o direito de revogar o consentimento a qualquer momento, conforme previsto no artigo 8º, § 5º da LGPD. O consentimento não pode ser obtido mediante erro, dolo, coação, lesão, estado de perigo ou fraude, de acordo com o artigo 8º, § 4º da mesma lei.

Ademais, o consentimento deve ser específico para cada situação, requerendo a renovação quando houver mudanças no tratamento dos dados, de acordo com o artigo 11 da LGPD. Caso o titular não deseje mais consentir com o tratamento de seus dados pessoais, mesmo após a renovação, ele tem o direito de revogá-lo a qualquer momento, conforme o artigo 8º, § 5º da LGPD, desde que o faça de maneira expressa, gratuita e facilitada.

O controlador de dados, conforme determinado no Artigo 5º, deve esclarecer ao titular a necessidade dos dados coletados para a prestação do serviço, bem como se os dados são tratados exclusivamente por ele ou se há compartilhamento com terceiros.

É crucial salientar que o controlador será monitorado durante todo o período de uso dos dados, uma vez que esses dados não pertencem nem ao operador nem ao controlador, conforme preconizado nos artigos 5º e 6º da LGPD. O controle e a responsabilidade pela conformidade com a LGPD recaem inteiramente sobre o controlador, conforme estabelecido nos artigos 6º e 41 da LGPD. Portanto, é imperativo que ele esteja em conformidade com a legislação, garantindo a proteção dos dados pessoais do titular e cumprindo com as obrigações previstas na LGPD.

#### 4.2. A IMPORTÂNCIA DA TRANSPARÊNCIA EM TODAS AS ETAPAS DO MANUSEIO DOS DADOS

Um dos pilares fundamentais de uma sociedade democrática reside na confiança que os cidadãos depositam no Estado, e a transparência desempenha um papel primordial nessa construção. A importância da transparência varia ao longo da história, mas é inegável a contínua luta pela sua preservação.

Recentemente, em meio a debates acalorados sobre a administração do imenso volume de dados gerados pela 4ª revolução industrial, tomadores de decisão, a sociedade e instituições se envolveram em discussões profundas. Escândalos recentes trouxeram à tona as inúmeras possibilidades de utilização de informações pessoais, suscitando uma crescente preocupação em relação aos riscos políticos e regulatórios associados a essa questão.

No Brasil, o artigo 5º da Constituição Federal de 1988 assegura o acesso à informação

como um direito de todos os cidadãos. Em 2004, o Ministério da Transparência e Controladoria-Geral da União lançou o Portal da Transparência do Governo Federal<sup>ii</sup>, que passou por reformulações para atender à demanda crescente e às obrigações de transparência.

Em 2011, a promoção da transparência pública ganhou ainda mais destaque com a promulgação da Lei do Acesso à Informação (Brasil, 2011), marcando um avanço significativo na democratização do acesso às informações públicas em nosso país.

Além de ampliar a visibilidade dos atos governamentais e simplificar o acesso aos dados de gestão, as informações passaram a ser divulgadas de maneira mais clara e organizada, pelo menos essa era a expectativa. Qualquer questionamento sobre transparência, seja por parte dos cidadãos ou da mídia, é imediatamente considerado.

O estímulo contínuo às ações que promovem o acesso à informação é evidente. Há não muito tempo, o governador do Rio de Janeiro, Wilson Witzel, sancionou a Lei Estadual 8.719/2020, proposta pelo deputado Carlo Caiado (DEM)<sup>iii</sup>, que determina a criação de um portal de transparência dedicado à divulgação dos gastos provenientes de royalties e participação na produção de petróleo repassados pela União.

A importância da transparência em todas as etapas do manuseio de dados está respaldada em diversos dispositivos legais, principalmente na Lei Geral de Proteção de Dados (LGPD) no Brasil. Abaixo, apresento a relevância da transparência através dessa lei:

**Respeito à Privacidade (Artigo 2º):** A LGPD, em seu Artigo 2º, estabelece o respeito à privacidade como um de seus princípios fundamentais. A transparência é um elemento essencial para garantir que os titulares de dados tenham conhecimento das práticas de tratamento e possam exercer seus direitos de privacidade.

**Princípio da Finalidade (Artigo 6º):** O Artigo 6º da LGPD determina que o tratamento de dados pessoais deve ocorrer para finalidades legítimas, específicas e informadas ao titular dos dados. Essa informação deve ser comunicada de forma transparente, garantindo que os titulares compreendam as finalidades do tratamento.

**Direito de Acesso (Artigo 18):** A LGPD concede aos titulares dos dados o direito de acessar informações sobre o tratamento de seus dados pessoais. A transparência é crucial para permitir o exercício desse direito, assegurando que os titulares dos dados saibam como suas informações estão sendo tratadas.

**Direito de Retificação e Exclusão (Artigo 18):** Os titulares dos dados têm o direito de solicitar a correção de dados imprecisos e a exclusão de informações irrelevantes ou desnecessárias. A transparência é fundamental para garantir que os titulares dos dados tenham

conhecimento desses direitos e possam exercê-los.

**Responsabilidade das Organizações (Artigo 6º):** A LGPD estabelece que as organizações são responsáveis pelo tratamento de dados pessoais. Isso inclui a responsabilidade de ser transparente sobre as práticas de tratamento, implementar medidas de segurança e garantir a conformidade com a lei.

**Encarregado de Proteção de Dados (Artigo 41):** A designação de um Encarregado de Proteção de Dados (DPO) é obrigatória em certas situações, de acordo com o Artigo 41 da LGPD. O DPO desempenha um papel crítico na supervisão das questões de privacidade e proteção de dados e é um ponto de contato para os titulares dos dados, promovendo a transparência nas operações da organização.

**Penas e Sanções (Artigo 52):** A LGPD estabelece sanções para organizações que não cumprem suas disposições, incluindo multas substanciais. A falta de transparência nas práticas de tratamento de dados pode resultar em penalidades, destacando a importância da transparência na conformidade com a lei.

**Relações com Regulamentações Internacionais (Artigo 33):** A LGPD estabelece requisitos específicos para a transferência internacional de dados. A transparência sobre essas transferências e o cumprimento de padrões internacionais são essenciais para garantir a conformidade com a LGPD em cenários globais.

Em síntese, a LGPD enfatiza a importância da transparência em todas as etapas do manuseio de dados pessoais. A legislação não apenas estabelece a obrigatoriedade de ser transparente em relação ao tratamento de dados, mas também prevê direitos e responsabilidades específicos para garantir que os titulares de dados tenham informações claras e acesso aos seus dados pessoais. A conformidade com essas disposições legais contribui para a proteção da privacidade e o respeito pelos direitos dos titulares de dados.

Esse enfoque, ao exigir que as empresas comuniquem de forma transparente aos usuários como exatamente os dados coletados serão utilizados, reforça a tendência à transparência no tratamento de dados pessoais.

Um exemplo recente que demonstra a importância da transparência e conformidade com regulamentos de proteção de dados é a multa imposta pela agência de proteção de dados da França ao Google, no valor de 50 milhões de euros (cerca de R\$ 213 milhões), por violação da Regulamento Geral de Proteção de Dados (GDPR)<sup>iv</sup>, que regula o uso de dados na União Europeia.

O regulador francês alegou que o Google não estava sendo transparente e claro ao

informar aos usuários como os dados pessoais eram coletados em seus serviços, incluindo o YouTube, o Maps e o mecanismo de busca, para a personalização de anúncios publicitários.

A LGPD foi inspirada na GDPR e, como a legislação europeia, tem um alcance global. Isso significa que empresas em todo o mundo, mesmo aquelas sem sede na União Europeia, precisam ajustar seus procedimentos de tratamento de dados pessoais se tiverem filiais, representações ou operações na região.

A LGPD, portanto, tem como principal objetivo proteger a privacidade dos cidadãos e demandar maior transparência por parte das empresas que coletam dados sensíveis. Além disso, quando se trata de dados públicos, há um reconhecimento generalizado de sua importância na gestão de riscos políticos e regulatórios. O acesso transparente a esses dados é essencial para que os cidadãos possam compreender como os recursos públicos são utilizados e permanecerem informados sobre questões relacionadas à administração pública no Brasil.

A análise criteriosa de dados públicos permite aos gestores tomarem decisões mais informadas e estratégicas. Com informações transparentes, abrangentes e precisas, as empresas ganham uma vantagem competitiva significativa, atraindo investidores e evitando situações adversas que possam prejudicar sua reputação. A transparência nos dados é, portanto, um pilar fundamental para a conformidade com regulamentos de proteção de dados e para o sucesso nos negócios.

#### 4.3. CASOS EM QUE O CONSENTIMENTO É DISPENSADO

A Lei Geral de Proteção de Dados (LGPD) revolucionou o tratamento de informações pessoais no Brasil, estabelecendo princípios e regras claras para proteger a privacidade dos cidadãos. No cerne dessa legislação, encontra-se o artigo 7º, que define as hipóteses nas quais o tratamento de dados pessoais é permitido, mesmo na ausência do consentimento do titular.

##### **4.3.1. Hipóteses para o Tratamento de Dados Pessoais sem Consentimento do Titular**

O artigo 7º da LGPD delimita as situações em que o tratamento de dados pessoais é autorizado sem a necessidade de consentimento explícito do titular. Essas hipóteses refletem os princípios fundamentais da LGPD, como o respeito à autodeterminação do titular e a promoção da transparência e segurança no uso de informações pessoais.

Cumprimento de Obrigação Legal (Inciso II): O tratamento é permitido para atender a obrigações legais ou regulatórias, garantindo o cumprimento da lei.

Administração Pública (Inciso III): A administração pública pode utilizar dados para políticas públicas, desde que siga as disposições da lei.

Realização de Estudos por Órgãos de Pesquisa (Inciso IV): Órgãos de pesquisa podem tratar dados pessoais para estudos, desde que anonimem sempre que possível.

Execução de Contrato (Inciso V): O tratamento é autorizado na execução de contratos dos quais o titular é parte.

Exercício de Direitos em Processos (Inciso VI): O tratamento é autorizado para o exercício regular de direitos em processos judiciais, administrativos ou arbitrais.

Proteção da Vida e Incolumidade (Inciso VII): A segurança da vida e integridade física do titular ou terceiros justifica o tratamento de dados.

Tutela da Saúde (Inciso VIII): Profissionais de saúde e autoridades sanitárias podem tratar dados para a saúde, com foco na segurança e qualidade do atendimento.

Interesses Legítimos (Inciso IX): O controlador pode tratar dados para atender a interesses legítimos, desde que não prejudique os direitos fundamentais do titular.

Proteção do Crédito (Inciso X): O tratamento é autorizado para a proteção do crédito, de acordo com a legislação aplicável.

#### **4.3.2. Outras Disposições Relevantes**

Além dessas hipóteses, a LGPD estabelece regras adicionais que reforçam a proteção de dados:

Tratamento de Dados Públicos (§ 3º): Dados de acesso público devem ser tratados com base na finalidade, boa-fé e interesse público que justificaram sua disponibilização.

Dados Manifestamente Públicos (§ 4º): Para dados tornados manifestamente públicos pelo titular, o consentimento não é necessário, contanto que sejam respeitados os direitos do titular e os princípios da LGPD.

Compartilhamento de Dados (§ 5º): Quando o controlador precisa compartilhar dados com outros controladores, um consentimento específico do titular é necessário, exceto em casos de dispensa previstos na lei.

Obrigações Permanentes (§ 6º): A ausência de consentimento não isenta os agentes de tratamento de outras obrigações da LGPD, incluindo a observância dos princípios e garantia

dos direitos do titular.

Tratamento Posterior (§ 7º): Dados citados nos §§ 3º e 4º podem ser tratados posteriormente para novas finalidades, desde que se respeitem os propósitos legítimos, a proteção dos direitos do titular e os fundamentos e princípios da LGPD.

#### 4.4. LEGÍTIMO INTERESSE

A Lei Geral de Proteção de Dados (LGPD) no Brasil representa um marco importante na garantia da privacidade e proteção dos dados pessoais dos cidadãos. No entanto, um dos aspectos mais desafiadores e debatidos da LGPD é a utilização do "legítimo interesse" como base legal para o tratamento de dados pessoais sem o consentimento do titular. Embora essa base legal tenha sua relevância, é crucial que seja aplicada com cautela, devido à sua natureza ampla e interpretativa.

O Artigo 10 da LGPD define o legítimo interesse do controlador como uma base legal para o tratamento de dados pessoais, desde que esse tratamento seja destinado a finalidades legítimas, consideradas a partir de situações concretas. As finalidades legítimas podem incluir o apoio e promoção das atividades do controlador, bem como a proteção dos direitos do titular ou a prestação de serviços benéficos a ele. No entanto, a LGPD não fornece uma definição exata do que constitui legítimo interesse, preferindo deixá-lo de forma ampla e exemplificativa (Bioni, 2019).

É importante destacar que o legítimo interesse não deve ser usado para preencher lacunas de fundamentação legal. Em vez disso, é recomendável que o controlador busque obter o consentimento do titular sempre que possível, antes de realizar qualquer tratamento de dados. Somente quando isso não for viável, o legítimo interesse deve ser considerado como uma alternativa (Bioni, 2019).

Para garantir a aplicação adequada do legítimo interesse, o controlador deve avaliar cuidadosamente a situação em questão. Essa avaliação envolve vários aspectos:

**Finalidade Legítima:** O tratamento de dados deve ter uma finalidade legítima que não viole a legislação vigente. Além disso, o contexto em que os dados são processados deve ser

levado em consideração, indo além do respeito às leis, conforme destacado pela Opinião 03/2013 do Grupo de Trabalho do Artigo 29 (WP29).

Situação Concreta: Deve haver uma relação prévia entre o controlador e o titular dos dados para que o legítimo interesse seja utilizado. A existência de uma legítima expectativa por parte do titular e a compatibilidade do novo tratamento com a finalidade original da relação entre as partes também são considerações cruciais.

Respeito aos Princípios da LGPD: O controlador deve observar os princípios da LGPD, conforme estabelecido no Artigo 10, §1º e §2º. Isso inclui tratar apenas os dados pessoais estritamente necessários para a finalidade pretendida e adotar medidas para garantir a transparência do tratamento.

Além disso, o controlador deve estar preparado para fornecer um relatório de impacto à proteção de dados pessoais quando solicitado pela autoridade nacional, observando os segredos comerciais e industriais.

Uma prática recomendada, embora não explicitamente exigida pela LGPD, é a realização de uma "Avaliação de Legítimo Interesse" (LIA). Essa avaliação, comumente utilizada em países com rigorosas regulamentações de proteção de dados, visa encontrar um equilíbrio entre o uso do legítimo interesse pelo controlador e o respeito aos direitos e liberdades dos titulares de dados pessoais. A LGPD não exige explicitamente o LIA, mas o Artigo 37 ressalta a necessidade de manter registros das operações de tratamento de dados pessoais, especialmente quando baseado no legítimo interesse, o que pode ser considerado uma boa prática (Bioni, 2019).

Outro ponto de atenção é o uso do legítimo interesse por terceiros. A LGPD menciona a possibilidade, mas não fornece diretrizes específicas para essa situação, deixando espaço para regulamentações adicionais da Autoridade Nacional de Proteção de Dados (ANPD).

Em conclusão, o legítimo interesse é uma base legal importante na LGPD, mas sua aplicação requer uma avaliação criteriosa e respeito aos princípios da lei. A ampla margem interpretativa e a falta de diretrizes específicas tornam sua utilização um desafio que a ANPD deve abordar com orientações claras. Em última análise, o equilíbrio entre a proteção da privacidade dos titulares de dados e as necessidades das organizações é essencial para uma implementação eficaz da LGPD.

#### 4.5. SANÇÕES ADMINISTRATIVAS DA LGPD: GARANTINDO O CUMPRIMENTO

## DA LEI COM RESPONSABILIDADE PROATIVA

Seguindo as diretrizes estabelecidas por Bioni (2021), a Lei Geral de Proteção de Dados (LGPD) estabelece um conjunto de sanções administrativas aplicáveis aos agentes de tratamento de dados em caso de infrações às normas previstas na legislação. Essas sanções visam assegurar que a LGPD seja efetivamente cumprida e que os direitos dos titulares de dados sejam protegidos. Abordaremos essas sanções, bem como os critérios que orientam sua aplicação.

### Sanções Aplicáveis:

**Advertência:** Os agentes de tratamento podem receber uma advertência, que inclui a indicação de um prazo para tomar medidas corretivas.

**Multa Simples:** Uma multa que pode atingir até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada a R\$ 50.000.000,00 por infração.

**Multa Diária:** Além da multa simples, a LGPD permite a aplicação de multas diárias, observando o limite total estabelecido para a multa simples.

**Publicização da Infração:** Após a devida apuração e confirmação da infração, os detalhes da violação podem ser publicizados.

**Bloqueio de Dados:** A LGPD possibilita o bloqueio dos dados pessoais relacionados à infração até que esta seja regularizada.

**Eliminação de Dados:** Em casos mais graves, os dados pessoais relacionados à infração podem ser eliminados.

**Suspensão do Funcionamento do Banco de Dados:** Pode haver a suspensão parcial do funcionamento do banco de dados relacionado à infração, pelo período máximo de 6 meses, prorrogável.

**Suspensão do Exercício da Atividade de Tratamento:** A autoridade nacional pode suspender o exercício da atividade de tratamento dos dados pessoais relacionados à infração pelo período máximo de 6 meses, prorrogável.

**Proibição de Atividades de Tratamento de Dados:** Também pode ser aplicada a proibição, total ou parcial, do exercício de atividades relacionadas ao tratamento de dados.

### Critérios para Aplicação:

Conforme previsto no § 1º do artigo 52, as sanções da LGPD são aplicadas considerando vários critérios e parâmetros, como:

- I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- II - a boa-fé do infrator;
- III - a vantagem auferida ou pretendida pelo infrator;
- IV - a condição econômica do infrator;
- V - a reincidência;
- VI - o grau do dano;
- VII - a cooperação do infrator;
- VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
- IX - a adoção de política de boas práticas e governança;
- X - a pronta adoção de medidas corretivas; e
- XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

#### **4.5.1. Responsabilidade Proativa e Governança**

A LGPD, de acordo com Danilo Doneda (), traz à tona a importância da responsabilidade proativa por parte das organizações. É fundamental adotar medidas preventivas para evitar prejuízos, pois lidar com danos após sua ocorrência pode ser complexo e dispendioso.

A legislação também exige governança, cumplicidade e responsabilidade por parte das organizações no que diz respeito ao tratamento de dados pessoais. Os agentes de tratamento precisam agir de forma ética e transparente, adotando políticas internas que visem ao tratamento seguro e adequado de dados.

A LGPD veio para estabelecer limites ao que pode ser feito com informações que não pertencem à empresa. Ela visa proteger a privacidade e os direitos dos titulares de dados, além de garantir que as organizações ajam de maneira responsável e em conformidade com a legislação.

Em um mundo cada vez mais digital, em que os dados são ativos valiosos, a LGPD desempenha um papel crucial na proteção desses dados e na promoção da confiança entre as empresas e os indivíduos.

## CONCLUSÃO

A Lei Geral de Proteção de Dados (LGPD) marca um divisor de águas na forma como a sociedade lida com informações pessoais no contexto digital. Sua promulgação reflete a necessidade de garantir os direitos fundamentais de liberdade, intimidade e privacidade em um cenário cada vez mais voltado para a coleta, processamento e compartilhamento de dados. Para isso, a LGPD estabelece um conjunto de prerrogativas e limites que afetam tanto os titulares de dados quanto as organizações que lidam com informações pessoais.

Do ponto de vista dos titulares de dados, a LGPD confere um conjunto de direitos fundamentais. Eles têm o direito de conhecer quais informações pessoais estão sendo coletadas e com que finalidade. Além disso, podem acessar seus próprios dados, corrigi-los, anonimizá-los e, em muitos casos, transferi-los para outros provedores de serviços. A revogação do consentimento é outro direito importante, permitindo que os titulares retirem sua autorização para o tratamento de seus dados. Isso proporciona aos indivíduos um nível significativo de controle sobre suas informações pessoais.

Por outro lado, a LGPD impõe limites significativos às organizações que tratam dados pessoais. Elas devem atuar de maneira responsável, coletando e processando apenas os dados necessários para fins legítimos e em conformidade com a lei. Isso requer a implementação de medidas de segurança para proteger essas informações e a transparência no tratamento de dados. A legislação também estabelece sanções administrativas para as organizações que não cumprem suas disposições, incluindo multas substanciais e outras medidas corretivas. As multas podem variar de advertências iniciais até multas pesadas, com o valor das multas diárias adicionais em caso de não conformidade contínua.

Essas prerrogativas e limites impostos pela LGPD são essenciais para equilibrar a proteção da privacidade do cidadão com a capacidade de inovar e utilizar dados para aprimorar produtos e serviços. A LGPD não pretende inibir o progresso tecnológico, mas sim garantir que ele ocorra de maneira ética e responsável, sob a ameaça de penalidades significativas para as organizações que não cumpram a lei.

Em conclusão, a LGPD desempenha um papel fundamental em nossa sociedade digital. Ela fornece aos cidadãos os meios para proteger sua privacidade e seus dados pessoais, enquanto impõe limites necessários para garantir que as organizações ajam de maneira responsável e transparente. As penalidades estabelecidas pela LGPD são um lembrete claro de que o não cumprimento pode resultar em consequências sérias, tornando a conformidade com

essa lei essencial tanto para a proteção dos cidadãos quanto para a continuidade dos negócios no cenário digital atual.

## REFERÊNCIAS

ADVOGADOS, Assis e Mendes. Histórico das leis de proteção de dados e da privacidade na internet. Disponível em: <https://assisemendes.com.br/historico-protecao-de-dados/>. Acesso em: 28 out. 2021.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Gen, Editora Forense, 2021.

BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 9 ed. rev. atual. – São Paulo, 2021.

BRASIL. Câmara dos Deputados. Agência Câmara de Notícias. Disponibilizado em: [https://www.camara.leg.br/noticias/886604-medida-provisoria-transforma-a-autoridade-nacional-de-protecao-de-dados-em-autarquia/#:~:text=A%20Medida%20Provis%C3%B3ria%201124%2F22,ter%C3%A7a%2Deira%20\(14\)](https://www.camara.leg.br/noticias/886604-medida-provisoria-transforma-a-autoridade-nacional-de-protecao-de-dados-em-autarquia/#:~:text=A%20Medida%20Provis%C3%B3ria%201124%2F22,ter%C3%A7a%2Deira%20(14).). Acessado em: 18 de junho de 2023.

BRASIL. Decreto-lei nº 200, de 25 de fevereiro de 1967. Disponibilizado em: [https://www.planalto.gov.br/ccivil\\_03/decreto-lei/del0200.htm](https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm). Acesso em: 18 de junho de 2023.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial [da República Federativa do Brasil], Poder Legislativo, Brasília, DF, 23 abr. 2014. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/ato2011-2014/2014/lei/112965.htm](https://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/112965.htm). Acesso em: 19 abr. 2023.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: [\[https://www.planalto.gov.br/ccivil\\_03/ato2011-2014/2011/lei/112527.htm\]](https://www.planalto.gov.br/ccivil_03/ato2011-2014/2011/lei/112527.htm). Acesso em:

01/10/2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/ato2019-2022/2020/lei/114020.htm](https://www.planalto.gov.br/ccivil_03/ato2019-2022/2020/lei/114020.htm)>. Acesso em: 19 abr. 2023.

BRASIL. Medida Provisória nº 954/2020. <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619#:~:text=Disp%C3%B5e%20sobre%20o%20compartilhamento%20de,emerg%C3%Aancia%20de%20sa%C3%BAde%20p%C3%BAblica%20de>. Acesso em: 11 de outubro de 2023.

BRASIL. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/decreto/d0678.htm](https://www.planalto.gov.br/ccivil_03/decreto/d0678.htm). Acesso em: 19 de junho de 2023.

BRASIL. Senado Federal. Medida Provisória nº 1124, de 2022. Disponível em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/15361>. Acessado em: 18 de junho de 2023.

CARVALHO, João Paulo Furtado. História da Privacidade de Dados e suas Legislações. ZUP, 2021. Disponível em: <https://www.zup.com.br/blog/historia-da-privacidade-de-dados>. Acesso em: 25 out. 2021.

CONGRESSO NACIONAL. CÂMARA DOS DEPUTADOS. Entenda a Tramitação da Medida Provisória. Disponibilizado em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/entenda-a-tramitacao-da-medida-provisoria>. Acessado em: 18 de junho de 2023.

COUTINHO, Clara Pereira; BOTTENTUIT JUNIOR, João Batista. Blog e Wiki: os futuros professores e as ferramentas da Web 2.0. 2007. Disponível em: <https://repositorium.sdum.uminho.pt/handle/1822/7358>. Acesso em: 12 de março de 2022.

DONEDA, D. Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral

de proteção de dados. São Paulo: Thomson Reuters Brasil, 2019.

GRINBERG, Keila. Quem é o Grande Irmão?. Rio de Janeiro: Universidade federal do Rio de Janeiro, Instituto Ciência Hoje, 2023. Disponível em: <https://cienciahoje.org.br/coluna/quem-e-o-grande-irmao/>. Acesso em: 19 de junho de 2023.

GUERRA, Sidney. O Direito à Privacidade na Internet, 1ª edição, editora América Jurídica, 2014.

HAYEK, Friedrich. O Caminho da Servidão. São Paulo: LVM Editora, 2010.

LEI Geral de Proteção de Dados Pessoais (LGPD). Tribunal Regional Federal da 3ª Região, 2020. Disponível em: <https://www.trf3.jus.br/lei-geral-de-protecao-de-dados-pessoais-lgpd/principios>. Acesso em: 27 out. 2021.

LEMOS, Ronaldo. O marco civil como símbolo do desejo por inovação no Brasil. In Marco Civil da Internet. George Salomão, Ronaldo Leite (coordenadores). São Paulo: Atlas, 2014. p. 04.

LGPD: o que é, principais determinações e resumo. FIA – Fundação Instituto de Administração, 30 dez. 2019. Disponível em: <https://fia.com.br/blog/lgpd/>. Acesso em: 25 out. 2021.

LIMA, Cíntia Rosa Pereira D. ANPD e LGPD: Desafios e perspectivas. [Digite o Local da Editora]: Grupo Almedina (Portugal), 2021. Ebook. ISBN 9786556272764. Disponível em: <https://unibb.minhabiblioteca.com.br/#/books/9786556272764/>. Acesso em: 20 set. 2022.

MACIEL, Rafael Fernandes. Manual prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18). Goiânia: RM Digital Education, 2019.

MARRIOT, Emma. A história do mundo para quem tem pressa. Rio de Janeiro: Valentina, 2015.

MARX, Karl. O Capital. São Paulo: Veneta, 2014.

MEDEIROS, Júlia Mayara. Advogada, <https://www.hsbs.com.br/importancia-do-consentimento-para-a-lgpd/#:~:text=Ser%20utilizado%20para%20uma%20finalidade,de%20dados%20pessoais%20ser%C3%A3o%20nulas>. Acesso em: 11 de outubro de 2023.

MELLO, Celso Antônio Bandeira. Curso de Direito Administrativo. 26 ed. São Paulo: Malheiros. 2009. p. 882 – 883.

MORAIS, Carlos Tadeus Queiroz de; LIMA, José Valdeni de; FRANCO, S. R. K. Conceitos sobre Internet e Web. Porto Alegre: Editora da UFRGS, 2017.

Organização Para a Cooperação e Desenvolvimento Económicos. Síntese Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais. Disponível em: <https://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em: 18 de junho de 2023.

ORWELL, Jorge. 1984. São Paulo: Principis, 2021.

PAESANI, Liliana Minardi. Direito e Internet: liberdade de informação, privacidade e responsabilidade civil. 6. ed. São Paulo: Atlas, 2014.

PECK, Patrícia. Proteção de dados pessoais. 2. ed. São Paulo: Editora Saraiva, 2020.

PEREIRA, Marcelo Cardoso. Direito à Intimidade na Internet, 4ª edição, editora Juruá, 2016.

PESTANA, Marcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). São Paulo: Revista Consultor Jurídico, 2020. Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 14 out. 2021.

POHLMANN, Sérgio Antônio. LGPD Ninja – Entendendo e implementando a Lei Geral de Proteção de Dados nas empresas. São Paulo: Editora Fross, 2019.

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

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.

Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral de Proteção de Dados - RGPD).

Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 19 abr. 2023.

REZENDE, Rafaela Couto. INFOESCOLA. Período Quaternário. Disponível em: <https://www.infoescola.com/geologia/periodo-quaternario/>. Acesso em: 15 de junho de 2023.

SANTOS, Maykon Adler Oliveira. ARAÚJO, Jeferson Sousa de. REGO, Ihgor Jean. A história Brasileira de proteção aos dados: o advento da lei geral de proteção de dados pessoais e a sua influência no acesso aos dados médicos no Brasil. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano. 06, Ed. 12, Vol. 01, pp. 172-198. Dezembro de 2021. ISSN: 2448-0959. Disponível em: <https://www.nucleodoconhecimento.com.br/lei/advento-da-lei>. Acesso em 19 de junho de 2023.

SMITH, Adam. A Riqueza das Nações. Rio de Janeiro: Nova Fronteira, 2023.

TREIN, Daiana; SCHLEMMER, E. D. R. Projetos de aprendizagem baseados em problema no contexto da web 2.0: Possibilidades para a prática pedagógica. Revista ECurriculum, São Paulo, v. 4, ed. 2, 2019.

TZU, Sun. A arte da guerra: os treze capítulos originais. São Paulo: Geração Editorial, 2009.

WESTIN, Alan F. Privacy and Freedom. Nova Iorque: Atheneum Publishers, 1967.

---

<sup>i</sup> BBC News Brasil. O que é a 4ª revolução industrial - e como ela deve afetar nossas vidas. Disponível em: <https://www.bbc.com/portuguese/geral-37658309>. Acessado em: 01/10/2023.

<sup>ii</sup> Portal da Transparência. O que é e como funciona. Disponível em: <https://portaldatransparencia.gov.br/sobre/o-que-e-e-como-funciona>. Acessado em: 01/10/2023.

<sup>iii</sup> Assembleia Legislativa do estado do Rio de Janeiro. AGORA É LEI: RIO TERÁ PORTAL DA TRANSPARÊNCIA DOS ROYALTIES DO PETRÓLEO. Disponível em: <https://www.alerj.rj.gov.br/Visualizar/Noticia/48098?AspxAutoDetectCookieSupport=1>. Acessado em: 01/10/2023.

<sup>iv</sup> **O Globo**. França multa Google em 50 milhões de euros por violação de lei de privacidade na UE. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/01/21/franca-multa-google-em-50-milhoes-de-euros-por-violacao-de-lei-de-privacidade-na-ue.ghtml>.